## Request for Proposals (RFP) for South Dakota Medicaid Enterprise Prior Authorization, Utilization Management and Care Management Information System

PROPOSALS ARE DUE NO LATER THAN July 9, 2019 5:00 pm CDT

<table>
<thead>
<tr>
<th>RFP #1710</th>
<th>BUYER: South Dakota Department of Social Services, Division of Medical Services</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>POC: Dawson Lewis <a href="mailto:Dawson.Lewis@state.sd.us">Dawson.Lewis@state.sd.us</a></td>
</tr>
</tbody>
</table>

### READ CAREFULLY

<table>
<thead>
<tr>
<th>FIRM NAME:</th>
<th>____________________________</th>
<th>AUTHORIZED SIGNATURE:</th>
<th>____________________________</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADDRESS:</td>
<td>____________________________</td>
<td>TYPE OR PRINT NAME:</td>
<td>____________________________</td>
</tr>
<tr>
<td>CITY/STATE:</td>
<td>____________________________</td>
<td>TELEPHONE NO:</td>
<td>____________________________</td>
</tr>
<tr>
<td>ZIP (9 DIGIT):</td>
<td>____________________________</td>
<td>FAX NO:</td>
<td>____________________________</td>
</tr>
<tr>
<td>FEDERAL TAX ID#:</td>
<td>____________________________</td>
<td>E-MAIL:</td>
<td>____________________________</td>
</tr>
</tbody>
</table>

### PRIMARY CONTACT INFORMATION

<table>
<thead>
<tr>
<th>CONTACT NAME:</th>
<th>____________________________</th>
<th>TELEPHONE NO:</th>
<th>____________________________</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAX NO:</td>
<td>____________________________</td>
<td>E-MAIL:</td>
<td>____________________________</td>
</tr>
</tbody>
</table>
1.0 GENERAL INFORMATION

1.1 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

The State of South Dakota (the “State”) is engaged in a Medicaid Enterprise System Modernization Program (the “MES Modernization Program”). As part of the Modernization Program, by way of this RFP the State Department of Social Services (“DSS”), Division of Medical Services (“DMS”), is requesting proposals to provide, implement, maintain, operate and support a functionally comprehensive, state-of-the-art, flexible, scalable and extensive information system that will support prior authorization, utilization management and care management functions (“System”). Initially the System will support the State’s Medicaid and CHIP programs, but the State expects that over time the functionality of the System will be extended to other programs and possibly to other State agencies.

DSS may also be interested in the capability of the Offerors to provide prior authorization professional services required to support the South Dakota Medicaid program. For clarity, the prior authorization professional services are considered as an Optional Scope of Work for this procurement to be used for consideration during the contract award process.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Division of Medical Services is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Social Services. The reference number for the transaction is RFP #1710. Refer to this number on all proposals, correspondence, and documentation relating to the RFP.

Please refer to the Department of Social Services website link http://dss.sd.gov/keyresources/rfp.aspx for the RFP, any related questions/answers, changes to schedule of activities, amendments, etc.

1.3 LETTER OF INTENT

All interested offerors are requested to submit a non-binding Letter of Intent to respond to this RFP. While preferred, a Letter of Intent is not mandatory to submit a proposal.

The letter of intent must be received by email in the Department of Social Services by no later than May 21st, 2019 and must be addressed to Mr. Dawson Lewis via email at: Dawson.Lewis@state.sd.us. Place the following, exactly as written, in the subject line of your email: Letter of Intent for RFP #1710. Be sure to reference the RFP number in any attached letter or document. The Letter of Intent must clearly name the Contractor intending to submit the bid and must provide a contact name, phone number and email address for any future correspondence.

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication May 7, 2019
Letter of Intent to Respond Due (optional) May 21, 2019
Deadline for Submission of Written Inquiries May 21, 2019
Responses to Offeror Questions June 4, 2019
Proposal Submission July 9, 2019
Oral Presentations/discussions (if required) August 12 – 16, 2019
Anticipated Award Decision September 20, 2019

1.5 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received in the Division of Medical Services by the date and time indicated in the Schedule of Activities.

Proposals received after the deadline will be late and ineligible for consideration.
An original, 6 identical copies, and one (1) digital, Portable Document Format (PDF) copy loaded on a USB flash drive of the Technical proposal, including all attachments.

An original paper copy, and one (1) digital Portable Document Format (PDF) copy of the Cost proposal must also be submitted in a separate sealed envelope and clearly labeled Contractor Name and “Cost Proposal RFP #1710.”

All proposals must be signed in ink by an officer of the responder legally authorized to bind the responder to the proposal, and sealed in the form intended by the respondent. Proposals that are not properly signed may be rejected. The sealed envelope must be marked with the appropriate RFP Number and Title. The words “Sealed Proposal Enclosed” must be prominently denoted on the outside of the shipping container. Proposals must be addressed and labeled as follows:

Request For Proposal #1710 Proposal Due July 9, 2019  
South Dakota Department of Social Services  
Division of Medical Services  
Attention: Dawson Lewis  
700 Governors Drive  
Pierre SD 57501-2291

No punctuation is used in the address. The above address as displayed must be the only information in the address field.

No proposal may be accepted from, or any contract or purchase order awarded to any person, firm or corporation that is in arrears upon any obligations to the State of South Dakota, or that otherwise may be deemed irresponsible or unreliable by the State of South Dakota.

1.6 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION – LOWER TIER COVERED TRANSACTIONS

By signing and submitting this proposal, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation, by any Federal department or agency, from transactions involving the use of Federal funds. Where the offeror is unable to certify to any of the statements in this certification, the bidder must attach an explanation to their offer.

1.7 NON-DISCRIMINATION STATEMENT

The State of South Dakota requires that all contractors, vendors, and suppliers doing business with any State agency, department, or institution, provide a statement of non-discrimination. By signing and submitting their proposal, the offeror certifies they do not discriminate in their employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.8 MODIFICATION OR WITHDRAWAL OF PROPOSALS

Proposals may be modified or withdrawn by the offeror prior to the established due date and time. No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered.

1.9 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after May 21, 2019. Email inquiries must be sent to Dawson Lewis at Dawson.Lewis@state.sd.us with the following wording, exactly as written, in the subject line: RFP #1710 Questions. Questions must be submitted in the question format provided in Attachment A and can be sent any time after RFP release through the cutoff date for questions.
The Department of Social Services (DSS) will respond to offerors’ inquiries by posting offeror aggregated questions and Department responses on the DSS website at http://dss.sd.gov/keyresources/rfp.aspx no later than June 4, 2019. For expediency, DSS may combine similar questions. Offerors may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.10 PROPRIETARY INFORMATION

The proposal of the successful offeror(s) becomes public information. Proprietary information can be protected under limited circumstances such as client lists and non-public financial statements. Pricing and service elements are not considered proprietary. An entire proposal may not be marked as proprietary. Offerors must clearly identify in the Executive Summary and mark in the body of the proposal any specific proprietary information they are requesting to be protected. The Executive Summary must contain specific justification explaining why the information is to be protected. Proposals may be reviewed and evaluated by any person at the discretion of the State. All materials submitted become the property of the State of South Dakota and may be returned only at the State's option.

1.11 LENGTH OF CONTRACT

The State is looking for the implementation of the System with the Division of Medical Services within twelve (12) months of contract execution. If the State determines that any other programs will be added to the initial system deployment, the State and Contractor will agree on a planned implementation schedule and, if applicable, an adjusted price. The maintenance and operations period will begin at the end of the warranty period. The total initial contract length will be five years from contract execution, with the possibility of two 1-year options to renew. Should the State determine that it is in the best interest of the State to “takeover” the system and move it to the State for ongoing maintenance and operation by BIT, the State may entertain a mutually beneficial contract length beyond the above mentioned two, one-year renewals to accommodate knowledge transfer and transition of the system to BIT. While Contract years will generally coincide with State fiscal years (which begin on July 1), the first Contract year may be abbreviated depending on the Contract execution date. Both the initial contract and any extensions are subject to Centers for Medicare & Medicaid Services (CMS) review and approval.

1.12 GOVERNING LAW

Venue for any and all legal action regarding or arising out of the transaction covered herein shall be solely in Hughes County, State of South Dakota. The laws of South Dakota shall govern this transaction.

1.13 DISCUSSIONS WITH OFFERORS (ORAL PRESENTATION/NEGOTIATIONS)

An oral presentation by an offeror to clarify a proposal may be required at the sole discretion of the State. However, the State may award a contract based on the initial proposals received without discussion with the offeror. If oral presentations are required, they will be scheduled after the submission of proposals. Oral presentations will be made at the offeror’s expense.

This process is a Request for Proposal/Competitive Negotiation process. Each Proposal shall be evaluated, and each respondent shall be available for negotiation meetings at the State's request. The State reserves the right to negotiate on any and/or all components of every proposal submitted. From the time the proposals are submitted until the formal award of a contract, each proposal is considered a working document and as such, will be kept confidential. The negotiation discussions will also be held as confidential until such time as the award is completed.

2.0 STANDARD AGREEMENT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include, at minimum, the State’s standard terms and conditions as seen in Attachment F DSS Consultant Contract. As part of the negotiation process, the contract terms listed in Attachment F may be altered or deleted. The Offeror shall indicate in their response any issues they have with any specific contract terms. If the Offeror does not indicate any contract term issues, then the State will assume the terms
are acceptable. Depending on the hosting option the Offeror bids, some provisions included in the BIT Information Technology Clauses of the Consultant Contract may not apply. The successful Contractor will also be required to sign Attachment G – Business Associate Agreement (BAA). Finally, the selected Contractor must comply and agree to the Federal requirements contained in Attachment H and must acknowledge in their proposal that they understand and will abide by all applicable Federal regulations including those contained therein.

3.0 BACKGROUND

3.1 CURRENT STATE BUSINESS ENVIRONMENT

South Dakota’s Medicaid and CHIP programs are based on a traditional fee-for-service (FFS) delivery model. As such State staff are the primary reviewers of prior authorization and medical necessity determinations, although the State contracts with the South Dakota Foundation for Medical Care (SDFMC) for the secondary review of certain PA requests. Within the Division of Medical Services (DMS), the Prior Authorization Unit (PA Unit) accepts, processes and adjudicates approximately 500 to 700 prior authorization requests per month. These PA requests are for select medical and behavioral health services covered by the State’s Medicaid and CHIP programs; Medicaid and CHIP-covered services subject to prior authorization are listed on the following website: http://dss.sd.gov/medicaid/providers/pa/.

PA Unit staff, all of whom are Registered Nurses (RNs), review and approve prior authorization requests based on medical necessity and DMS regulations and policies. PA Unit staff are located at the DMS office in Pierre and in regional offices throughout the State.

Providers fax in PA request forms and required documentation (“PA request attachments”) to the PA Unit, which then retrieves the hard copy forms, scans the documents into an electronic (pdf) format, stores them in files in a document management system, and manually creates records with the required data elements into a homegrown system (“legacy PA system”) and into a subsystem of the State’s Medicaid Management Information System (MMIS). Upon approving or denying the request, PA Unit staff update the aforementioned records and fax a form with the resulting approval/denial to the requesting Provider. If a denied PA request is appealed, a PA Unit staff member and the DMS Medical Director attend administrative hearings to support their denial determinations.

In addition to the previously described process for select medical services that require prior authorization, the DSS Division of Behavioral Health (DBH) performs a clinical review and prior authorization determination of the following high-intensity substance use disorder (SUD) treatment services for Medicaid recipients:

- Level 3.7 intensive inpatient services for adults and for adolescents, also known as Psychiatric Residential Treatment Facility (PRTF) for substance use disorder treatment;
- Level 3.7 intensive inpatient services;
- Level 3.1 clinically-managed low intensity residential treatment for pregnant women and/or women with dependent children; and
- Specialized intensive methamphetamine treatment.

The above SUD treatment services require a clinical review completed by a Certified or Licensed Addictions Counselor using Addiction Society of American Medicine (ASAM) Criteria, 3rd Edition to ensure referrals to high intensity services meet clinical and medical necessity. Services are reviewed in accordance with the eligibility requirements found in Administrative Rule of South Dakota (ARSD) §67:61.

Operating as an extension of DBH, SDFMC is involved in reviewing requests for inpatient psychiatric admission and continued stay using InterQual criteria (but moving to MCG criteria in the future). SDFMC also reviews requests for SUD treatment for adolescents. SDFMC maintains its own information system and interfaces with DSS to obtain PA case numbers that are then entered into the SDFMC database. On an ongoing weekly basis, SDFMC sends PA status information in a file to be imported into the MMIS/claims management subsystem. DBH is required to make the determination of clinical appropriateness for high intensity SUD treatment within 1 business day, including notification to the referring entity. In FY 2017 DBH received 131 prior authorization

1 While prior authorizations for select prescription drugs are also required, those requests are handled by a contracted vendor and are not within the scope of this RFP.
requests on average per month. Each prior authorization request review takes approximately a half hour to complete.

Also within DSS, the Division of Child Protective Services (CPS) relies upon prior authorization processes to determine placements of youth who are unable to function in a family or group setting due to significant mental health challenges in psychiatric residential treatment facilities (PRTF). A two-part review process ensures that eligibility and provision of PRTF services are provided in compliance with ARSD 67:16:47. Each referral for a PRTF placement is first reviewed by a multi-agency State Review Team comprised of representatives from DSS and Departments of Corrections, Human Services and Education. The Team reviews a set of required documentation to determine if criteria have been met to justify a PRTF placement. If criteria have been met, the prior authorization request is sent on to SDFMC for further review by a clinician using InterQual criteria to verify medical necessity and authorize a length of stay. On an ongoing basis during the course of treatment in the PRTF, a progress report must be submitted in accordance with ARSD 67:42:08:07 or 67:42:15:11 and is used by SDFMC to evaluate requests for continued stay; those requests are submitted directly to SDFMC for review and adjudication.

3.2 CURRENT STATE TECHNICAL ENVIRONMENT

At present, for tracking PA requests and recording the disposition of said requests the PA Unit utilizes a Microsoft Access-based system built by the state’s Bureau of Information and Telecommunications (BIT); this system is hereafter referred to as the “legacy PA system”. This system is accessed via a network shared drive maintained by BIT; legacy PA system users within the PA Unit have distinct network and system account IDs and passwords. The functionality of the legacy PA system is limited – it serves mainly as a tool for recording activities related to the processing of PA requests.

The legacy PA system is not interfaced to the subsystem within the state’s mainframe-based Medicaid Management Information System (MMIS) that handles claim intake, processing and disposition. For each approved PA request a PA Unit staff member manually creates a PA record in the MMIS; the PA record has a unique control number. As part of the claim processing job stream, the PA record is matched to a claim submitted with that same PA control number.

Documents associated with the processing of a PA request are not stored in the legacy PA system. The PA Unit uses File Director, the document management system used by various South Dakota state government agencies and maintained by BIT, for storing and cataloging documents associated with a PA transaction. For each PA transaction a designated PA Unit resource creates a PA file with a unique ID in File Director; documents associated with that particular PA request are scanned and stored in that file. File Director is also used on a limited basis as a workflow management system; some PA requests are routed via File Director to PA Unit staff members. File Director is not interfaced to the legacy PA system or the state’s MMIS.

3.3 DESIRED FUTURE STATE BUSINESS AND TECHNICAL ENVIRONMENT

DSS is pursuing a clear vision and pathway for modernizing its information infrastructure in order to streamline the operations of its public programs, improve services for recipients and achieve greater cost effectiveness. As a first priority, the new Prior Authorization, Utilization Management, and Care Management system (“System”) will support critical areas of operation within the Division of Medical Services related to prior authorization, and significantly improve current manual processes. The System is also expected to support DSS with additional utilization and care management functions related to the administration of Medicaid benefits and services and payment of claims. Subsequently, system supports will extend to other agency divisions and programs not directly related to Medicaid claims administration. The following definitions highlight key functions referred to and further described throughout this RFP.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description/Scope of Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilization Management</td>
<td>A broad category of activities focused on ensuring the provision of medically necessary services. Activities include review of individual cases i.e., prior authorization, concurrent review, discharge planning, and referrals to care management for high complexity/high cost cases. UM also includes identifying and</td>
</tr>
<tr>
<td>Module</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>improving utilization patterns through monitoring, analytics and reporting activities (see definition below). UM supports include alerts and notifications regarding utilization of services that are outside of set parameters and cases that warrant referrals for care management services and/or retrospective review.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Provider Access</strong></td>
<td>A streamlined, secure, single point of access for providers to obtain: information about PA/UM/CM policies and procedures including services that do and do not require authorization; appropriate forms required to submit various types of authorization requests; real time information about the status of PA requests and place to initiate appeals.</td>
</tr>
<tr>
<td><strong>Recipient Access</strong></td>
<td>A streamlined, secure, single point of access for Recipients to obtain: information about PA/UM/CM policies and procedures including services that do and do not require authorization; ability to see real time status of PA requests; source of appropriate information and place to initiate request for reconsideration/follow up on adverse PA determinations.</td>
</tr>
<tr>
<td><strong>PA Request Intake</strong></td>
<td>Receiving, importing, and determining whether requests are legitimate (eligible providers, recipients, and services) then making requests available for prior authorization determinations relative to treatment, services and program participation, in accordance with administrative rules and agency policies and procedures. Requests will come from various sources including: in and out of state providers; providers that are or are not currently registered as Medicaid providers; individuals within internal agencies and divisions; contractors; and Recipients.</td>
</tr>
<tr>
<td><strong>PA Request Review and Determination</strong></td>
<td>Functionality that supports processing and adjudication of requests to authorize services in accordance with the state’s rules, policies and timelines with accommodation for levels of review that include auto adjudication by the System and additional levels of review by designated internal and external reviewers.</td>
</tr>
<tr>
<td><strong>Care Management Referrals and Supports</strong></td>
<td>Functionality that enables authorized System users to identify and refer individual recipients with high complexity and/or costs for more intensive care monitoring and care coordination. Includes configurable decision supports that proactively identify recipients as candidates for care management through monitoring of utilization data. Provides the ability to flag cases for incremental review during the course of care management.</td>
</tr>
<tr>
<td><strong>Notifications</strong></td>
<td>Ability to generate notices and other types of communications as part of prior authorization, utilization management and care management processes. The communications will be designed to notify the applicable parties about service utilization, service limits, the status and outcome of authorization requests and reconsiderations and other in-scope transactions in accordance with the state’s administrative rules. Communications will incorporate pre-configured, standardized content as well as content customized by authorized users with specific data and text.</td>
</tr>
<tr>
<td><strong>Appeals and Grievance Management</strong></td>
<td>Functionality including notifications (see above definition) and supports for staff involved in adjudicating appeals and grievances by providing access to required background information available in the System, MMIS and other relevant attachments.</td>
</tr>
<tr>
<td><strong>Electronic Document Management</strong></td>
<td>Functionality that enables accurate, secure and retrievable documents related to the gamut of PA, UM and Care Management processes in accordance with the state’s administrative rules and policies. Includes appropriately identifying, indexing, storing and providing access to all forms, documents, and recipient-specific determinations.</td>
</tr>
<tr>
<td><strong>Workflow Management</strong></td>
<td>Functionality that streamlines PA, UM and CM processes and enables optimized workforce productivity and use. Includes configuration and support of workload queues and selective automation that enables routing of various types of requests to designated authorized System users or otherwise to available users in order to balance workload. Functionality includes the ability to conduct real time monitoring of the status of reviewer workloads and related transactions, generation of management reports that track individual and aggregate productivity metrics.</td>
</tr>
<tr>
<td><strong>Monitoring, Analytics and Reporting</strong></td>
<td>Analytic capabilities that enable authorized users to monitor and analyze the utilization of type of services by individual and population, including by agency,</td>
</tr>
</tbody>
</table>
division and/or program, as well as performance and program metrics related to PA, UM and CM processes. Ability to configure and generate routine and ad hoc reports on real-time and pre-scheduled bases. This includes the ability to conduct real time monitoring of the status of reviewer workloads and related transactions and generation of management reports that track individual and aggregate productivity metrics.

Detailed system requirements associated with these functions are provided in Attachment B – Functional Requirements.

- The System will be used by Providers, internal agency/department staff (e.g. the PA Unit) and select contractors (e.g. the South Dakota Foundation for Medical Care), and Medicaid recipients.
- Furthermore, the System will enable optimized work flows, improved access to data, more powerful analytics, and the ability for Providers, DSS and recipients to interact more efficiently and effectively.
- Finally, the System will be interfaced to the MMIS so that duplicate PA transaction records are not required. As part of the aforementioned MES Modernization Program, the State plans to modernize/replace various MMIS subsystems including the claims management "module". Thus, vendors must propose solutions that can interoperate with legacy and future MMIS subsystems/modules.

To further articulate expectations for the System, DMS developed use cases to illustrate common scenarios for how the System will be used to carry out required business processes; refer to Attachment D – Use Cases. All systems proposed in response to this RFP must be able to support these use cases; moreover, in State-organized Oral Presentations and Demonstrations invited vendors may be asked to demonstrate how their proposed systems support these use cases. It is not the intent of the State for Contractors to specifically respond to the use cases as part of the technical proposal.

All of the above notwithstanding,

- These use cases are illustrative and do not encompass all of the detailed System requirements. They are to be considered along with the detailed functional and technical requirements matrices attached to the RFP. These constitute a more complete list of desired system functionality and reflect agency input into what they desire from the System solution.
- The focus of these use cases is to highlight critical functionality that will be required for information capture, information sharing and collaboration within and across programs related to the provision of services supported by each agency.
- A deeper dive into specific program workflows is expected to occur after a Contractor is selected, as part of Requirements Validation and Configuration, Customization and Integration activities.

Additionally, DMS developed a conceptual, future state, high-level workflow to illustrate how a solution might facilitate prior authorization requests and link to related utilization management and care management functions. Refer to Attachment E – Future State Workflow.

### 3.4 ABOUT THE BUREAU OF INFORMATION AND TELECOMMUNICATIONS (BIT)

The Bureau of Information and Telecommunications (BIT) is responsible for providing select information technology (IT) services to DSS and other State departments and agencies. BIT manages all information technology services (hardware, software, network infrastructure, application development for State-supported systems, etc.). BIT is responsible for operating, maintaining and managing the legacy PA system, the MMIS, and a majority of the DSS programs. BIT will support the successful Vendor in the data conversion and interface configuration activities. The Vendor will be required to complete, sign, and submit the BIT Security Acknowledgement (Attachment F Exhibit A) and the BIT Technical and Security Questionnaire (Attachment I) before the contract is executed.

### 4.0 SCOPE OF WORK

This RFP has the following mandatory scope of work components that all vendors must address in their responses:
1. Provision of a system that meets functional requirements;
2. Provision of implementation services for the proposed system; and
3. Maintenance and Support Services after the system has been implemented.

Additionally, vendors have the option of addressing a fourth scope of work component, if applicable based on its proposal:

4. Operations and Hosting Services for the implemented system.

4.1 PROVISION OF SYSTEM

The State prefers a System that is currently operational and has been certified by CMS as a part of an MMIS solution OR is in the process of being certified. The State is NOT interested in a solution that has significant development required for Phase I of the project. The State understands and expects that there will be development work related to data conversion, interfaces and ensuring the system meets South Dakota specific requirements. There is an expectation that a majority of the system can be configured to meet the South Dakota requirements and will not require extensive programming or development.

4.1.1 TYPES OF BIDS

While the State prefers solution hosted on the Contractor’s infrastructure or cloud vendor, each prospective Contractor shall indicate which option they are proposing and why they believe it is most advantageous to the State. The State expects only one proposal per prospective Contractor or team of prospective Contractors and will not accept multiple proposals from one prospective Contractor or team of prospective Contractors. Each prospective Contractor shall submit bid(s) reflecting the bid option(s) that the prospective Contractor believes are likely to be the most advantageous to the State:

- Contractor hosts an existing solution on the Contractor’s infrastructure;
- Contractor hosts an existing solution on a cloud vendor solution;
- Contractor works with existing state client to allow the State to use that state’s infrastructure and system;
- Supported by the Contractor and hosted at the State or in a cloud tenant location of the State’s choosing and which the State manages and/or controls.

Depending on the hosting option the Contractor bids, some provisions included in the BIT Information Technology Clauses of the Consultant Contract may not apply.

4.2 IMPLEMENTATION SERVICES

The Contractor will perform and take responsibility for all functions, services, tasks, steps, activities and responsibilities required to implement the System and render it fully operational including configuring the System, converting, transforming, formatting and migrating active case data and one year of historical data, testing and the like (the “Services”). The Contractor shall manage the project in accordance with industry standard, accepted project management principles outlined in the Project Management Body of Knowledge (PMBOK) from the Project Management Institute (PMI), or acceptable equivalent. The Contractor shall provide the Services in accordance with the Master Project Plan and Master Project Schedule developed by the Contractor during the Project Management & Planning Phase and agreed to by the State. The System is subject to Acceptance and will not be elevated into production prior to Acceptance following completion of the Implementation Activities and Tasks. The Contractor shall perform the Implementation Activities and Tasks during the period beginning on the date the Agreement is executed and ending on the day the State provides its Acceptance of the System following the Warranty period. The Contractor shall provide the State contact information for, and direct access to, all personnel providing any of the Implementation Activities and Tasks.

System implementation will proceed in phases as noted below:
• **Phase 1**: During this Phase, the Contractor will complete the Implementation Activities and Tasks with respect to all functional and technical requirements supporting the Division of Medical Services recipient requests that rely on current Medicaid claims and PA systems.

• **Phase 2**: During this Phase, the Contractor will complete the applicable Implementation Activities and Tasks required to configure interfaces and enable access and workflow that allows shared case management of Medicaid recipients with the Division of Behavioral Health, Child Protective Services, the South Dakota Foundation for Medical Care, and the Department of Human Services.

### 4.2.1 MINIMUM CONTRACTOR RESPONSIBILITIES

- Produce all deliverables within the timeframe specified in the Schedule of Milestones and Deliverables and based on the approved Detailed Work Plan attached to the contract
- Conduct Requirements Validation sessions involving State stakeholders to validate and provide a detailed description of specific requirements and design elements to be incorporated into the System
- Document and distribute RV session requirements, notes and minutes
- Provide complete traceability of requirements through design, test scripts and training
- Schedule and facilitate walkthroughs/review sessions to gather State feedback as needed
- Develop the system according to requirements
- Participate in the Change Control Board process
- Support the CMS Stage Gate Review Process
- Perform all testing as defined in Section 4.2.7.6
- Support the State in the completion of User Acceptance Testing
- Review all identified State systems, develop conversion strategy as defined in Section 4.2.7.5 and work with the State to execute the conversion strategy
- Train State staff as defined in Section 4.2.7.7
- Participate in and perform all required tasks and activities related to final pre-implementation tasks (Go/No Go checkpoints)

### 4.2.2 MINIMUM STATE RESPONSIBILITIES

- Provide a team that includes Subject Matter Experts (SME) on the business requirements, design, development, testing, training and implementation of the System
- Participate in Requirements Validation sessions and data conversion sessions to assist the Contractor in understanding the requirements for each business function
- Review, provide comments and accept or reject all deliverables
- Establish a Change Control Board
- Establish a Data Governance Group to advise and guide the project team through the data governance issues
- Establish a Governance Council to serve as a leadership stakeholder group to meet on a periodic basis to receive project status and pave way through project issues and risks
- Conduct User Acceptance Testing
- Attend deliverable walkthroughs to enhance understanding and facilitate the approval process

### 4.2.3 DEVELOPMENT LIFE CYCLE

Throughout the SDLC, the Contractor shall map their schedule and artifacts to the CMS Enterprise Lifecycle guidance, and the Medicaid Enterprise Certification Lifecycle (MECL) framework in alignment with the MECL Toolkit and prepare for and participate in meetings required by the State including with governmental authorities including CMS. Unless otherwise directed by the State, these meetings may be attended by conference calls or webinar and do not necessitate all parties to be available in person.
4.2.4  **SYSTEM CERTIFICATION**

The Contractor shall lead the efforts and provide the State assistance with respect to the State’s effort to pass each of the CMS Stage Gate Reviews contained in the MECL. The Contractor shall complete certification checklists, provide all documents required for the Stage Gate Review process (“Stage Gate Deliverables”), and map documents to the certification checklists. The Contractor shall supply all such documentation at least 10 business days prior to the deadline for the State to submit materials to the State Project Leader and then to IV&V Vendor or CMS in advance of the scheduled review.

4.2.5  **DELIVERABLE REVIEW PROCESS.**

Deliverables will be submitted by the Contractor and accepted or rejected by the State per the Deliverable Review Process. The process shall include the use of a Deliverables Expectations Document (DED) and a Deliverable Acceptance Form.

All proposed deliverables shall be included in the Detailed Work Plan and delivered in accordance with the Project Management Plan. The Detailed Work Plan must have tasks delineating the deliverable date. During the life of the contract, the State may, with proper notification to the Contractor, add or subtract deliverables and / or adjust the contents of deliverables as necessary.

All deliverables submitted to the State must have, at a minimum, a cover letter outlining contents for delivery and a copy of the deliverables in electronic form, unless directed otherwise by the State Project Leader and Project Manager.

The State Project Leader and Project Manager will coordinate, manage, and monitor the review and comments by State staff and the IV&V consultant, if needed, and will convene, as necessary, a review panel to review the deliverable. The State Project Leader may also request a walkthrough of any deliverable submitted by the Contractor.

The State shall have at least ten (10) business days (or such other time period identified in the Contractor’s Work Plan as approved in writing by the State) to review each deliverable after the receipt date. Additional review time may be required at the discretion of the State Project Leader. If the deliverable is determined to be in need of modification, the State Project Leader must send written notification to the Contractor outlining the issues. The Contractor must make the corrections within five (5) business days (or such other time period approved in writing by the State) and resubmit the deliverable to the State Project Leader for final review at which time the State has at least five (5) business days (or such other time period identified in the Contractor’s Work Plan as approved in writing by the State) to review. Reviews of resubmitted deliverables will focus on the revision, plus related regression content, and be performed by the same State staff. This five (5) day cycle will continue until the State accepts the deliverable. Upon approval, an acceptance letter, signed by DCH, will be submitted to the Contractor.

4.2.6  **STAFFING**

The Contractor shall provide the following Key Staff during all Implementation Phases and meet the Key Staff Qualifications described in Attachment C – Technical and Contractor Scope of Work Requirements:

- Project Executive
- Project Manager
- Solution Architect
- Data Manager
- Interface Manager
- Testing Manager
- Security Manager
- Knowledge Transfer and Training Manager
The Contractor shall adhere to the following general requirements for Key Staff as well as the detailed requirements described in Attachment C – Technical and Contractor Scope of Work Requirements:

- The Contractor shall have selected a Project Executive and have that individual under the contractor’s employ at the time the proposal is submitted
- The Contractor must employ all Key Staff or must have a written, legally binding commitment from them to join the Contractor’s organization by the beginning of the contract start date
- The Contractor must commit Key Staff named in the proposal to the project from the contract signing date and may not reassign Key Staff during the project, except in cases of resignation or termination, or unless the State has agreed in advance
- The Contractor must make Key Staff available after hours as required by the State
- The Contractor must ensure Key Staff are available as mutually agreed upon during applicable project phases

Additionally, The Contractor shall develop and maintain compliance with the Project Staffing Plan accepted as a part of the Project Management and Communication Plan deliverable. The plan, at minimum, shall:

- Describe the overall project organization structure and how the project team is integrated with the overall contractor organization
- Include job titles and job functions, roles and responsibilities of the Key Staff, and staffing levels
- Disclose the planned use of another company or individual consultant with which the contractor will contract to perform the services described in this RFP
- Include a resource calendar describing the staff required for each phase of the project, if the staff will be on or off-site and the allocation percent
- Provide a communication plan for managing secure communications between onsite and offsite staff
- Describe the expected interaction between contractor teams and State staff
- Describe retention strategies and plans to minimize the impact of personnel changes throughout the life of the contract

4.2.7 ACTIVITIES, TASKS, & DELIVERABLES

This section of the scope of work describes the objectives, descriptions, and expected outcomes of each project lifecycle activity. The State expects Contractor deliverables to be the result of the completion of all activities and tasks even when they are not explicitly identified as individual deliverables in this contract. The State reserves the right to verify and validate selected activities independently. When a determination is made that deliverables are being produced without conformance to the underlying principles defined below, the State may consider the level of risk in the delivery to be unacceptable until the Contractor has demonstrated that these activity principles have been incorporated into the Contractor’s delivery system.

Refer to Attachment C – Technical and Contractor scope of Work Requirements for detailed requirements related to the Scope of Work Activities.

<table>
<thead>
<tr>
<th>No.</th>
<th>Activity</th>
<th>Tasks and Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Project Initiation and Planning</td>
<td>1.1: Project Kickoff, Protocol and Materials Package</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2: Detailed Work Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.3: Project Management and Communications Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.4: Risk Management Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.5: Project Documentation and Collaboration Portal Design</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.6: Issue Management Plan</td>
</tr>
<tr>
<td>No.</td>
<td>Activity</td>
<td>Tasks and Deliverables</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>Project Reporting</td>
<td>2.1: Project Status Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.2: Decision Management Plan</td>
</tr>
<tr>
<td>3</td>
<td>Requirements Validation</td>
<td>3.1: Requirement Elaboration and Specification Definition Protocol and Materials Package</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.2: Functional Specification Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.3: Requirements Traceability Matrix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.4: Data Integration/Interface Specifications Documents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.5: Deployment Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.6: Security and Privacy Plan</td>
</tr>
<tr>
<td>4</td>
<td>Configuration, Customization and Integration</td>
<td>4.1: Configuration Management Plan</td>
</tr>
<tr>
<td>5</td>
<td>Data Conversion and Migration</td>
<td>5.1: Data Conversion and Migration Plan</td>
</tr>
<tr>
<td>6</td>
<td>Testing</td>
<td>6.1: Test Plan including Test Scenarios, Test Cases and Test Scripts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.2: Solution Test Results</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.3 User Acceptance Testing Readiness Report</td>
</tr>
<tr>
<td>7</td>
<td>Knowledge Transfer and Training</td>
<td>7.1: Knowledge Transfer and Training Plans</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.2: Training Materials Package</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.3: End-User Manuals and Quick Reference Guides</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.4: Solution Technical Documentation</td>
</tr>
<tr>
<td>8</td>
<td>Deployment: Cutover and Acceptance</td>
<td>8.1: Cutover and Acceptance Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.2: Incident and Defect Resolution Log and Report</td>
</tr>
<tr>
<td>9</td>
<td>Implementation Closeout</td>
<td>9.1: Closeout Report</td>
</tr>
<tr>
<td>10</td>
<td>Solution Maintenance and Support</td>
<td>10.1: Solution Maintenance and Support Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.2: Maintenance and Support Activity Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.3: Incident Reports – Solution Maintenance</td>
</tr>
<tr>
<td>11</td>
<td>Solution Operations and Hosting</td>
<td>11.1: Solution Operations and Hosting Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11.2: Incident Reports – Operations and Hosting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11.3: Availability and Performance Reports</td>
</tr>
<tr>
<td>12</td>
<td>Project Turnover</td>
<td>12.1: Turnover Plan</td>
</tr>
</tbody>
</table>

**4.2.7.1 PROJECT INITIATION AND PLANNING**

**Description**
The Contractor will have a repeatable, tested approach for kicking off the implementation of the System project. The aim of Project Initiation is to ensure that the State and relevant stakeholders understand and approve of the Contractor’s approach to implementation, communications, documentation review and issue management throughout the lifespan of the project. On a mutually agreed upon date, The Contractor will schedule and conduct a project kickoff. Project Initiation will include the following deliverables.

**Deliverables**

1.1 *Project Kickoff Protocol and Materials Package* – By a mutually agreed upon date, the Contractor will provide a documented protocol for project initiation, and a package of materials that, once customized, would be used in meetings, presentations and other project kickoff activities.

1.2 *Detailed Work Plan* - By a mutually agreed upon date, the Contractor will produce a baseline Detailed Work Plan. The Contractor’s Detailed Work Plan will demonstrate that the Contractor has a thorough understanding of the Scope of Work and what must be done to satisfy the project requirements. The Detailed Work Plan must include detail sufficient to give the State an understanding of how the Contractor intends to:

- Manage the work;
- Guide work execution;
- Utilize Contractor resources for certain project activities;
- Rely on County resources for certain project activities;
- Document assumptions and decisions;
- Facilitate communication among stakeholders; and
- Define key management review as to content, scope, and schedule.

The Contractor’s Detailed Work Plan shall be constructed in accordance with industry standards, accepted project management principles outlined in the Project Management Body of Knowledge (PMBOK) from the Project Management Institute (PMI), or acceptable equivalent. Additional criteria for the Detailed Work Plan are reflected in the following:

- The Detailed Plan shall include, at a minimum: a three-level work breakdown structure; project milestones; and deliverables.
- For this project, it will be crucial to coordinate activities and resources with pertinent State staff. Thus, in its Detailed Work Plan the Contractor must clearly specify deliverables and dates that require BIT staff involvement for technical setup and project environments and the involvement of DMS staff in implementation activities.
- The Contractor must build, produce and maintain the Detailed Work Plan in Microsoft Project or comparable project management system approved by the State. The State shall have access to the MS Project plan at all times.

1.3 *Project Management and Communications Plan* - By a mutually agreed upon date, the Contractor, with input from State staff, will produce a mutually agreeable Project Management and Communications Plan that defines how the project will be executed, monitored, and controlled as well as how various project stakeholders will be engaged throughout the life of the project to ensure all impacted parties are aware of project progress and are consulted as needed. The plan will include the proposed project management methodology, milestone schedule, staffing plan and organizational chart. Included will be:

- A list of deliverables and milestones, describing exactly what will be provided to meet those deliverables
- Metrics used to determine when deliverables have been met
- Project schedule associated with each deliverable

The Contractor is expected to participate in regularly scheduled on-site project management meetings and provide weekly status reports.
1.4 **Risk Management Plan** – By a mutually agreed upon date, the Contractor will produce a Risk Management Plan. The Risk Management Plan must be a forward-looking plan that describes:

- How the Contractor has already identified – based on prior experience and organizational experience - and will, during the course of the implementation, identify issues that could affect the achievement of project objectives;
- How the Contractor will systematically assess and rank the risk associated with these issues;
- How the Contractor is already pursuing or would rapidly develop and implement mitigation strategies that effectively address the risks associated with the aforementioned issues; and
- The tools the Contractor will use for tracking internal (Contractor) and external (State) issues and related risks, including both technical and non-technical issues that could affect the project deliverables, schedule and/or budget.

The State expects that, at a minimum, the plan will contain the following:

- Risk Management Approach - This section of the Risk Management Plan should provide a general description for the approach the Contractor will take to identify and manage the risks associated with the project.
- Risk Identification - This section of the Risk Management Plan should explain the process by which the risks associated with the System will be identified. It should describe the method(s) for how the Contractor identifies the risks, the format in which risks are recorded, and the forum in which this process will be conducted.
- Risk Qualification and Prioritization - This section of the Risk Management Plan should describe the Contractor’s approach to determining the probability and impact of each risk in order to allow the project manager to prioritize the risk avoidance and mitigation strategy. This is usually done with a risk matrix. This section should also explain how risks will be qualified and prioritized for this project.
- Risk Monitoring - This section of the Risk Management Plan should discuss how the risks in the project will be actively monitored ensuring that it is continuous throughout the life of the project and includes the identification of trigger conditions for each risk and thorough documentation of the process.
- Risk Mitigation and Avoidance - Once risks have been qualified, determination must be made on how to address those risks which have the greatest potential probability and impact on the project. This section of the Risk Management Plan should explain the considerations which must be made and the options available to the project manager in managing these risks.

1.5 **Project Documentation and Collaboration Portal Design** - By a mutually agreed upon date, the Contractor will produce a Project Documentation and Collaboration Portal Design document.

The Contractor’s Project Documentation and Collaboration Portal Design document must describe the environment which the Contractor would set up to manage the flow of project-related documents and information and to facilitate collaboration among project team members.

1.6 **Issue Management Plan** - The Issue Management Plan describes the Contractor’s process for problem management including: problem logging, problem resolution, tracking of unresolved problems, problem escalation procedures, and problem closeout and reporting practices. The plan should describe the integration of problem management across sub-contractors, if applicable, such as the use of an automated system. The plan shall include at a minimum:

- Issue management policies describing the guidelines under which issue management is to be performed
- Issue management process to be implemented
- Issue categories and profiles
- Issue analysis to include impact
- Monitoring
- Monthly reviews with the State
1.7 Organizational Change Management Plan - By a mutually agreed upon date, the Contractor will produce an Organizational Change Management Plan to include protocol, staffing, and method of communicating changes.

4.2.7.2 PROJECT REPORTING

Description

The Project Reporting activity monitors and communicates the status of the project and ensures that the project performs according to plans and schedules, within budget, and in compliance with the requirements of this RFP. As a result of the successful implementation of Project Reporting, at a minimum, the progress of the project is monitored and reported in weekly status meetings.

Deliverables

2.1 Project Status Reports - The Contractor produces the weekly Project Status Reports. At a minimum, the Project Status Report must include accomplishments, critical issues, personnel utilization, activity, tasks, defect reporting (as appropriate during the testing and validation phase) and deliverable status, budget status, and items planned for the next reporting period. It will also summarize schedule performance and budget performance to compare actual project performance with plan(s).

2.2 Decision Management Plan - The Decision Management Plan shall define and apply a practical strategy for decision-making to include issue identification, escalation process, actions to be taken, and implementation. The plan shall be organized, purposeful, accountable, and measurable. The plan shall provide a template of how the item in need of a decision will be documented. The template shall include a description of the decision to be made, stakeholders, pros and cons to each decision considered, actions, and deadlines, and shall also specify what will be the outcome and who is responsible. The plan shall also address how the decision outcomes will be maintained and traced to other decisions that have been made.

4.2.7.3 REQUIREMENTS VALIDATION

Description

Subsequent to project initiation, the Contractor will undertake Requirement Validation and specification definition activities including but not limited to design sessions/workshops with select State personnel. This work will include eliciting and documenting input from stakeholders to gain a greater understanding of user requirements and needs, demonstration of the current solution, work across teams to identify new workflows, and determine the user priorities of the system. A gap analysis may be required to determine the differences and distinctions between current functionality and proposed system features and functions, and solutions to those gaps.

The aim of Requirement Validation is to clearly outline the detailed design and configuration of the solution and identify any required customization. This task must be completed in accordance with the dates set forth in the approved Detailed Work Plan and must:

- Identify required product modifications,
- Determine interface requirements, and
- Modify the implementation plan as deemed appropriate.

The solution shall be implemented in a manner that will allow for the evolution of operations and business practices with minimal impact and rework. As a result of these activities, the implementation and deployment plans may need to be modified.

The following deliverables are relevant to this task.
Deliverables

3.1 Requirement Elaboration and Specification Definition Protocol and Materials Package - The Contractor will conduct requirement elaboration and specification definition activities in accordance with its proposed protocol. The protocol will be outlined in the Requirement Elaboration and Specification Definition Protocol and Materials Package, to be completed in accordance with the dates set forth in the approved Detailed Work Plan. The protocol must engage stakeholders in certain requirement elaboration and specification definition activities.

3.2 Functional Specification Documents – In accordance with the dates set forth in the approved Detailed Work Plan, the Contractor will develop Functional Specification Documents which it will submit to the State for review in a manner prior approved by the State. This document should be a detailed description, from a user’s perspective, of what the solution will look like and how it will behave. Functional specification documents will serve multiple purposes, including:

- Configuration and, if applicable, customization instructions to developers;
- A basis for estimating configuration/customization level of effort and work duration;
- Agreement with the State on exactly what will be built; and
- A point of synchronization for the whole project team.

The Functional Specification Documents will also be inputs to implementation and deployment plans. After functional specifications are reviewed and approved, changes to the specifications will require State approval.

3.3 Requirements Traceability Matrix - The State expects that a major deliverable of this task is a detailed functional requirements traceability matrix. The matrix will be completed in accordance with the dates set forth in the approved Detailed Work Plan. This matrix will reflect the actual configuration required to implement the system. This matrix will be used throughout the life of the project, including acceptance testing.

3.4 Data Integration/Interface Specifications Document - The Contractor will specify and document the need to exchange or accept data from other information systems and how said data will be transmitted. For each interface, the Contractor will define the interface in terms of format, content and transmission method. At a minimum, this document will include:

- The concept of operations for each interface;
- Definitions of the message structure and protocols that govern the interchange of data;
- Identification of the communication paths along which the project team expects data to flow;
- A description of the data exchange format and protocol for exchange;
- A general description of each interface;
- Assumptions where appropriate; and
- Estimated size and frequency of data exchange.

The Data Integration/Interface Specifications Document will be completed in accordance with the dates set forth in the approved Detailed Work Plan.

3.5 Deployment Plan - The Contractor will define a deployment plan for the solution. The Deployment Plan should be produced in accordance with the dates set forth in the approved Detailed Work Plan. This document should be comprised of two sections, the Deployment Strategy and the Deployment Plan. The Deployment Strategy section will be used to formulate a deployment approach for the solution and should include timeline information, a description of the deployment approach (such as waves, regular release cycle, “big bang” and direct installation vs. parallel installation), and associated benefits, assumptions and risks. The Deployment Plan section will contain schedule and resource information, the engagement and promotion strategy, deployment methods, technology infrastructure and support considerations, deployment testing and training requirement, and any known conflicts or issues with the software.
3.6 Security and Privacy Plan – The contractor will develop for State review and approval a system and operations security plan describing how the Contractor will protect the State data and how System meets all Federal and State security regulations, including HIPAA privacy and security, NIST standards, and comply with South Dakota BIT security scan requirements. The plan and resulting documentation must meet all CMS requirements prior to planned implementation date.

4.2.7.4 CONFIGURATION, CUSTOMIZATION AND INTEGRATION

Description

The Contractor shall perform solution configuration, as-needed customization and integration activities in accordance with the Detailed Work Plan and the outputs of the requirements elaboration and specifications definition task.

It is expected that, as part of this task, the Contractor will partner with BIT to develop and agree on specifications for operating hardware and software, end user hardware and software, and other information technology assets and services for which the State would be responsible.

The Contractor shall configure the solution to meet operational and performance requirements, including but not limited to setting up multiple user environments, all internal and external interfaces, and information security mechanisms. The following deliverables are relevant to this task.

Deliverables

4.1 Configuration Management Plan - A Configuration Management Plan must be developed and implemented. The plan must define the strategy for the identification, disposition, release, and control of changes to the items subject to configuration control. The plan must describe all configuration management activities and procedures, and schedule for performing, at a minimum, the following activities:

- Configuration identification. Selection and identification of a configuration item provides the basis for which product configuration is defined and verified, products and documents are labeled, changes are made, and accountability is maintained.
- Configuration status accounting. Information is recorded and reported as to when appropriate data about the configuration item should be provided. This information includes a listing of accepted configuration identification, status of proposed changes to the configuration, and the implementation status of accepted changes.
- Configuration verification and audit. Configuration verification and configuration audits ensure the composition of a project’s configuration items is correct and that corresponding changes are registered, assessed, accepted, tracked, and correctly implemented. This ensures the functional requirements defined in the configuration documentation have been met.

4.2.7.5 DATA CONVERSION AND MIGRATION

Description

As a critical part of implementing the solution, the Contractor shall perform all applicable data conversion and migration activities in conjunction with State staff.

Deliverables

5.1 Data Conversion and Migration Plan - The Contractor will be required to develop a Data Conversion and Migration Plan. The plan will be produced in accordance with the dates set forth in the approved Detailed Work Plan. The plan should outline:

- The scope of data conversion activities;
- An inventory/catalog and profile of data to be converted;
The approach to be followed for all data conversion and migration activities for the functional areas including a detailing of specific activities, their durations and applicable dependencies;
A list of applications impacted;
A list of conversion and reconciliation tools to be employed;
An outline of conversion roles and responsibilities;
A description of conversion resource requirements;
The approach to be followed for data cleanup;
The approach and methodology to data translations;
The approach to be followed for methodology for conversion testing/validation; and
An outline of acceptance criteria.

It is expected that the Contractor's approach to the completion of the following tasks will be addressed in the Data Conversion and Migration Plan:

- Ensure database backups are in place;
- Execute data conversion routines/packages;
- Validate converted data to confirm success;
- Revert to backup if conversion failed;
- Provide the State with the results of the conversion and any exceptions; and
- Work with the State to resolve nulls and non-converted data

Provide post conversion support through requested ad-hoc reporting and provision of access to the pre-and post-converted data for State confirmation analysis.

4.2.7.6 TESTING

Description
The Contractor must demonstrate through a formal, prior-approved testing process that the solution performs as required and that the system appears to meet or exceed the State's functional and technical requirements. The testing process will incorporate all levels of testing: unit/module, integration, system and end user acceptance. The Contractor and the State shall mutually develop specific written criteria for any testing that will objectively measure each functional and technical requirement. Deliverables relevant to the task of testing are listed below.

Deliverables

6.1 Test Plan including Test Scenarios, Test Cases and Test Scripts - The Contractor will submit a comprehensive Testing Plan to the State in accordance with the dates set forth in the approved Detailed Work Plan. Testing will include all software components in accordance with published functions and features, based on business scenarios and user friendliness. Interfaces will be tested based on design and business scenario. At a minimum, the test plan must incorporate unit, integration, user acceptance, performance, interface, load, fail-over and security tests. For each of the various types of tests that will need to be performed, the Testing Plan must outline the following:

- Scope;
- Objective;
- Roles and Responsibilities;
- Test Schedule;
- Test Execution Protocol/Workflow;
- Assumptions for Test Execution;
- Constraints for Test Execution;
- Test Scripts – these must be tied to functional requirements;
- Test Data Requirements;
• Test Resource Requirements;
• Expected Results;
• Acceptance Criteria (including item pass/fail criteria);
• Issue Tracking;
• Issue Reporting;
• Testing Status Reports;
• Phase Completion Reports;
• Test Final Report Sign-Off;
• Risk Mitigation;
• Testing Facilities;
• Testing Tools;
• Issue Tracking Tools;
• Issue Severity and Priority Definition;
• Issue Reporting; and
• Remediation Process.

6.2 Solution Test Results - The final acceptance test must use South Dakota approved data which adequately represent the live system and include report generation. The Contractor must test back-up/recover and failover features successfully. The failure of any specific portion of the test will require that the entire test be rerun, not just the failed portion of the test. The system is accepted only when the State Project Leader has reviewed documented Solution Test Results and certified in writing of final acceptance of the product. No warranty period shall begin until after such certification of successful user acceptance testing is issued from the State.

In addition, the Contractor shall conduct the follow testing and provide documented results:

• Performance Testing: In cooperation with the State, the Contractor shall test the Solution to endpoint workstations located within and external to the State’s data network. At its preference, the State may monitor internal bandwidth during this testing.
• Stress Testing: The Contractor shall perform stress testing in collaboration with the State to assess the solution’s performance under realistic load conditions, to determine under what conditions the solution will degrade, and to specify sufficient hardware for a full deployment. Based on an analysis of the test results, the Contractor shall recommend actions to improve performance, if necessary.
• Security Testing: The Contractor shall perform security and vulnerability testing in collaboration with State to assess the solution’s security. The cost of this evaluation shall be incorporated into the Cost Proposal. The Contractor must provide a distinct environment for testing activities. Based on an analysis of the test results, the Contractor shall recommend actions to improve security, if necessary.
• For the hosted solution, the Contractor will provide results of vulnerability scans conducted within the last year.

6.3 User Acceptance Testing Readiness Report - The Contractor will produce the UAT Readiness Report, which certifies that the solution, its domains, functions, data, processes, documentation, operational procedures, and all other associated support are in place and ready for operation. This readiness report will identify that the system is ready for each user acceptance testing (UAT) activity by the State. User documentation to support the UAT shall be available to each participant.

UAT is designed to demonstrate that the system meets requirements and performs all functions and processes correctly. This shall include operational readiness and on-going testing for maintenance, modifications, and enhancements, regardless of the number and complexity of the modifications. All system functions and interfaces shall be tested with fully converted data. Components of the test shall require that the vendor demonstrate readiness to perform all vendor system functions and contractual requirements, including manual processes.

User Acceptance Testing shall be conducted in a controlled and stable environment. No modifications to the software or files in a UAT library shall be made without prior approval from the State.
4.2.7.7 KNOWLEDGE TRANSFER AND TRAINING

Description

The Contractor shall conduct on-site knowledge transfer and training activities for State project team resources, system administrators, and State staff end users. The aim of Knowledge Transfer and Training is to ensure that State staff, including administrators and end users, have the knowledge and documentation to use and support the solution beyond implementation.

The Contractor shall discuss and reach agreement with the State on the optimal staging and provision of knowledge transfer and training activities.

The State will assist the Contractor in the scheduling of training programs. If the solution go-live date is significantly delayed due to the Contractor’s actions or faults, any repeat training sessions as determined by the State must be performed at no cost to the State.

It is expected that, as part of this task, the Contractor will bring to bear resources with organizational change management (OCM) expertise and incorporate OCM best practices and techniques into its training plan.

Deliverables

7.1 Knowledge Transfer and Training Plans - The Contractor will develop and execute, in cooperation with the State, a Knowledge Transfer and Training Plan that will be approved by the State Project Leader. The plan should be completed in accordance with the dates set forth in the approved Detailed Work Plan and shall outline separate, detailed approaches for two distinct audiences: system administrators and end users.

- For each audience, (system administrators and end-users), the Knowledge Transfer and Training Plan shall include at a minimum:
  - A recommended approach or approaches to knowledge transfer (system administrators) or training (end-users); the approaches should be designed for adult learners possessing a variety of backgrounds, experiences, and learning styles and should recommend approaches for an organization of the State’s size and complexity;
  - A recommended approach to acquired skills assessment;
  - An inventory of tasks, deliverables and resources necessary to complete the knowledge transfer or training effort, including tools and documentation necessary to support the proposed effort; and
  - For each method or course:
    - A course description;
    - The target audience (system administrator, end user or other);
    - Proposed training goals;
    - Proposed training standards;
    - The specific plan for training relevant personnel;
    - The delivery timeframe (by phase, implementation step) with a strategy for providing training early in the project to allow the training goals to be implemented throughout the project life cycle;
    - A description of training deliverables and format (i.e., online, written documentation, course materials); and
    - A description of skill sets achieved at the end of training and how training effectiveness will be measured and addressed.

The Contractor’s State-approved training schedule must be closely coordinated with State staff to coincide with the installation of the software and hardware. Upon acceptance by the State Project Leader, the Contractor shall implement the approved plan.

7.2 Training Materials Package - The Contractor will organize and/or develop materials for use in training activities. Materials should include training guides with sufficient detail to be employed by future trainers in
addition to materials for use with training participants. The State will review and approve these materials prior to their use and expects to receive final versions of training materials in hardcopy and electronic formats. All training materials must be edited to reflect the State’s specific environment, technology, and post-configured screen shots. The State will have full authority to edit/customize all Contractor provided end user and system administrator training documentation.

7.3 End-User Manuals and Quick Reference Guides – The Contractor shall be responsible for providing reference materials and takeaway documents, such as user manuals, user guides, video tutorials, or job aids to complement initial knowledge transfer and training activities and to provide follow-up reference material for trainees and future users. The State will review and approve these materials prior to their use.

7.4 Solution Technical Documentation - The State requires that the Contractor maintain and make available full documentation of the solution, including any data interfaces within the Contractor’s span of control, throughout the life of the contract.

4.2.7.8 DEPLOYMENT: CUTOVER AND ACCEPTANCE

Description

As part of implementation, a Cutover Work Group comprised of State personnel, the Contractor, and other stakeholders as deemed applicable will plan and execute the cutover. The activity will include a series of tasks that must be accomplished starting 120 days prior to the planned implementation or go-live date. As driven by and described in the Cutover and Acceptance Plan, the activity includes the delivery of implementation “checklists” to facilitate Implementation Checkpoints 120 days, 90 days, 60 days, and 30 days prior to the proposed date in the Detailed Work Plan.

Deliverables

8.1 Cutover and Acceptance Plan - The Contractor is required to provide a solution Cutover and Acceptance Plan that details the process whereby the Contractor will move the fully configured and customized products that make up the solution into production and go-live. The Cutover and Acceptance plan must be produced in accordance with the dates set forth in the approved Detailed Work Plan.

The Cutover and Acceptance Plan must address, at a minimum:

- Deployment activities;
- Sequencing of all deployment events;
- Deployment schedule;
- Implementation Checkpoints (120, 90, 60, 30 days);
- Go/No-Go Decision Point criteria;
- Incident and Defect Resolution documentation and tracking; and
- Cut-off schedule for legacy applications.

8.2 Incident and Defect Resolution Log and Report - During deployment, and through final solution acceptance, the Contractor shall maintain a document which serves as a combined log/report in which the following information is maintained:

- Recording and codification of incidents, problems with the solution that compromise its availability or performance. At a minimum the following information shall be captured for each incident: incident’s reporting origin, a description of the incident including the incident’s impact, and the codification of the incident based on potential cause(s), magnitude and resolution priority.
- Recording and codification of defects, problems with the solution that limit or otherwise adversely impact its functionality. At a minimum the following information shall be captured for each defect: defect’s
reporting origin, a description of the defect including the defect’s scope and functionality affected, and the codification of the defect based on potential cause(s), magnitude and resolution priority.

- Resolution of incidents and defects – at a minimum, the log/report shall capture, irrespective of reporting origin, interim and final measures taken by the Contractor (and, if applicable, the State) to resolve incidents and defects.
- Date/time stamps for events associated with all of the above.

### 4.2.7.9 IMPLEMENTATION CLOSEOUT

**Description**

Implementation Closeout is intended to ensure that the Contractor has completed the project work expected by the State based on the agreed-upon project scope, deliverables, schedule and budget. It also is an opportunity to share best practices and lessons learned. It is expected that the Contractor will schedule a Project Closeout meeting with the State to review the project and obtain formal approval that all services, products and deliverables have been submitted and accepted and the Implementation Phase of the project is considered complete. The Closeout Report can be used to ensure the project closeout covers all the necessary aspects of the project.

**Deliverables**

9.1 **Closeout Report** - When directed by the State, the Contractor will submit a Closeout Report that, at a minimum, will include the following information:

- Project successes;
- Project lessons learned;
- A summary of project evaluation metrics including:
  - Actual vs. planned scope
  - Actual vs. planned budget comparisons
  - Actual vs. planned schedule comparisons
  - User satisfaction with the System functionality;
  - Benefits gained over previous systems; and
  - Ongoing contingencies/remaining issues or defects.

### 4.2.7.10 COOPERATION WITH THE INDEPENDENT VERIFICATION AND VALIDATION (IV&V) VENDOR

The State is required to secure the services of an IV&V Vendor. The IV&V Vendor will monitor and report on the execution of project duties of both the Contractor and the State to CMS. The IV&V vendor will be an integral part of the CMS Medicaid Enterprise Certification Life Cycle (MECL) Gate Review process. The selected Contractor will be required to fully cooperate with the IV&V vendor in all requests for information, documentation and data. This cooperation will include support of the State, its project management vendor and IV&V vendor during the CMS Certification preparation process. The Contractor shall describe its experience with working with an IV&V vendor and how they will propose to meet IV&V vendor requirements for this project.

### 4.3 SOLUTION MAINTENANCE AND SUPPORT SERVICES

**Description**

Upon final acceptance certification, and upon termination of the warranty period, the Contractor will transition into maintenance and support mode. As part of this task, the Contractor will provide technical support and maintenance services as described in the M&S Plan.

**Deliverables**

10.1 **Solution Maintenance and Support (M&S) Plan** – The Contractor shall develop a comprehensive Solution M&S plan. At a minimum the M&S plan shall address:
• Ensuring the contractor's solution continually meets State requirements – this includes evaluation of new or revised functionality stemming from programmatic, organizational, legal or regulatory changes and related requirements elicitation and elaboration;
• Ensuring that solution maintenance windows do not interfere with State business or occur during business hours;
• Accommodating new legislation and evolving regulations, standards, and State organizational processes;
• Providing regular and periodic maintenance to the solution on a schedule agreed upon by the contractor and the State; and
• Ensuring that solution training materials, manuals and reference guides, and technical documentation are kept up-to-date throughout the life of the contract.

The M&S plan shall incorporate the following elements:

• Scope;
• Resource Roles and Responsibilities;
• Configuration Management Protocol;
• Change Management Protocol;
• Levels of Support;
• Onsite vs. Remote Support;
• Service Level Agreements; and
• Reporting and Management Protocols.

10.2 Maintenance and Support Activity Reports - The Contractor shall produce reports that detail maintenance and support activity; these reports will enable the State to gage maintenance and support activity and to identify trends in support activity that can lead to process improvement, training and other efforts aimed at reducing the activity.

10.3 Incident Reports – Solution Maintenance - The Contractor shall produce reports that detail incidents associated with solution maintenance activity, e.g. a security patch that had to be backed out and subsequently reapplied after further testing was conducted. The reports shall indicate the cause of any incidents and how the incident was resolved.

4.4 SOLUTION OPERATIONS AND HOSTING SERVICES (OPTIONAL)

Description

Upon final acceptance certification, and upon termination of the warranty period, the Contractor will transition into operations and hosting mode. As part of this task, the Contractor will operate the System solution - including but not limited to running system jobs - and host the System – including but not limited to supplying the solution’s operating environment, monitoring the environment, proactively flagging any availability and performance issues, and rapidly resolving said issues in accordance with the contract between the State and the Contractor.

Deliverables

11.1 Solution Operations and Hosting (O&H) Plan- The Contractor shall develop a comprehensive Solution O&H plan. The O&H plan must, at a minimum, incorporate the following elements:

• Scope;
• Resource Roles and Responsibilities;
• Job/Job Stream Processing Protocol;
• Availability and Performance Monitoring and Tuning Protocols;
• Availability and Performance Measures;
• Service Level Agreements; and
• Incident Reporting and Management Protocols.
11.2 Incident Reports – O&H - The Contractor shall produce reports that detail incidents associated with solution operations and hosting activity, e.g. a firmware update that had to be backed out and subsequently reapplied after further testing was conducted. The reports shall indicate the cause of any incidents and how the incident was resolved.

11.3 Availability and Performance Reports - The Contractor shall produce reports that detail availability and performance of the System as a whole and, as deemed applicable, the availability and performance of select system modules or components. Availability and performance shall be measured based on a mutually agreed upon methodology.

4.4.1 TURNOVER SERVICES

Description

If so directed by the State, the Contractor shall provide the State such assistance as the State may reasonably request with respect to: (i) the assignment of any hosting agreement to the State, if applicable; (ii) the implementation of the System on State or State designee infrastructure, if applicable; (iii) the transition of maintenance, operations and support of the System to BIT or one or more State designees. The details of such assistance shall be set forth in the Turnover Plan.

Deliverables

12.1 Turnover Plan – The Contractor shall develop a comprehensive turnover plan that documents the task and activities to be performed to efficiently transition the project from the Contractor to BIT or any other State designee. The plan should include:

- Project specifications
- Code documentation
- Assets transfer
- Development credentials
- Deployment procedures
- Any other technical information

4.5 OPTIONAL SCOPE OF WORK – PRIOR AUTHORIZATION PROFESSIONAL SERVICES

The State may be interested in optionally procuring the prior authorization professional services required to support the South Dakota Medicaid program. If engaged to support the optional prior authorization professional services scope of work, the Contractor shall have the capability of using the System and supporting one of the following service models:

- First level review for all prior authorization request conducted by a complement of qualified staff, which must include registered nurses (RNs) or licensed practical nurses (LPNs), to review and approve requests based on medical necessity and DMS regulations and policies; or
- First level review for certain PA types as defined by DMS; or
- All prior authorization requests, including support for appeals of denied requests and Medical Director review as defined by DMS regulations and policies.

The State is most interested in prior authorization professional services that can leverage the facility and telecommunication infrastructure of an existing clinical review operation. This should be reflected in the costs included for the Infrastructure/ Integration/ Implementation category of the Cost Proposal Table for the Optional Scope of Work.

Contractors shall indicate CLEARLY in the proposal whether the response includes Optional Scope of Work – Prior Authorization Professional Services. See Section 7.0 Proposal Response Format and specifically 7.2.3.2 Scope of Work Requirements.
Note: This RFP is requesting proposals to provide, implement, maintain, operate and support a functionally comprehensive, state-of-the-art, flexible, scalable and extensive information system. The response to section 4.5 will not be scored as part of the Technical or Cost Evaluation; it will be used as a consideration during the contract award process with the apparent successful prospective Contractor.

5.0 MINIMUM QUALIFICATIONS TO BID AND RESPONSE REQUIREMENTS

To bid on the project, Contractors must meet the minimum criteria set forth in this Section 5. Contractors must include in their responses facts and evidence to support their assertion that they meet, or by the time of the contract is executed will meet, the minimum qualifications.

5.1 Contractors must be a United States-based company.

5.2 Contractors must submit with its response a current risk management plan and latest risk assessment report, which shall include a HIPAA Privacy and Security risk assessment.

5.3 Contractors must have an existing solution that:

5.3.1 Is currently operational in at least three U.S. state, county or city.
5.3.2 Is currently operational in at least two health and human services agency program.
5.3.3 Supports the functional areas defined in section 3.3 Desired Future State Business and Technical Environment.
5.3.4 Meets all governmental requirements including CMS requirements.
5.3.5 Has obtained CMS certification or is currently in the certification process.

5.4 Contractors must disclose all pending or current ongoing litigation with State, county or city clients, or other private sector clients or contractors. Please list each case title, plaintiff and defendant and a paragraph summarizing the case. Please also provide the current status of the case and expected final adjudication date.

6.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

6.1 FAILURE TO SUBMIT INFORMATION

The Contractor is cautioned that it is the Contractor's sole responsibility to submit information related to the evaluation categories and that the State of South Dakota is under no obligation to solicit such information if it is not included with the proposal. The Contractor's failure to submit such information may cause an adverse impact on the evaluation of the proposal.

6.2 CONTRACTOR'S CONTACTS

Contractors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all of their questions or comments regarding the RFP, the evaluation, etc. to the point of contact of the buyer of record indicated on the first page of this RFP. Contractors and their agents may not contact any state employee other than the buyer of record regarding any of these matters during the solicitation and evaluation process. Inappropriate contacts are grounds for suspension and/or exclusion from specific procurements. Contractors and their agents who have questions regarding this matter must contact the buyer of record.

6.3 The Contractor MUST submit a copy of their most recent independently audited financial statements.

6.4 The selected Contractor will be required to provide a copy of its most recent System and Organization Controls, Statement on Standards for Attestation Engagements (SOC 1 SSAE18) report, then annually thereafter for the term of the agreement. For SOC 1 SSAE 18 the Contractor must identify which of the following can be provided on an annual basis: SOC 1, SOC 2, SOC 3, or SOC for Cybersecurity. If unable to provide a copy of the most recent report, Contractor must explain why and whether in the future the selected Contractor will be able to provide a report.
6.5  Provide the following information related to at least three previous and current service/contracts performed by the Contractor's organization which are similar to the requirements of this RFP. Provide this information for any service/contract that has been terminated, expired or not renewed in the past three years:

   a. Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted;
   b. Dates of the service/contract; and
   c. A brief, written description of the specific prior services performed and requirements thereof.

6.6  The Contractor must submit information that demonstrates their availability and familiarity with the locale in which the project(s) are to be implemented.

6.7  The Contractor must detail examples that document their ability and proven history in handling special project constraints.

6.8  If a Contractor's proposal is not accepted by the State, the proposal will not be reviewed/evaluated.

7.0  PROPOSAL RESPONSE FORMAT

7.1  An original and 6 copies must be submitted.

   7.1.1  In addition, the Contractor must submit one (1) copy of their entire proposal, including all attachments and cost proposal(s), in PDF digital format loaded on a USB flash drive. Contractors may not send the electronically formatted copy of their proposal via email.

   7.1.2  The proposal must be page numbered and must have an index and/or a table of contents referencing the appropriate page numbers. The proposal must adhere to page limit guidance for each section of the response as noted with a minimum font size of 10.

7.2  All proposals must be organized and tabbed with labels for the following headings:

   7.2.1  RFP Form. The State’s Request for Proposal form completed and signed.

   7.2.2  Executive Summary. The executive summary is to briefly describe the Contractor's proposal. This summary should highlight the major features of the proposal. It must indicate any requirements that cannot be met by the Contractor. The reader should be able to determine the essence of the proposal by reading the executive summary. Proprietary information requests must be identified in this section. (5-page limit).

   7.2.3  Detailed Response. This section should constitute the major portion of the proposal and must contain at least the following information:

      7.2.3.1  Contractor’s Assessment. A complete narrative of the Contractor's assessment and understanding of the desired solution based on the Desired Future State Business and Technical Environment and the Use Case Assumptions, of the work to be performed, the Contractor's ability and approach to performing the work including a work breakdown structure, and the resources necessary to fulfill the requirements. This section of the response should also include an understanding of challenges of and insights regarding the transition from a highly manual environment to an automated, workflow driven environment. Include an articulation of how the proposed solution meets each of the functional areas described in section 3.3 Desired Future State Business and Technical Environment. For example:

<table>
<thead>
<tr>
<th>Function</th>
<th>Using a bulleted list, indicate up to five ways in which features of your proposed solution support each function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilization Management</td>
<td></td>
</tr>
</tbody>
</table>
To support this proposal section, the Contractor must also include a system architecture and process flow diagram for the proposed solution showing connectivity to the States infrastructure.

If the Offeror is hosting the solution provide a diagram giving an overview of the proposed system. This diagram must be provided as a separate document. The file must be named “(Your Name) Hosted System Diagram”.

If the State will be hosting the solution the Offeror will provide a system diagram. The diagram must be detailed enough that the State can understand the components, the system flow, and system requirements. This diagram must be provided as a separate document. The file must be named “(Your Name) System Diagram and Requirements”. (10-page limit, excluding diagrams).

7.2.3.2 Scope of Work Requirements. A specific point-by-point response, in the order listed, to each requirement in the RFP as detailed in Sections 4. The response must identify each requirement being addressed as enumerated in the RFP. (60-page limit, excluding response to 4.5 Optional Scope of Work – Prior Authorization Professional Services)

Note: If the proposal does not include a response to the Optional Scope of Work – Prior Authorization Professional Services, the response should clearly state such. For example:

4.5 Optional Scope of Work – Prior Authorization Professional Services
This proposal does not include a response for Prior Authorization Professional Services.

7.2.3.3 Minimum Qualifications to Bid. A response to each subsection of Section 5.0, providing the requested information. Prospective Contractors must acknowledge sections that don’t explicitly ask the prospective Contractor to provide a response or discuss previous experience. (10-page limit)

7.2.3.4 Proposal Requirements and Company Qualifications. Prospective Contractors must respond to and provide all of the information requested in Section 6.0.

7.2.3.5 System Requirements. Review and respond to each of the requirements by completing and submitting Attachment B – Functional Requirements and Attachment C – Technical and Contractor Requirements as part of the response. No narrative response required.

7.2.4 Cost Proposal. Cost will be evaluated independently from the technical proposal. Contractors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.
The cost proposal must be submitted in a separate sealed envelope labeled “Cost Proposal”.

See section 9.0 for more information related to the cost proposal.

8.0 PROPOSAL EVALUATION AND AWARD PROCESS

8.1 After determining that a proposal satisfies the mandatory requirements stated in the Request for Proposal, the evaluator(s) will use subjective judgment in conducting a comparative assessment of the proposal by considering each of the following criteria listed in order of importance:

8.1.1 Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;
    8.1.1.1 Contractor's response to Contractor Assessment;
    8.1.1.2 Contractor's response to Section 4.0 Scope of Work;
8.1.2 Response to Functional and Technical Requirements;
8.1.3 Cost proposal;
8.1.4 Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;
8.1.5 Resources available to perform the work, including any specialized services, within the specified time limits for the project;
8.1.6 Proposed project management techniques;
8.1.7 Ability and proven history in handling special project constraints;
8.1.8 Availability to the project locale, and
8.1.9 Familiarity with the project locale.

8.2 Experience and reliability of the Contractor's organization are considered subjectively in the evaluation process. Therefore, the Contractor is advised to submit any information which documents successful and reliable experience in past performances, especially those performances related to the requirements of this RFP.

8.3 The qualifications of the personnel proposed by the Contractor to perform the requirements of this RFP, whether from the Contractor's organization or from a proposed subcontractor, will be subjectively evaluated. Therefore, the Contractor must submit detailed information related to the experience and qualifications, including education and training, of proposed personnel.

8.4 The State reserves the right to reject any or all proposals, waive technicalities, and make award(s) as deemed to be in the best interest of the State of South Dakota.

8.5 AWARD

The requesting agency and the highest ranked Contractor shall mutually discuss and refine the scope of services for the project and shall negotiate terms, including compensation and performance schedule.

8.5.1 If the agency and the highest ranked Contractor are unable for any reason to negotiate a contract at a compensation level that is reasonable and fair to the agency, the agency shall, either orally or in writing, terminate negotiations with the contractor. The agency may then negotiate with the next highest ranked contractor.

8.5.2 The negotiation process may continue through successive Contractors, according to agency ranking, until an agreement is reached, or the agency terminates the contracting process.

9.0 COST PROPOSAL

9.1 PROPOSAL EXPECTATIONS
The State, with support from CMS, does not expect to pay any development charges for a system that already has been developed and is operational in another state beyond those costs associated with configuration for the State’s specific requirements, data conversion and interface development.

9.2 IMPLEMENTATION, MAINTENANCE AND OPERATIONS SUBJECT TO COST PROPOSAL

The State is looking for competitive Cost Proposals for both the Implementation phase of the project and the proposed costs for ongoing Maintenance and Operations of the solution once it has been implemented. Prospective Contractors shall provide the State their most competitive pricing for both the implementation phase of the project and the ongoing maintenance and operations phase.

9.3 COST PROPOSAL WEIGHTING TO REFLECT STATE COSTS

The Cost proposal for the Implementation Cost will be weighted to reflect the estimated costs to the State. Likewise, the Maintenance and Operations bid costs will be weighted to reflect the estimated costs to the State over the life of the contract.

9.4 COST PROPOSAL POINT METHODOLOGY

The State will award the proposal with the lowest overall weighted cost, the maximum number of Cost proposal points, and then will provide a pro-rata share of points to each prospective Contractor in descending (next lowest cost) order using a standard formula of: (Prospective Contractor with Lowest Weighted Total Cost / prospective Contractor being evaluated Weighted Total Cost) X Maximum number of Cost Proposal points.

Assume, for example, that there are three hypothetical Contractor bids for the complete project:

<table>
<thead>
<tr>
<th>Prospective Contractor</th>
<th>Implementation Cost</th>
<th>M&amp;O Costs</th>
<th>Total Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contractor A</td>
<td>$200,000</td>
<td>$400,000</td>
<td>$600,000</td>
</tr>
<tr>
<td>Contractor B</td>
<td>$400,000</td>
<td>$300,000</td>
<td>$700,000</td>
</tr>
<tr>
<td>Contractor C</td>
<td>$500,000</td>
<td>$250,000</td>
<td>$750,000</td>
</tr>
</tbody>
</table>

In this example, if the Implementation Costs are weighted at 10 percent and the Maintenance and Operations Costs are weighted at 25 percent, the above “raw” bid amounts would have the following resulting weighted bid costs:

<table>
<thead>
<tr>
<th>Prospective Contractor</th>
<th>Weighted Implementation Cost</th>
<th>Weighted M&amp;O Costs</th>
<th>Weighted Total Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contractor A</td>
<td>$20,000</td>
<td>$100,000</td>
<td>$120,000</td>
</tr>
<tr>
<td>Contractor B</td>
<td>$40,000</td>
<td>$75,000</td>
<td>$115,000</td>
</tr>
<tr>
<td>Contractor C</td>
<td>$50,000</td>
<td>$62,500</td>
<td>$112,500</td>
</tr>
</tbody>
</table>

While Contractor A has the lowest total overall cost, when weights are added, Contractor C provides the best cost value to the State and is awarded the Maximum amount of Cost proposal points.

Contractor B receives the following pro-rata share of points: $112,500/$115,000 = 97.8% therefore Contractor B is awarded 98% of the Maximum Cost Proposal points.

Contractor A receives the following pro-rata share of points: $112,500/$120,000 = 93.7%; therefore, Contractor A is awarded 94% of the Maximum Cost Proposal points.

9.5 CONTRACTOR COST CLARIFICATIONS

Once submitted, prospective Contractors will not be able to make changes to their Cost Proposals, other than through Best and Final Offers (if the Contractor is selected to participate) prior to contract award unless the State
issues an amendment to the RFP with guidance and clarification for ALL prospective Contractors who submitted a cost bid to resubmit their Cost Proposals.

The State has created a series of templates for all prospective Contractors to complete to ensure that it has an “apples to apples” comparison, to the extent possible.

The State will closely scrutinize costs and may ask questions or request clarifications to prospective Contractors for any costs that appear to be anomalous. Prospective Contractors should be cautious about “front loading” or “back loading” costs to give the appearance that either the implementation costs or ongoing operations costs are skewed.

9.6 MISCELLANEOUS INFORMATION THAT MAY IMPACT PRICING

Prospective Contractors can reference Statistical Data for all programs in this RFP on the DSS website at: http://dss.sd.gov/keyresources/statistics.aspx.

All work must be done from within the United States. No offshore development or work of any kind is allowed on this project.

Prospective Contractors shall ensure that the System will include, without additional charge to the State, fully paid-up licenses for the State to use all third-party software and other products required to run the System.

9.7 INSTRUCTIONS FOR COMPLETING THE COST PROPOSAL

The Cost Proposal must provide the following information:

- A narrative response discussing how the prospective Contractor arrived at the overall costs and a declaration that the prospective Contractor is not using offshore resources;
- A narrative response describing implementation costs and cost drivers;
- A narrative response describing maintenance and operations costs and cost drivers;
- Discussion of any items or requirements that the prospective Contractor believes inflated the costs, if any;
- Assumptions the prospective Contractor used in creating the Cost Proposal. The State expects the prospective Contractors to perform the necessary research and due diligence to prepare and issue proposals that have few if any assumptions;
- A commitment that the proposed costs have been derived in good faith and are valid for up to 180 days after the State has made a decision and announced the apparent successful prospective Contractor;
- Completed detailed level costs templates for hardware, software and license fees; and
- Completed Summary level Cost Proposal Templates.

9.8 COST PROPOSAL TEMPLATE INSTRUCTIONS

- Prospective Contractors are advised that they must provide a record of all costs proposed for this Project. The Project is to be bid as a “firm fixed price” and the State contract will reflect the final, negotiated contract costs that will be or will originate from what the prospective Contractor submits as the Cost Proposal via the Cost Templates.
- The State has created a Summary Cost Proposal template that all prospective Contractors will complete to provide the State with a fair comparison of costs across all bidders. The first template breaks out cost by Implementation phase. The second template must be completed to show Maintenance and Operations costs for Phase 1 and Phase 2.
- For each row in the Summary Cost template, complete with either “N/A” for Not Applicable or provide a fixed price cost. If additional rows are needed to add other items not captured in the State’s Cost template, add them accordingly. The prospective Contractor may create an MS Excel spreadsheet to document the costs and submit that with their cost proposal narrative if they choose.
Contractors will also complete detail level cost templates documenting all Hardware, Software, and License fees. The detailed level cost templates must support the final cost presented in the Summary level cost template.

### SUMMARY COST PROPOSAL TEMPLATE - IMPLEMENTATION PHASE

<table>
<thead>
<tr>
<th>Cost Proposal Matrix</th>
<th>Phase 1 Implementation Costs</th>
<th>Phase 2 Implementation Costs</th>
<th>Elaboration / Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation Phase Category</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solution Acquisition/License Fees</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acquisition/License Fees for Other Software (specify)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirement Validation and Specifications Development</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface Development</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Conversion and Migration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge Transfer and Training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contract Deliverable Creation and Finalization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Costs (Specify)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total Costs – Implementation Phase</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### SUMMARY COST PROPOSAL TEMPLATE – MAINTENANCE AND OPERATIONS

<table>
<thead>
<tr>
<th>Maintenance and Operations</th>
<th>Year 1 (Initial 12 months)</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yearly Maintenance Fees</td>
<td>None anticipated during Implementation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yearly Operations Fees</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Annual Product Licenses Fees (where applicable)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other M&amp;O Fees (Specify)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total Costs – M&amp;O</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** The State assumes Yearly Maintenance includes all costs associated with system corrections and changes requested to the system to support the requirements within the scope of the RFP. Prospective Contractors must include a discussion of how they will manage change requests and system defect corrections within the yearly maintenance fees proposed. Costs associated with new scopes of work or the South Dakota share of costs for new Federal or State requirements will be paid via change request, agreed upon by DSS Change Control Board. Yearly Operations fees must
include those costs associated with providing ongoing services to the State as defined in 4.3 Solution Maintenance and Support Services.

**SUMMARY COSTS -- FINAL COSTS**

<table>
<thead>
<tr>
<th>South Dakota Medicaid Enterprise Prior Authorization, Utilization Management and Care Management System</th>
<th>Implementation</th>
<th>Maintenance and Operations</th>
<th>Grand Total – All Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Project Costs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SUMMARY COST PROPOSAL TEMPLATE -- OPTIONAL PRIOR AUTHORIZATION PROFESSIONAL SERVICES**

<table>
<thead>
<tr>
<th>PA Professional Services Cost Proposal Category</th>
<th>Post Implementation Contract Year 1 Cost Estimate</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical Staff Blended Rate</td>
<td>200 – 499 PAs per Month</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>500 – 700 PAs per Month</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>701 – 1000 PAs per Month</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrative Staff</td>
<td>200 – 499 PAs per Month</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>500 – 700 PAs per Month</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>701 – 1000 PAs per Month</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Staff (please specify)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure/Integration/Implementation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Costs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE: The State would accept a blend of RNs and LPNs for; not LPNs exclusively) The information included in the Cost Proposal Template - Optional Scope of Work, Prior Authorization Professional Services for the Infrastructure/Integration/Implementation category should reflect the cost associated with operationalizing the Prior Authorization Professional Services scope of work into an existing clinical review-related operation.

The Cost Proposal Optional Scope of Work Prior Authorization Professional Services Cost Table must:
- A narrative response discussing how the prospective Contractor arrived at each of the cost categories including assumptions used in determining costs;
- A declaration that the prospective Contractor would not using offshore resources;
- A narrative response describing costs and cost drivers.
10.0 ATTACHMENTS

ATTACHMENT A – RFP Questions Template
ATTACHMENT B – Functional Requirements Matrix
ATTACHMENT C – Technical and Contractor Scope of Work Requirements Matrix
ATTACHMENT D – Use Cases
ATTACHMENT E – Future State Workflow
ATTACHMENT F – South Dakota DSS Consultant Contract
ATTACHMENT G – State of South Dakota Business Associate Agreement
ATTACHMENT I – BIT Security and Vendor Questionnaire
# ATTACHMENT A – RFP Questions Template

## Instructions

Please provide all questions by populating the tab labeled "Question and Answer Template." For each question, specify the RFP document to which the question pertains and then reference the relevant section number (e.g. 3.2.4) for that document. Next, specify a general question topic. Finally, provide the detailed question.

## Note to Respondents:

All questions submitted in this Template are subject to the provisions of RFP Section 1.9 - Offeror Inquiries. All questions must be submitted to the State by the date specified in the RFP Procurement Timetable. The State reserves the right to refuse to answer any questions submitted in a different format from this Template.

## Respondent Name:

Please Complete Yellow Shaded Regions

<table>
<thead>
<tr>
<th>Question No.</th>
<th>RFP Area</th>
<th>Section</th>
<th>Question Topic</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question No.</td>
<td>RFP Area</td>
<td>Section</td>
<td>Question Topic</td>
<td>Question</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>---------</td>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question No.</td>
<td>RFP Area</td>
<td>Section</td>
<td>Question Topic</td>
<td>Question</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>---------</td>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td>54</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>68</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>69</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>74</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>76</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>77</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>79</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>82</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>83</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>84</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>85</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>86</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>87</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question No.</td>
<td>RFP Area</td>
<td>Section</td>
<td>Question Topic</td>
<td>Question</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>---------</td>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td>88</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>89</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>90</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>92</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>93</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>94</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>95</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>98</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>99</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ATTACHMENT B – Functional Requirements Matrix

Functional Requirements Instructions:
Check ("x") the box below which correspond to how the proposed solution meets a particular requirement.

For purposes of completing this exercise, the following definitions apply:
- **Configuration**: a software application’s features or behavior can be changed through the use of functionality, tools and/or utilities native to/built into the software application, i.e. without the need for custom programming/coding.
- **Customization**: a feature, extension or modification of a software application’s feature that requires custom programming/coding.
- **System**: refers to PA - UM - CM System to be acquired

Configuration to be indicated for each requirement using one of following definitions.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meets Requirement “Out of the Box” - No Configuration Needed</td>
<td>Indicates no configuration or modification or customization required by vendor/client.</td>
</tr>
<tr>
<td>Meets Requirement - Configuration Needed</td>
<td>Indicates the requirement is supported, and can be configured by the Offeror.</td>
</tr>
<tr>
<td>Only Meets Requirement via Customization</td>
<td>Indicates the functionality necessary to meet the requirement would need to be custom-built.</td>
</tr>
<tr>
<td>Does Not Provide Required Functionality</td>
<td>Indicates the functionality cannot be met by the Offeror.</td>
</tr>
</tbody>
</table>

**Functional Requirement Category Reference**

<table>
<thead>
<tr>
<th>Category</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access/ Recipient Portal</td>
<td>ARP</td>
</tr>
<tr>
<td>Access/Provider Portal</td>
<td>APP</td>
</tr>
<tr>
<td>Access</td>
<td>AC</td>
</tr>
<tr>
<td>PA Intake</td>
<td>PAIN</td>
</tr>
<tr>
<td>Referrals</td>
<td>REF</td>
</tr>
<tr>
<td>PA Request Review/ Determinations</td>
<td>REV</td>
</tr>
<tr>
<td>Utilization Management/ Care Management Referrals and Supports</td>
<td>UMCM</td>
</tr>
<tr>
<td>Notifications &amp; Correspondence</td>
<td>NC</td>
</tr>
<tr>
<td>Electronic Document Management</td>
<td>EDM</td>
</tr>
<tr>
<td>Monitoring, Analytics and Reporting</td>
<td>AR</td>
</tr>
<tr>
<td>Appeals &amp; Grievances Management</td>
<td>AG</td>
</tr>
<tr>
<td>Workflow Management</td>
<td>WF</td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>ARP</td>
<td>1</td>
</tr>
<tr>
<td>APP</td>
<td>1</td>
</tr>
<tr>
<td>ARP</td>
<td>2</td>
</tr>
<tr>
<td>APP</td>
<td>2</td>
</tr>
<tr>
<td>AC</td>
<td>1</td>
</tr>
<tr>
<td>AC</td>
<td>2</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>PAIN</td>
<td>2</td>
</tr>
<tr>
<td>PAIN</td>
<td>3</td>
</tr>
<tr>
<td>PAIN</td>
<td>4</td>
</tr>
<tr>
<td>PAIN</td>
<td>5</td>
</tr>
<tr>
<td>PAIN</td>
<td>6</td>
</tr>
<tr>
<td>PAIN</td>
<td>7</td>
</tr>
<tr>
<td>PAIN</td>
<td>8</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td>PAIN</td>
<td>9</td>
</tr>
<tr>
<td>PAIN</td>
<td>10</td>
</tr>
<tr>
<td>PAIN</td>
<td>11</td>
</tr>
<tr>
<td>PAIN</td>
<td>12</td>
</tr>
<tr>
<td>REF</td>
<td>1</td>
</tr>
<tr>
<td>REF</td>
<td>2</td>
</tr>
<tr>
<td>PA Request Review and Determinations</td>
<td></td>
</tr>
<tr>
<td>REV</td>
<td>1</td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td>REV 2</td>
<td></td>
</tr>
<tr>
<td>REV 3</td>
<td></td>
</tr>
<tr>
<td>REV 4</td>
<td></td>
</tr>
<tr>
<td>REV 5</td>
<td></td>
</tr>
<tr>
<td>REV 6</td>
<td></td>
</tr>
<tr>
<td>REV 7</td>
<td></td>
</tr>
<tr>
<td>REV 8</td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td>REV</td>
<td>9</td>
</tr>
<tr>
<td>REV</td>
<td>10</td>
</tr>
<tr>
<td>REV</td>
<td>11</td>
</tr>
<tr>
<td>REV</td>
<td>12</td>
</tr>
<tr>
<td>REV</td>
<td>13</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td>REV</td>
<td>14</td>
</tr>
<tr>
<td>REV</td>
<td>15</td>
</tr>
<tr>
<td>REV</td>
<td>16</td>
</tr>
<tr>
<td>REV</td>
<td>17</td>
</tr>
<tr>
<td>REV</td>
<td>18</td>
</tr>
<tr>
<td>REV</td>
<td>19</td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td>REV</td>
<td>20</td>
</tr>
<tr>
<td>REV</td>
<td>21</td>
</tr>
<tr>
<td>REV</td>
<td>22</td>
</tr>
<tr>
<td>REV</td>
<td>23</td>
</tr>
<tr>
<td>REV</td>
<td>23</td>
</tr>
</tbody>
</table>

**Notifications and Correspondence**

<p>| NC | 1 | The System shall support reliable messaging, including guaranteed message delivery (without duplicates) and support for non-deliverable messages. |  |  |  |  | |
| NC | 2 | The System shall support messaging among internal agency personnel and contracting external entities to support the continuum of PA review, UM and CM activities. |  |  |  |  | |
| NC | 3 | The System shall have capacity to configure recipient and provider notifications with standard and customized content. |  |  |  |  |
|-----|----|-----------------------------------------------------------------------------------------|--------------------------------------------------------------|-----------------------------------------|------------------------------------------|----------------------------------------|------------------------|
| NC  | 4  | The System shall support the capacity to generate correspondence electronically and print for mailing. |                                                              |                                         |                                          |                                        |                        |
| NC  | 5  | The System shall have the capacity to generate electronic and other forms of notifications of PA approvals/denials to providers and recipients |                                                              |                                         |                                          |                                        |                        |
| NC  | 6  | The System shall automatically deny and alert/notify providers and PA reviewers of PA requests awaiting provider feedback if the provider has not responded within a timeframe defined by the state. |                                                              |                                         |                                          |                                        |                        |
| UMCM| 1  | The System can be configured to accept and assign a PA case number to provider generated and/or HIE notifications about recipient inpatient admissions that may not be initially subject to PA requirements, but will be subject to monitoring and potentially concurrent review as well as retrospective review. |                                                              |                                         |                                          |                                        |                        |
| UMCM| 2  | The System can be configured to monitor timelines associated with protocols for concurrent review and notify designated staff for required review and/or action. |                                                              |                                         |                                          |                                        |                        |
| UMCM| 3  | The System can be configured to flag cases for potential referral for care management based on diagnoses, utilization profile, high cost claims, and other factors. |                                                              |                                         |                                          |                                        |                        |</p>
<table>
<thead>
<tr>
<th>UMCM</th>
<th>4</th>
<th>The System shall provide imbedded decision supports that enable reviewers to view and evaluate adherence to utilization management</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>protocols, eligibility for programs, and need for referrals for care management.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMCM</td>
<td>5</td>
<td>The System shall support documentation and information sharing by designated agency care management personnel related to Recipient, caregiver, provider and other interactions during the continuum of care management activities.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMCM</td>
<td>6</td>
<td>The System shall have provisions to identify, monitor and report on Recipients receiving care management supports.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Electronic Document Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDM</td>
<td>1</td>
<td>The System shall provide for the digital identification, tracking and storing of all PA requests and documentation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDM</td>
<td>2</td>
<td>The System shall store digital photos or electronic imaging of PA attachments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDM</td>
<td>3</td>
<td>The System shall link attachments to the PA request with a tracking number, regardless of mode of submission.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDM</td>
<td>4</td>
<td>The System will retain incomplete PA request submissions for state-defined number of years before deleting the record.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDM</td>
<td>5</td>
<td>The System shall retain access to all relevant reports and PA records in accordance with DSS record retention policy.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDM</td>
<td>6</td>
<td>The organization provides for the recovery and reconstitution of the information System to a known state after a disruption, compromise, or failure. Recovery of the information System after a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------</td>
<td>----------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>failure or other contingency shall be done in a trusted, secure, and verifiable manner.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoring, Analytics and Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AR</td>
<td>1</td>
<td>The System can be configured to generate standardized and customized ad hoc reports to comply with DSS requirements.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AR</td>
<td>2</td>
<td>The System can access, compile, analyze and generate reports containing information from diverse sources i.e., other agencies, and external review entities for UM/CM related analytics.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AR</td>
<td>3</td>
<td>The System shall have analytic capabilities that enable authorized users by agency, division and/or program, to monitor and analyze the utilization of type of services by individual and population, including by agency, division and/or program, as well as performance and program metrics related to PA, UM and CM processes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AR</td>
<td>4</td>
<td>The System shall capture and display the PA data for any Recipient which includes status of the PA request, including pending, denied, approved, or modified, PA number, recipient information, receive date, date approved, expiration date, date adjudication notice sent to provider and recipient, ID of authorizing person, free-form text area for special considerations and capturing notes which will be printed on the PA notice, using predefined messages as well as unique messages (e.g., informing providers of cases where the original code requested was changed to reflect the diagnosis on the PA) or special considerations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>-------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>AR</td>
<td>5</td>
<td>The System’s analytic functions support financial analysis as required by Medicaid budgetary operations, including identification of financial liabilities related to pre-authorized services.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>In this column, elaborate as deemed appropriate on how the proposed solution meets a particular requirement OR why the proposal does not include functionality that meets that requirement.</td>
</tr>
<tr>
<td>AR</td>
<td>6</td>
<td>The System can be configured to monitor and analyze provider and recipient utilization patterns, detect unusual conditions and route System alerts and alarms to trigger further investigation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AG</td>
<td>1</td>
<td>The System shall have the capacity to support adjudication of PA re-determinations and links to the appeals and grievances process as appropriate, including documentation, monitoring and issuing notifications electronically and hard copy.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AG</td>
<td>2</td>
<td>The System provides supports for staff involved in adjudicating appeals and grievances by providing access to required background information available in the System, MMIS and other relevant attachments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WF</td>
<td>1</td>
<td>The System shall support monitoring workload, staff assignments and productivity and tracking individual PA status including across agencies and divisions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WF</td>
<td>2</td>
<td>The System generates performance measures for specific business processes using predefined and ad hoc reporting methods.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WF</td>
<td>3</td>
<td>Functionality includes the ability to conduct real time monitoring of the status of reviewer workloads and related transactions, generation of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>--------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------</td>
<td>----------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>WF</td>
<td>4</td>
<td>management reports that track individual and aggregate productivity metrics.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>In this column, elaborate as deemed appropriate on how the proposed solution meets a particular requirement OR why the proposal does not include functionality that meets that requirement.</td>
</tr>
<tr>
<td>WF</td>
<td>5</td>
<td>The System shall provide a CRM solution with assignment, queue tracking and status update capability.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WF</td>
<td>5</td>
<td>The System shall ensure that authorized users have access to user activity history and other management functions, including log-on approvals/disapprovals and log search and playback.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# ATTACHMENT C – Technical and Contractor Scope of Work Requirements Matrix

Non-Functional Requirements Instructions:
Please review the non-functional requirement and for those that can be answered with a Yes or No and, if no, the effort of level required to become compliant.

The vendors should review the requirement and provide a concise narrative response in the area provided if needed.

<table>
<thead>
<tr>
<th>Non-Functional Requirement Category Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Technical</td>
</tr>
<tr>
<td>Implementation Methodology and Plan</td>
</tr>
<tr>
<td>Conversion</td>
</tr>
<tr>
<td>Testing</td>
</tr>
<tr>
<td>Knowledge Management, Transfer, and Training</td>
</tr>
<tr>
<td>Deployment, Transition, and Cutover</td>
</tr>
<tr>
<td>Maintenance and Operations</td>
</tr>
<tr>
<td>Issue and Problem Management</td>
</tr>
<tr>
<td>Solution Administrator Support</td>
</tr>
<tr>
<td>Staffing</td>
</tr>
<tr>
<td>Assurances</td>
</tr>
<tr>
<td>Hosting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Technical</strong></td>
<td><strong>Solution architecture</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>1</td>
<td>The system shall be comprised of modular components that can be added on or subtracted from through installation addition or license expansion.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>1.02</td>
<td>Modular additions shall not require custom coding effort.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>1.03</td>
<td>The system as architected shall be consistent with/conforms with the Seven Standards and Conditions (modularity, MITA, interoperability, business results, leverage/reuse, industry standards, reporting)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>1.04</td>
<td>The system shall use a modular architecture, adhering to Service Oriented Architecture (SOA) principles, that provides clear separation of system components even as the components are designed to interoperate with other components, including components developed by other companies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>1.05</td>
<td>The system shall provide the ability for concurrent users to simultaneously view the same record, documentation and/or template and, where applicable, work on the same record including create, read, update and delete transactions recording said</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant.</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>GT</td>
<td>1.06</td>
<td>The system shall be highly re-configurable, providing ability to reposition and rename field labels / data fields, remove or “turn-off” unused fields, maintain data, modify the layout of the user interface, and allow addition of custom-defined fields with minimal or no customization.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>1.07</td>
<td>The system uses standardized business rules definitions that reside in a separate application or rules engine.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>1.08</td>
<td>Any website or web application hosted by the Offeror that generates email cannot use “@state.sd.us” as the originating domain name per state security policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>2</td>
<td><strong>Interface and interoperability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>2.01</td>
<td>The system shall be built to support data integration with other systems using web services, application programming interfaces (APIs) compliant with current and proposed federal rules or other mechanisms that do not require custom programming and both localize and minimize the impact of new technology insertion.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>2.02</td>
<td>The system shall support the dynamic exchange of data from multiple solutions in real time and batch.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>2.03</td>
<td>The system shall support linkage to the state's document management solution (File Director) as well as a contractor-proposed document management system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>2.04</td>
<td>The contractor shall work with the State to develop optimized interfaces - i.e. interfaces that accomplish the objective of exchanging the requisite data and simultaneously require the least amount of custom programming and maintenance - between the solution and state systems with pertinent source data and/or requiring data from the solution for downstream functions. These State systems include but are not limited to: Medicaid Management Information System (MMIS), DSS Master Person Index (when available), DSS Data Warehouse (when available), FACIS (DSS Division of Child Protection Services case management system), STARS (DSS Division of Behavioral Health Services case management system). The complete list of relevant state systems will be finalized during the requirements finalization phase.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>2.05</td>
<td>The contractor shall partner with the State in the development of State-specific transaction/event code sets, data exchange and reporting standards and will conform to such standards as stipulated in the plan to implement the standards.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>2.06</td>
<td>Where web services are used in the engineering of applications, the contractor’s systems shall conform to World Wide Web Consortium (W3C) standards such as</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>XML, UDDI, WSDL and SOAP so as to facilitate integration of contractor systems with state systems.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Point-to-point integrations shall be avoided to the extent possible. Application integration shall be achieved to the extent possible via a central service model.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The contractor shall work with the State to develop and implement an Interface transition strategy consistent with any agreed-to phase-in of solution functionality (whether phase-in is based on programs or regions/geography) such that the solution and legacy systems are both properly populated, and the associated programs operating appropriately, during the implementation phase-in. This may involve some interface redundancy in the short term.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>User access modalities including mobility enablement</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall allow for access to executive level dashboard reports via mobile/tablet device.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall allow for secure access to select client and end user functionality via mobile/tablet device without loss/degradation of functionality</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall support multiple user access modalities including remote access connection (Windows) and web browser (state-supported browsers)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Security including identity management and verification and access management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall enable role-based security to allow designated security staff to assign and repeal roles from user accounts as needed.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall support multi-factor authentication.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>At a minimum, the system shall meet HIPAA requirements and guidelines for password management including but not limited to password length and composition, previous use and change frequency.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall support user single sign on (SSO) using the State-provided Microsoft standard integration toolkit.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall support field and record level security.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The contractor shall ensure all electronic data transfers and access comply with all applicable State, federal and HIPAA Privacy and Security requirements.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall allow users to reset passwords if not SSOed with another system.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall allow the deletion or deactivation of user accounts.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall encrypt all stored passwords.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system's online user interface shall only be accessible remotely via a secure, encrypted session.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The system shall encrypt data at rest and in motion/transit.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant.</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| GT  | 4.12 | The contractor’s system shall employ an access management function that restricts access to varying hierarchical levels of system functionality and Information. The access management function shall:  
  • Restrict access to information on a "need-to-know" basis, e.g. users permitted inquiry privileges only will not be permitted to modify information;  
  • Restrict access to specific system functions and Information based on an individual user profile, including inquiry only capabilities; global access to all functions will be restricted to specified staff jointly agreed to by the State and the contractor; and  
  • Restrict attempts to access system functions to three (3), with a system function that automatically prevents further access attempts, records these occurrences and generates a notification to the designated security administrator(s)/resources. |                    |                                                               |
| GT  | 4.13 | If the system is contractor-hosted, the contractor shall provide for the physical safeguarding of its data processing facilities and the systems and information housed therein in accordance with HIPAA and pertinent State requirements. The contractor shall provide the State with access to data facilities upon the State’s request. The physical security provisions shall be in effect for the life of this Contract. |                    |                                                               |
| GT  | 4.14 | If the system is contractor-hosted, the contractor shall restrict perimeter access to equipment sites, processing areas, and storage areas through a card key or other comparable system, as well as provide accountability control to record access attempts, including attempts of unauthorized access in accordance with HIPAA and pertinent State requirements. |                    |                                                               |
| GT  | 4.15 | If the system is contractor-hosted, the contractor shall include physical security features designed to safeguard processor site(s) through required provision of fire retardant capabilities, as well as smoke and electrical alarms, monitored by security personnel. |                    |                                                               |
| GT  | 4.16 | The contractor shall ensure that the operation of all of its systems is performed in accordance with State and federal regulations and guidelines related to security, confidentiality, and encryption of the protected information managed by the contractor, and shall strictly comply with HIPAA Privacy and Security Rules, as amended, and with the Breach Notification Rules under the HITECH Act. |                    |                                                               |
| GT  | 4.17 | The contractor shall ensure compliance with:  
  • 42 CFR Part 431 Subpart F (confidentiality of information concerning applicants and Enrollees of public medical assistance programs);  
  • 42 CFR Part 2 (confidentiality of alcohol and drug abuse records); and |                    |                                                               |
<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant.</th>
</tr>
</thead>
<tbody>
<tr>
<td>GT</td>
<td>4.18</td>
<td>The system shall adhere to the principle of “Fail Safe” to ensure that, if parts of the system have been compromised, that the unauthorized user cannot access certain information maintained in the system, alter certain system functions, or leave any access controls vulnerable to future attacks.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>4.19</td>
<td>The software used to install and update the system, independent of the mode or method of conveyance, shall be certified free of malevolent software (&quot;malware&quot;). Contractor may self-certify compliance with this standard through procedures that make use of commercial malware scanning software. Alternatively, the State reserves the right to run security scans and, based on those scans, require the contractor to correct issues identified.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>4.20</td>
<td>The system, when storing PHI on any device intended to be portable/removable (e.g. smartphones, portable computers, portable storage devices), shall support use of a standards based encrypted format using Advanced Encryption Standard (AES) or its successor.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>4.21</td>
<td>The contractor shall review and analyze the key risks to the important assets and functions provided by the System to certify that the Common Weakness Enumeration (CWE)/SANS Institute Top 25 Most Dangerous Software Errors (<a href="http://cwe.mitre.org/top25">http://cwe.mitre.org/top25</a>) have been mitigated and document the mitigation.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>4.22</td>
<td>The system shall be subject to a Security Impact/Risk Assessment and security scans - including security scans to be performed by BIT without exception - prior to implementation or the release of any updates into production. The State reserves the right to utilize State resources and/or third parties to conduct security scans and to approve of any third party used by the contractor to conduct a Security Impact/Risk Assessment. Moreover, the contractor will be required to respond in writing regarding mitigation plans for the security vulnerabilities and pass a final follow-up security scan for the website(s), software and/or cloud services to be acceptable products to the State.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>4.23</td>
<td>If the contractor hosts the system, all system servers shall have hardened operating environments by eliminating any unnecessary system services, accounts, network services, and limited user access rights throughout all of the environments.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>4.24</td>
<td>The system contains verification mechanisms that are capable of authenticating authority (as well as identify) for the use or disclosure requested. For example:  • Denies general practitioner inquiry for recipient eligibility for mental health services</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>-------------------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>GT</td>
<td>4.25</td>
<td>• Permits inquiries on claim status only for claims submitted by the inquiring provider.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>4.25</td>
<td>The system must protect electronic protected health information (ePHI) from improper alteration or destruction including authentication mechanisms and to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. The following is the minimal set of information that must be safeguarded: (1) Names, unique identifiers and addresses. (2) Medical services provided. (3) Social and economic conditions or circumstances. (4) Agency evaluation of personal information. (5) Medical data, including diagnosis and past history of disease or disability. (6) If applicable, any information received for verifying income eligibility and amount of medical assistance payments. Income information received from SSA or the Internal Revenue Service must be safeguarded according to the requirements of the agency that furnished the data. (7) If applicable, any information received in connection with the identification of legally liable third party resources.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>4.26</td>
<td>After 20 minutes of inactivity, the system should initiate a session lock; the session lock should remain in place until the user reestablishes access using established identification and authentication procedures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>4.27</td>
<td>If the contractor’s solution is a web-accessible application or provisioned on a Software-as-a-Service basis, the contractor will utilize the most current version of Active Directory Federation Service (ADFS) for all user logins of State of South Dakota staff. If the contractor cannot make use of ADFS, the contractor must explain how State staff will be informed not to use their State password to log into the contractor’s solution.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5</td>
<td><strong>Availability including Business Continuity and Disaster Recovery (BC-DR)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.01</td>
<td>The system shall be architected such that changes to operating environment or component applications/modules can be effected without availability being compromised.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.02</td>
<td>The system shall be available for UI access and adhoc reporting during standard state business hours.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.03</td>
<td>The system shall process data off hours as needed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.04</td>
<td>The BC-DR plan shall include initial development, continuous updates, ad-hoc updates as warranted by certain events/developments.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant.</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>GT</td>
<td>5.05</td>
<td>The contractor shall ensure that critical systems, including but not limited to the client and user portals, as well as phone-based functions and information services, available to the applicable system users twenty-four (24) hours a day, seven (7) Calendar Days a Week, except during periods of scheduled System Unavailability agreed upon by the State and the contractor. Unavailability caused by events outside of a contractor’s span of control is outside of the scope of this requirement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.06</td>
<td>The contractor shall ensure that at a minimum all non-critical system functions and information are available to the applicable system users between the hours of 7:00 a.m. (Central Time) and 7:00 p.m. (Central Time) Monday through Friday.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.07</td>
<td>The contractor shall develop an automated method of ascertaining the state, performance and availability of critical systems on at least a thirty (30) minute basis twenty-four (24) hours a day, seven (7) days per week.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.08</td>
<td>Upon discovery of any problem within its span of control that may jeopardize system availability and performance as defined in the contract, the contractor shall notify the applicable state staff in person, via phone, and/or electronic mail. The contractor shall deliver notification as soon as possible but no later than 7:00 pm (Central Time) if the problem occurs during the Business Day and no later than 9:00 am (Central Time) the following Business Day if the problem occurs after 7:00 pm (Central Time).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.09</td>
<td>Where the operational problem results in delays in report distribution or problems in on-line access during the business day, the contractor shall notify the applicable State staff within fifteen (15) minutes of discovery of the problem, in order for the applicable work activities to be rescheduled or be handled based on System Unavailability protocols.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.10</td>
<td>Unscheduled system unavailability of system functions deemed “critical” caused by the failure of systems and telecommunications technologies within the contractor’s span of control shall be resolved, and the restoration of services implemented, within thirty (30) minutes of the official declaration of System Unavailability.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.11</td>
<td>Unscheduled system unavailability of all other contractor system functions caused by systems and telecommunications technologies within the contractor’s Span of Control shall be resolved, and the restoration of services implemented, • within four (4) hours of the official declaration of Unscheduled System Unavailability, when unavailability occurs during business hours, and • within two (2) hours of the start of the next Business Day, when unavailability occurs during non-business hours.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant.</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>GT</td>
<td>5.12</td>
<td>Cumulative system unavailability caused by systems and telecommunications technologies within the Contractor’s span of control shall not exceed one (1) hour during any continuous five (5) Calendar Day period for functions that affect client and enrollee services. For functions that do not affect clients and enrollees, cumulative System Unavailability caused by systems and telecommunications technologies within the Contractor’s span of control shall not exceed four (4) hours during any continuous five (5) Business Day periods.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.13</td>
<td>For any system outage that is not corrected within the required time limits, the contractor shall provide full written documentation that includes a Corrective Action Plan, describing how the problem will be prevented from occurring again, within five (5) Business Days of the problem’s occurrence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.14</td>
<td>Regardless of the architecture of its systems, the contractor shall develop and be continually ready to invoke a Business Continuity and Disaster Recovery (&quot;BC-DR&quot;) plan that at a minimum addresses the following scenarios: (i) the central computer installation and resident software are destroyed or damaged, (ii) System interruption or failure resulting from network, operating hardware, software, or operational errors that compromises the integrity of transactions that are active in a live system at the time of the outage, (iii) System interruption or failure resulting from network, operating hardware, software or operational errors that compromises the integrity of data maintained in a live or archival system, (iv) System interruption or failure resulting from network, operating hardware, software or operational errors that does not compromise the integrity of transactions or data maintained in a live or archival system but does prevent access to the system, i.e. causes unscheduled system unavailability. The BC-DR plan shall account for and be in effect during the entire period beginning with project kickoff and ending with the end of any turnover period. This BC-DR plan must be prior approved by the State.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.15</td>
<td>The contractor shall test its BC-DR plan through simulated disasters and lower level failures in order to demonstrate to the State that it can restore System functions per the standards outlined elsewhere in this Section. The results of these tests shall be reported to the state within thirty (30) Calendar Days of completion of said tests. The frequency of these tests will be agreed upon between the State and the contractor, but shall be annual at a minimum.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.16</td>
<td>In the event that the contractor fails to demonstrate in the tests of its BC-DR plan that it can restore system functions per the standards outlined in this Contract, the contractor shall be required to submit to the state a Corrective Action Plan that</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>describes how the failure will be resolved. The Corrective Action Plan will be delivered within five (5) Business Days of the conclusion of the test.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.17</td>
<td>The contractor shall submit a monthly Systems Availability and Performance Report to the State in accordance with specs mutually agreed to between the contractor and the State.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.18</td>
<td>The system will have the ability to support session replication and transparent failover using high-availability architectural options.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>5.19</td>
<td>The system’s Recovery Point Objective (RPO) shall be no more than one (1) hour of data loss, i.e. in case of a disaster that affects operations up to one (1) hour of data inputs to the system may be lost and need to be re-entered.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>6</td>
<td><strong>Performance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>6.01</td>
<td>The system response time during operations shall be 5 seconds or less for 95 percent of the search and lookup queries (does not include ad hoc queries and analytics) as tested in a sufficient number of state sites. Maximum response time will not exceed 15 seconds except for agreed to exclusions. Response time is defined as the time elapsed after depressing an ENTER key (or clicking on a button that triggers the transaction) until the system generates a response for the user.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>6.02</td>
<td>The system shall return a Dashboard report within 5 seconds or less, 95% of the time.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>6.03</td>
<td>The system shall return a Static Standard report within 5 seconds or less, 95% of the time.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>6.04</td>
<td>The system shall return a parameter-based report within 20 seconds or less.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>6.05</td>
<td>The contractor will provide access to a monitoring tool which the State can utilize to monitor the performance and operation of the contractor’s solution including but not limited to all solution components and connections. It is required that this tool be easy to use and provide a dashboard of the health of the proposed solution. The effectiveness of this monitoring tool will be a component of acceptance testing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>7</td>
<td><strong>Capacity, scalability and extensibility</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>7.01</td>
<td>The system shall be scalable and adaptable to meet future growth and expansion/contraction needs such that the system can be expanded on demand and be able to retain its performance levels when adding additional users, functions, and data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>7.02</td>
<td>The system shall possess capacity sufficient to handle the workload projected for the start of the program and will be scalable and flexible so they can be adapted as needed, within negotiated timeframes, in response to program or enrollment changes. This will be determined as part of solution and operational readiness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>activities that shall be conducted by the state in accordance with a mutually agreed upon protocol.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>7.03</td>
<td>The system's interfaces shall be scalable to accommodate changes in scale including changes in user population, transaction volume, in-scope programs, and user geographic distribution.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8</td>
<td><strong>Usability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.01</td>
<td>The contractor shall be able to demonstrate that its client and end user portals have undergone extensive usability testing with at least three independent groups and that the results of said testing have been incorporated into the design of the client and user portal - navigation, user interface/screen design, menu design, user prompts, ease to populate fields/provide information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.02</td>
<td>The layout and other applicable characteristics of the pages of contractor websites shall be compliant with federal “Section 508 standards” and Web Content Accessibility Guidelines developed and published by the Web Accessibility Initiative.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.03</td>
<td>The system shall have interface capabilities to devices and enhancements to assist persons with visual impairments and comply with Section 508, The Rehab Act of 1973, as amended, as well as Web Content Accessibility Guidelines (WCAG) Level 1 and 2. It shall accommodate the screen reader software, JAWS, DRAGON SPEAK, OPEN BOOK, and Zoom Text. The Vendor warrants that the IT solution offered under this bid proposal will provide equivalent access for effective use by both visual and non-visual means.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.04</td>
<td>The system shall allow users to complete all functions and navigate all fields by both keyboard and mouse.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.05</td>
<td>The system shall allow users to adjust screen and printed fonts both in size and color and adjust background colors and screen contrast (functionality should be similar to Microsoft Office applications).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.06</td>
<td>The system shall support undo and redo, or provide onscreen confirmation/acceptance to the user to confirm a change that is permanent and cannot be &quot;undone&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.07</td>
<td>The system shall allow users to create shortcuts (e.g. onscreen short cuts, hot-keys, etc.) for frequent actions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.08</td>
<td>The system shall provide users with a clearly marked &quot;emergency exit&quot; for the instances when a user mistakenly chooses a function and such &quot;emergency exit&quot; must be simple with minimal dialogue.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant.</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>GT</td>
<td>8.09</td>
<td>The system shall provide drop down and list boxes for all key entry, and text entry will display existing values for selection (system based auto fill) (but specifically disallow client browser based autofill).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.10</td>
<td>Wherever applicable, the system shall accommodate point and click selection and check box entry for all relevant data entries to ensure that the user does not have to enter textual data that may already be available to the system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.11</td>
<td>The system shall provide field level on-screen edits with limited user override capabilities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.12</td>
<td>The system shall provide the ability to make fields visible/invisible depending on parameters, user rights, consent, and access controls.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.13</td>
<td>The system shall not show fields not accessible to a given user based on access rights, client consent, nor will the System show fields not in use.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>8.14</td>
<td>The system cursor shall automatically advance to the next logical input field when the maximum allowed numbers of characters have been entered for the keyed field or when the user presses the &quot;Enter&quot; key.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9</td>
<td><strong>Data and document management including storage and retention</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.01</td>
<td>The contractor shall ensure that incremental backups of the entire system's database(s) are completed at least daily, and full backups are completed at least weekly.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.02</td>
<td>The system shall be built on a relational database (SQL2016 or higher).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.03</td>
<td>The system shall have a data dictionary that shall be kept regularly up-to-date. All changes shall be updated in the dictionary within 30 days of modification or addition of fields in production. The data dictionary shall provide definitions of data elements and data relationships amongst said elements such that these are understandable by system end users.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.04</td>
<td>The system shall maintain the integrity of data element sources used by reporting functions and integrate necessary data elements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.05</td>
<td>The information required for on line help functions shall be maintained in the data dictionary.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.06</td>
<td>The system shall include the ability to add new data sets and data sources as directed by the State and per federal guidelines.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.07</td>
<td>The system shall retain reports for the longer of (a) timeframes specified by the State or (b) at least four years of selected management reports and five years of annual reports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.08</td>
<td>The system shall include the ability to support the deletion of data when necessary.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant.</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>GT</td>
<td>9.09</td>
<td>The system shall include the ability to load and append information into the DSS/DW in accordance with state SLA time requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.10</td>
<td>The system shall provide the ability to identify if an error occurred during a load process and automatically notify a list of contacts by email and direct contact (text, page, or phone), and produce an error report. The error report would specify the type of error (i.e. data error, processing error, system error, etc.). State specific error types or codes can be added to a specific implementation with additional cost.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.11</td>
<td>The system database shall be updated with select claims data from batch adjudication to allow for accurate processing of the next related claim and for tracking of service units used vs. authorized. The update process shall handle voids and adjustments.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.12</td>
<td>The system shall employ proven database design and data management methodologies to validate, scrub (clean and error), and transform raw data. After loading the data, the database should be analytically ready to support data warehouse capabilities and methodologies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.13</td>
<td>The system shall provide the ability to rollback the most recent data load.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.14</td>
<td>The contractor shall ensure that incremental backups of all solution databases are executed daily, and full backups are executed at least weekly, without said backups impacting or compromising performance in a measurable manner.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.15</td>
<td>The system shall conform to HIPAA standards for data and document management.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.16</td>
<td>The system shall contain controls to maintain information integrity. These controls shall be in place at all appropriate points of processing. The controls shall be tested in periodic and spot audits following a methodology to be developed jointly by and mutually agreed upon by the contractor and the State.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.17</td>
<td>The contractor shall house indexed images of documents in the appropriate database(s) and document management systems so as to maintain the logical relationships between certain documents and certain data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.18</td>
<td>The system shall enable the State to modify the labels and arrangement of information in the data model documentation templates and can create custom data fields.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>9.19</td>
<td>System shall have the ability to maintain linkage between PA records and associated claim records in the State's Medicaid claims management system/module.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10</td>
<td><strong>Audit support and compliance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.01</td>
<td>The contractor shall provide secure, online access to select system functionality to at least three (3) State personnel to facilitate resolution of inquiries and to research issues as needed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant.</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>GT</td>
<td>10.02</td>
<td>The contractor shall provide a distinct method of communication between itself and the State to enable secure exchange of information regarding program integrity management and audit activities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.03</td>
<td>Audit trails shall be incorporated into all systems to allow information on source data files and documents to be traced through the processing stages to the point where the information is finally recorded. The audit trails shall: a. Contain a unique log-on or terminal ID, the date, and time of any create/modify/delete action and, if applicable, the ID of the system job that effected the action; b. Have the date and identification “stamp” displayed on any on-line inquiry; c. Have the ability to trace data from the final place of recording back to its source data file and/or document shall also exist; d. Be supported by listings, transaction reports, update reports, transaction logs, or error logs; e. Facilitate auditing of individual claim records as well as batch audits; and f. Be maintained for seven (7) years in either live and/or archival systems. The duration of the retention period may be extended at the discretion of and as indicated to the contractor by the State as needed for ongoing audits or other purposes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.04</td>
<td>The contractor shall institute processes to insure the validity and completeness of the data it submits to the State. At its discretion, the State will conduct general data validity and completeness audits using industry-accepted statistical sampling methods. Data elements that will be audited include but are not limited to: client ID, date of service, program category and sub category (if applicable) of service, claim processing and adjudication milestones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.05</td>
<td>The System shall support auditing at the object level (i.e. Table, Column)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.06</td>
<td>The System will allow an authorized administrator to set the inclusion or exclusion of auditable events based on organizational policy &amp; operating requirements/limits.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.07</td>
<td>The System shall be able to perform time synchronization using Network Time Protocol (NTP)/Simple Network Time Protocol (SNTP), and use this synchronized time in all security records of time.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.08</td>
<td>The System shall prohibit all users read access to the audit records, except those users that have been granted explicit read access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.09</td>
<td>The System shall protect the stored audit records from unauthorized deletion. The System will prevent modifications to the audit records.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.10</td>
<td>The System shall prevent modifications to the audit records.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant.</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>GT</td>
<td>10.11</td>
<td>The contractor shall support Enterprise Life Cycle (ELC) Gate Reviews as prescribed by CMS and other federally prescribed audit activities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.12</td>
<td>The contractor shall provide updated artifacts to support ELC and other federal reviews.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GT</td>
<td>10.13</td>
<td>The contractor shall provide support as needed during ELC and other federal reviews.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Implementation Methodology and Plan**

| IMP | 1 | Per the approved Project Management and Communication Plan described in RFP section 4.2.7.1, the contractor shall incorporate industry-standard project management processes to manage the system implementation. |                      |                                                             |
| IMP | 2 | The contractor shall propose and maintain a project meeting cadence to include, at a minimum, a:  
  • Weekly Status meeting  
  • Monthly Steering Committee meeting  
  • Issue & Risk Management meeting  
  • Functional Team meetings, as needed  
  • Program-specific meetings, as needed  
  • Other meetings as determined and agreed to by the contractor and state |                      |                                                             |
| IMP | 3 | The contractor shall implement, manage and administer access to a project-specific portal/website that support project management activities.                                                                            |                      |                                                             |
| IMP | 4 | The project-specific portal shall be accessible by contractor, state, and any other project assigned resources and granted access to portal content and functionality based on roles.                               |                      |                                                             |
| IMP | 5 | The project management portal shall support all phases and aspects of the project including, but not limited to, requirements traceability, change management, defect tracking and management, testing, training, performance standards management, issue and risk management, communications management, and deliverable management for the project. |                      |                                                             |

**Migration and Conversion**

<p>| CON | 1 | The contractor shall have a data migration and conversion strategy and approach that ensures data integrity and no loss of referential integrity.                                                                      |                      |                                                             |
| CON | 2 | The contractor shall have a document conversion strategy and approach for supporting migration of documents that emphasizes no loss of referential integrity and ensures linkages across documents and between documents and applicable records are preserved. |                      |                                                             |</p>
<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td>CON</td>
<td>3</td>
<td>The contractor shall have a record conversion strategy and approach that incorporates both data and document conversion and ensures no loss of referential integrity.</td>
<td>Compliant: Yes</td>
<td>If no, elaborate on level of effort required to be compliant</td>
</tr>
<tr>
<td>CON</td>
<td>4</td>
<td>The contractor's approach to data, document and record conversion shall incorporate - at a minimum - a repeatable methodology that allows for backing out of conversions based on certain problems or issues being identified, thorough project planning, a proven project management methodology, specifics on how the relationship between source and target data structures will be defined and ensured, any changes in valid codes/values, and the use of automated tools. All of these will be detailed in a conversion plan which will be provided to the State and approved by the State before conversion activities are effected.</td>
<td>Compliant: Yes</td>
<td>If no, elaborate on level of effort required to be compliant</td>
</tr>
<tr>
<td>CON</td>
<td>5</td>
<td>The Data Migration and Conversion Plan shall include a rollout schedule and the contractor will perform (at a minimum) the following tasks: • Ensure a database backup is in place • Execute the data conversion packages • Validate the converted data to confirm success • Revert to backup if conversion failed • Provide the State with results of the conversion and any exceptions • Support the State in the resolution of non-converted data • Provide post conversion support through requested ad-hoc reporting and provision of access to the pre and post converted data for State confirmation analysis.</td>
<td>Compliant: Yes</td>
<td>If no, elaborate on level of effort required to be compliant</td>
</tr>
<tr>
<td>CON</td>
<td>6</td>
<td>The contractor shall work with the State to develop and implement a data conversion transition strategy consistent with any agreed-to phase-in of solution functionality (whether phase-in is based on programs or regions/geography) such that the solution and legacy systems are both properly populated, and the associated programs operating appropriately, during the implementation phase-in. This may involve a phase-in of the conversion of certain data.</td>
<td>Compliant: Yes</td>
<td>If no, elaborate on level of effort required to be compliant</td>
</tr>
<tr>
<td>CON</td>
<td>7</td>
<td>The contractor shall be required to (a) migrate and convert a minimum of seven years of records, associated data and documents and (b) ensure that all records, data and documents for active cases are migrated and converted.</td>
<td>Compliant: Yes</td>
<td>If no, elaborate on level of effort required to be compliant</td>
</tr>
</tbody>
</table>

**Testing**

<p>| TEST | 1   | The contractor will develop and submit a Testing Plan. The Testing Plan will include the procedures for documenting the completion of each testing activity, test scripts, test conditions, test cases, and test reports. Detailed test plans will be created for the following testing areas: | Compliant: Yes | If no, elaborate on level of effort required to be compliant |</p>
<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant.</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEST 2</td>
<td>2</td>
<td>The contractor shall repeat any test cycle when a failure occurs at any stage of said cycle (e.g., a failure in User Acceptance Testing that necessitates a code change will require the component to go back through Unit Testing, Integration Testing, and so forth).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TEST 3</td>
<td>3</td>
<td>The contractor shall provide South Dakota with the results of all testing activities defined in the Test Plan.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TEST 4</td>
<td>4</td>
<td>The contractor shall update and maintain the test documents, procedures, and scripts throughout development and through full system acceptance to reflect the as-built design and current requirements.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| TEST 5 | 5 | The contractor shall produce a User Acceptance Test (UAT) results report. The contractor will support South Dakota User Acceptance Testing (UAT) activities, including:  
• Script development and requirements traceability  
• Technical & Health Analytics consultation for the duration of UAT  
• System support for the UAT environment  
• Document UAT Results for State approval |  |  |
| TEST 6 | 6 | The contractor shall correct any functionality that does not pass UAT within a timeframe agreed to by South Dakota and perform system Regression Testing. |  |  |

**Knowledge Management, Transfer, and Training**

<p>| KMT 1 | 1 | The contractor shall produce documentation for the entire system. |  |  |
| KMT 2 | 2 | The contractor shall produce user manuals including desk level procedures, for the system in the format and electronic version approved by the State. |  |  |
| KMT 3 | 3 | The contractor shall store system documentation and user manuals electronically in a central location accessible by State staff. |  |  |
| KMT 4 | 4 | The contractor shall produce updated documentation prior to the implementation of any system changes. |  |  |</p>
<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMT</td>
<td>5</td>
<td>The contractor shall write system and component narratives so that they are understandable by non-technical persons.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMT</td>
<td>6</td>
<td>The contractor shall prepare system documentation that contains a general system narrative, system architecture and data flow diagrams, a description of the operating environment and hierarchical, multi-level diagrams that depict both online and offline processes. Each component must be referenced and documentation must be consistent across all components.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMT</td>
<td>7</td>
<td>The contractor shall organize user documentation in a procedural, step-by-step format.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMT</td>
<td>8</td>
<td>The contractor shall include a table of contents and index in all documentation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMT</td>
<td>9</td>
<td>The contractor shall identify error messages including descriptions, for all fields incurring edits and provide the necessary steps to resolve. This list must be a composite of system level and component level errors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMT</td>
<td>10</td>
<td>The contractor shall ensure that the use of acronyms and codes are consistent with windows, screens, reports and databases or data dictionary.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| KMT | 11 | The contractor shall:  
- Use abbreviations consistently throughout the documentation  
- Use field names consistently for the same fields throughout the documentation  
- Include in the user manual tables of valid values for all data fields including codes  
- Include in the user manual illustrations of windows, frames, screens used, by component, with all data elements |  |  |
<p>| KMT | 12 | The contractor shall provide version control for all documentation to maintain historical document archives. |  |  |
| KMT | 13 | The contractor shall provide the ability to print select pages, sections, and entire manuals. |  |  |
| KMT | 14 | The contractor shall develop end user classroom training materials, including end of training assessment or comprehension tools. |  |  |
| KMT | 15 | The contractor shall deliver centralized or regional train the trainer (T3) training to designated State resources per a mutually agreed upon schedule prior to each go live phase or pilot. |  |  |
| KMT | 16 | The contractor shall provide online training functionality that includes a self-guided introduction to the system and a comprehensive training environment that supports training based on user roles and program rules. |  |  |
| KMT | 17 | The contractor shall provide a training environment that fully replicates the functionality and operations of the production system. This includes but is not |  |  |</p>
<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>limited to copies of software, tools, databases, and client, provider and transaction data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMT</td>
<td>18</td>
<td>The training environment shall have the functionality to add and change data based on user roles and business needs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMT</td>
<td>19</td>
<td>The training environment shall enable generation of any outputs that can be generated within the production environment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMT</td>
<td>20</td>
<td>The contractor shall have a process that ensures changes to the production system are applied in a timely manner in the end user training environment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KMT</td>
<td>21</td>
<td>The contractor shall provide knowledge transfer services at the end of the contract period as part of a turnover plan to ensure the State has knowledgeable system administrators and other technical support staff to maintain and operate the system independently.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Deployment/Transition/Cutover**

| DTC | 1  | The contractor shall provide a Deployment plan that at a minimum addresses the following:  
|-----|----|-------------------------|----------------------|----------------------------------------------------------|
|     |    | • The proposed methodology for system cutover to the appropriate entities.  
|     |    | • The approach to system and operations cutover based on the contractor’s proposed solution, and the contractor’s own experience with comparable projects.  
|     |    | • How the contractor will manage the transition while maintaining production and testing schedules;  
|     |    | • Requirements for integration between the replacement system and any legacy system(s) that will remain in use during a phased transition  
|     |    | • How the contractor will document, track and resolve issues during cutover and a subsequent transition to steady state operations period; this period will be mutually agreed to between the contractor and the State.  
|     |    | • How changes will be synchronized and distributed when multiple activities are occurring simultaneously across multiple environments (e.g. sandbox, configuration/development, test, quality assurance, production, training, and disaster recovery).  
|     |    | • How code will be migrated from design through coding, acceptance, unit, and integration testing, as well as promotion into production. |                      |                                                          |

**Maintenance and Operations**

<p>| MO  | 1  | Upon completion and acceptance of each project phase, the contractor shall provide a one hundred and eighty (180) calendar day warranty period for the respective phase in which the contractor will support the system at no additional |                      |                                                          |</p>
<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>cost to the state and provide all necessary technical support, updates and fixes necessary to operate the solution in the manner prescribed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MO</td>
<td>2</td>
<td>Upon expiration of the warranty, the contractor shall provide a fee-based annual maintenance program to include all technical support, updates and fixes necessary to operate the solution in the manner prescribed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MO</td>
<td>3</td>
<td>The contractor shall develop a comprehensive system maintenance plan. The maintenance plan shall be submitted to the state for review and approval and must, at a minimum: • Ensure the contractor’s system continually meets federal and state requirements; • Accommodate new legislation and evolving regulations, processes, architecture and standards; and • Provide regular and periodic maintenance to the system on a semi-annual basis or on a schedule agreed upon by South Dakota.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Issue and Problem Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISS</td>
<td>1</td>
<td>The contractor shall use a single Issue Tracking System that the contractor and South Dakota will use collaboratively for the tracking of system defects, security issues, data quality anomalies, enhancements, and other system issues or change management items.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISS</td>
<td>2</td>
<td>The Issue Tracking System shall, at a minimum, include: • All defects in the solution identified during any testing phase must be recorded, prioritized, tracked, and resolved in a timely manner. Each must be assigned a “Defect Level” based a mutually agreed upon standard (e.g., Critical, Serious, High, Moderate, Low, etc.) • The contractor will allow South Dakota full access to the Issue Tracking System.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Solution Administrator Support</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAS</td>
<td>1</td>
<td>The contractor shall provide a dedicated Help Desk. The Help Desk will provide the single point of contact for systems related issues. The Help Desk, to be staffed during business hours (to be determined by South Dakota), will provide support for issues related to the systems business and technical functionality which need to be escalated for investigation and resolution. The Help Desk, and associated staff must be physically located in the continental United States.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAF</td>
<td>1</td>
<td>The contractor shall develop and maintain compliance with the Project Staffing Plan accepted as a part of the Project Management and Communication Plan deliverable. The plan, at minimum, shall: • Describe the overall project organization structure and how the project team is</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant.</td>
</tr>
<tr>
<td>-----</td>
<td>----</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|     |    | integrated with the overall contractor organization  
• Include job titles and job functions, roles and responsibilities of the Key Staff, and staffing levels  
• Disclose the planned use of another company or individual consultant with which the contractor will contract to perform the services described in this RFP  
• Include a resource calendar describing the staff required for each phase of the project, if the staff will be on or off-site and the allocation percent  
• Provide a communication plan for managing secure communications between onsite and offsite staff  
• Describe the expected interaction between contractor teams and State staff  
• Describe retention strategies and plans to minimize the impact of personnel changes throughout the life of the contract |
| STAF | 2  | The contractor shall provide and retain qualified staffing at levels necessary to ensure successful implementation of the system, as well as support for the system through the life of the contract as bid.                                                                                                             |                      |                                                             |
| STAF | 3  | The contractor shall provide the following Key Staff during all Implementation Phases:  
• Project Executive  
• Project Manager  
• Solution Architect  
• Data Manager  
• Interface Manager  
• Testing Manager  
• Security Manager  
• Knowledge Transfer and Training Manager |
| STAF | 4  | The contractor shall adhere to the following general requirements for Key Staff:  
• The contractor shall have selected a Project Executive and have that individual under the contractor’s employ at the time the proposal is submitted  
• The contractor must employ all Key Staff or must have a written, legally binding commitment from them to join the contractor’s organization by the beginning of the contract start date  
• The contractor must commit Key Staff named in the proposal to the project from the contract signing date and may not reassign Key Staff during the project, except in cases of resignation or termination, or unless the State has agreed in advance  
• The contractor must make Key Staff available after hours as required by the State |

71
<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• The contractor must ensure Key Staff are available as mutually agreed upon during applicable project phases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAF</td>
<td>5</td>
<td>Key staff required for Maintenance and Operations will be under the contractor’s employ at least three months prior to the beginning of those project periods.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAF</td>
<td>6</td>
<td>The contractor shall obtain prior written consent of the State before Key Staff and other proposed project personnel can be reassigned or replaced.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAF</td>
<td>7</td>
<td>The contractor shall submit to the State the resumes of replacement candidates for Key Staff and provide the State an opportunity to interview and accept potential replacements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAF</td>
<td>8</td>
<td>The contractor shall name a temporary replacement acceptable to the State within five (5) calendar days of the date a Key Staff position becomes vacant.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAF</td>
<td>9</td>
<td>The contractor shall ensure a permanent replacement is working on the project within thirty 30 calendar days of the date a Key Staff position becomes vacant.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAF</td>
<td>10</td>
<td>The contractor shall obtain State approval prior to reducing staffing and skill levels.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAF</td>
<td>11</td>
<td>The contractor shall increase staffing levels if requirements or standards are not being met, based on the discretion of the State.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STAF</td>
<td>12</td>
<td>The contractor shall ensure the Key Staff meet the following qualifications during the life of the contract.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| STAF | 13 | Key Staff Qualification - Project Executive  
Minimum of eight (8) years of health and human service experience, leading and directing large scale system implementation projects. Senior executive capable of making binding decisions on behalf of the organization. |                     |                                                             |
| STAF | 14 | Key Staff Qualification - Project Manager  
PMP or equivalent certification or a minimum of ten (10) years of experience on similar scale projects. Minimum of five (5) years of end to end eligibility related system requirements, design, implementation and scope management experience including the management of one (1) eligibility systems design and development project similar in size and scope to this project. |                     |                                                             |
| STAF | 15 | Key Staff Qualification - Implementation Manager  
Minimum of five (5) years of implementation/change management experience in project management on assignments similar in size and scope to this project. Minimum of three (3) years of eligibility systems experience. Experience to include proven management skills including requirements gathering and traceability, change management, training, rollout, and field operations. A bachelor’s degree in business management or a related field or equivalent years of experience is required. |                     |                                                             |
<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant</th>
</tr>
</thead>
</table>
| STAF | 16 | **Key Staff Qualification - Data Manager**  
Minimum of five (5) years of data management, data migration and conversion experience on assignments similar in size and scope to this project. At least three (3) years experience in the conversion of large scale eligibility data. Data management experience includes (1) implementing complex data architecture infrastructures, preferably in the Health and Human Services environments and (2) data modeling and architecture, including expertise knowledge in metadata standards, SQL/PL/SQL, XML standards and middleware, data transfer standards, and web-based architecture. |                       |                                                          |
| STAF | 17 | **Key Staff Qualification - Interface Manager**  
Minimum of four (4) years of experience in system integration, messaging modules and interface development is required. A bachelor’s degree in information system engineering or related field, or equivalent years of experience is required. |                       |                                                          |
| STAF | 18 | **Key Staff Qualification - Testing Manager**  
Minimum of three (3) years experience conducting various test phases and leading teams through complex system test scenarios for a large scale government eligibility entity. |                       |                                                          |
| STAF | 19 | **Key Staff Qualification - Security Manager**  
Minimum of three (3) to four (4) years combined IT and security work experience with a broad exposure to infrastructure/network and multi-platform environments. Experience should include familiarity with technical and risk assessment techniques, tools and practices, and experience working with Federal security and privacy mandates. CISSP or CISA certification and proficiency with encryption, security within application development, change control, authentication/role-based security, and general holistic security practices. A bachelor’s degree in IT or similar field, or equivalent years of experience is required. |                       |                                                          |
| STAF | 20 | **Key Staff Qualification - Knowledge Transfer and Training Manager**  
Minimum of four (4) years experience in developing and delivering training to information system end users and system administrators. Experience includes developing training plan, curriculum, materials and assessment instruments and protocols; organizing training team and coordinating training team activities; developing solution documentation in its many forms to meet the needs of various recipients. |                       |                                                          |
| STAF | 21 | **Key Staff Qualification - Solution Architect**  
Minimum of five (5) years experience in system implementations where the resource has been responsible for ensuring the solution’s configuration meets client |                       |                                                          |
<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>requirements. Experience includes leading requirements elaboration and specification definition activities.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| STAF| 22 | The contractor shall adhere to the following general requirements for all staff:  
• The contractor must comply with all federal and State requirements concerning fair employment, employment of the disabled, and the treatment of all employees without regard to race, color, religion, national origin, or physical disability  
• The contractor must follow all federal and State laws regarding Social Security registration and legal work status of all staff employed or contracted by the contractor or subcontractor  
• All staff employed or contracted by the contractor or by any subcontractors working on the system must have a criminal background check completed using State-accepted criteria prior to project participation, and periodically as required by the State, with results submitted to the State for review. The background checks must be fingerprint-based and performed by the State of South Dakota with support from the State’s law enforcement resources. |                      |                                                             |
| STAF| 23 | The contractor shall provide the following information regarding subcontractors.  
• Subcontractors name and address  
• Subcontractors qualifications  
• Tasks the subcontractor will perform  
• The estimated percentage of total contract dollars for each subcontract  
• Plan for managing subcontractors  
Subcontractors are those that are employed and managed by the contractor, who have responsibilities of the project. The State reserves the right to prior accept all subcontractor(s) and their work locations. |                      |                                                             |
<p>| <strong>Assurances</strong>                                                                                                                                  |                      |                                                             |
| ASU | 1  | No offshoring of any business function or information technology service shall be allowed post-implementation of the replacement solution. Offshoring is hereby defined as the relocation, by a company, of (1) a business process from one country to another—typically an operational process, such as manufacturing, or supporting processes, such as accounting or (2) the outsourcing of technical and administrative services from outside the home country (&quot;offshore outsourcing&quot;), by means of internal (captive) or external (outsourcing) delivery models. |                      |                                                             |
| ASU | 2  | The contractor shall commit to stay continuously informed of all changes to program, information management and reporting regulations and sub regulatory guidance that HHS and the State issue and promulgate with regards to in-scope programs and proactively propose optimal approaches for addressing said changes. |                      |                                                             |</p>
<table>
<thead>
<tr>
<th>Ref</th>
<th>ID</th>
<th>Requirement Description</th>
<th>Compliant: Yes or No</th>
<th>If no, elaborate on level of effort required to be compliant.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>This assurance is aimed at achieving continual compliance with all applicable requirements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Operations and Hosting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HOST</td>
<td>1</td>
<td>If bid type is contractor-hosted, the contractor shall host, maintain, and operate South Dakota’s solution within the continental United States of America.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HOST</td>
<td>2</td>
<td>The contractor shall be responsible for hosting all systems during the DDI Period as required by the project.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HOST</td>
<td>3</td>
<td>The solution shall be hosted in a Tier III data center.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HOST</td>
<td>4</td>
<td>The contractor shall propose, specify, implement and support as many environments or instances within each environment type as necessary to fully support the design, construction, delivery, operation and ongoing maintenance of the solution as prescribed in this RFP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HOST</td>
<td>5</td>
<td>The contractor shall provide a System Operations, Maintenance, Support and Transition Plan for transitioning the production environment to the State of South Dakota’s Data Center, or another data center of the State's choosing, if so directed by the State.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Optional Scope of Work – Prior Authorization Professional Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAPS</td>
<td>1</td>
<td>The contractor shall provide qualified staff to support prior authorization professional services that includes at a minimum:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Prior Authorization Manager</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Primary contact for DMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Responsible for coordination of all prior authorization professional services related activities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Clinical Review Staff</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Licensed registered nurses (RNs) and licensed practical nurses (LPNs)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Licensed in the State of South Dakota</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Knowledge and experience using InterQual or Milliman criteria</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Administrative Staff</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Support the prior authorization professional services operations non-clinical tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Medical Director (if in scope)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Support appeals of denied requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Licensed in the State of South Dakota</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Knowledge and experience with nationally recognized, evidence based, clinical guidelines for determining medical necessity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ref</td>
<td>ID</td>
<td>Requirement Description</td>
<td>Compliant: Yes or No</td>
<td>If no, elaborate on level of effort required to be compliant.</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-----------------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>PAPS</td>
<td>1.02</td>
<td>Maintain sufficient staff to manage prior authorization professional services in order to meet and maintain compliance with service level requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAPS</td>
<td>1.03</td>
<td>Adhere to all general staffing requirements included in Attachment C, Reference ID STAF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAPS</td>
<td>2</td>
<td>Hours of Operation/Availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAPS</td>
<td>2.01</td>
<td>Provide prior authorization support Monday – Friday 8:00 – 6:00 Central, excluding State holidays.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAPS</td>
<td>2.01</td>
<td>Be accessible telephonically to DMS staff during hours of operation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAPS</td>
<td>3</td>
<td>Service Levels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAPS</td>
<td>3.01</td>
<td>95% completion of clean prior authorization requests within 3 days</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAPS</td>
<td>3.02</td>
<td>98% prior authorization determination accuracy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Modernizing South Dakota’s System for Prior Authorization, Utilization and Care Management

The South Dakota Department of Social Services (DSS) has a clear vision for modernizing its information infrastructure in order to streamline the operations of its public programs, improve services for recipients and achieve greater cost effectiveness. A major goal toward this end is acquiring a system to support the DSS operations that review, authorize, monitor and coordinate the provision of appropriate services to South Dakota Medicaid recipients by providers, both in South Dakota and other states. Prior Authorization is a core function within utilization management and a priority function to be supported by the System that DSS is seeking to acquire. Additional supports that are desirable include a gamut of utilization management activities and care management processes.

The new Utilization Management/Prior Authorization and Care Management system (System) to be acquired will be used by the Division of Social Services and interface and support these functions conducted by other agencies/divisions. The System will support functions to approve, monitor and support the provision of specific services that are requested and provided by participating Medicaid providers. These are functions that currently require extensive, manual efforts and often involve slow, outdated IT supports. The desired System will be used by providers, internal agency/department staff and contractors (i.e., the Foundation for Medical Care), and Medicaid recipients. This desired IT solution will enable optimized work flows, improved access to data, more powerful analytics, and the ability for providers, DSS and clients to interact more efficiently and effectively.

Acquiring the best technology solution to support South Dakota Medicaid involves considering the functionality required to support the range of day-to-day “business” for which the participating entities are accountable. The following use cases are a sampling of common scenarios for how the System will be used to carry out required business processes. Potential System vendors must be able to demonstrate that their product(s)/service(s) supports the activities outlined in this document. However, please note that:

- These use cases are illustrative and do not encompass all the detailed System requirements. They should be considered along with the detailed functional and technical requirements matrices attached to the RFP. These constitute a more complete list of desired system functionality and reflect agency input into what they desire from the System solution.
- The focus of these use cases is to highlight core agency and interagency functionality that will be required for information capture, information sharing and collaboration within and across programs related to the provision of services supported by each agency.
- A deeper dive into specific program workflows is expected to occur after a vendor is selected, as part of System configuration processes.

Prior Authorization, Utilization and Care Management System USE CASES

The use cases in this document illustrate major functionality that the System to be acquired is expected to provide. These scenarios illustrate different aspects of where and how prior authorization, utilization and care management occur.

Several cross-cutting assumptions apply across all use cases:

1. The System will need to integrate information from various agency record systems, DSS MMIS and provider platforms, ideally being able to accept requests and information submissions directly from provider EHR platforms.
2. The System will be capable of multiple modes of communication including electronic, email, portal, and hard copy.
3. The System will have the capability to upload and attach medical records that are retrievable as a permanent part of a case file.
4. The System will support workflows by enabling information capture and sharing among diverse providers, agency and community-based personnel and the Medicaid Recipient.
5. The System will have configurable business rules to support incremental levels of review involving automated decisions, and reviews by designated agency reviewers and qualified health care professionals.
o The System will optimize use of structured data including dropdown boxes with common responses from which to choose, combined with free text fields.
o The System will be able to imbed various templates or “forms” for different types of PA requests.

6. The System will be expected to support first, second and third levels reviews, with the ability to configure which types of requests require which levels of review.
o A “first level review” is that conducted by the System to confirm that a request is complete with required forms and documentation, and as appropriate, auto-adjudicate a PA request to approve or deny.

7. The System will support workflows with automated referrals and scheduling, as well as tracking, notifications and other timeliness/productivity supports.

8. Notifications issued by the System can be configured to include standard language regarding contact information, requests for reconsideration, and complaint, grievance and appeal processes.

9. All documentation of client information and PHI in the System will be secure and follow all necessary HIPAA and consent laws and regulations.

10. User access/roles in the System will govern who is able to see what information about Medicaid Recipients.

USE CASE #1: PRIOR AUTHORIZATION REQUEST FOR DURABLE MEDICAL EQUIPMENT (DME)

Mobility devices are covered for eligible Medicaid recipients with a limitation that impairs their ability to participate in one or more mobility related activities of daily living, and whose limitations can’t be resolved by use of an alternative device such as cane or walker. The DSS Prior Authorization Manual specifies a set of criteria for non-covered wheelchair related services and those requiring prior authorization, but also outlines in detail numerous criteria that must be met (along with billing codes to be used) to authorize various types of wheelchairs, accessories, repair and whether wheelchairs are purchased or rented. (See South Dakota Medicaid Prior Authorization Manual Specialty Mobility Devices pages 64-77)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>System Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>A request is received to provide a power wheelchair for a Recipient with a diagnosis of multiple sclerosis. A determination is made that a PA request is required for the service/DME requested. All information required to process the PA request is compiled to enable a review and determination. • If incomplete, the request will be returned to the originator of the request. • If complete, the PA request is reviewed.</td>
<td>The System receives a request through the provider portal, date and time stamps the electronic request, then verifies: • Recipient Medicaid ID # and eligibility • Provider Medicaid ID # and participation The System verifies: • The service codes in the PA request form are subject to PA. • Whether the PA request is for a rental or purchase • Whether the request is for repair or a new wheelchair The System accesses claims information to verify • Relevant diagnoses that make the Recipient potentially eligible for a wheelchair • Whether the mobility device request meets criteria specified in the Medicare list of DME items subject to a face to face encounter with a physician o If so, verifies claims data to confirm that a face to face visit has occurred prior to the PA request The System verifies completeness of the PA request, including data elements and documentation required to process the DME PA request: • A PA form, an e-signed Certificate of Medical Necessity, and e-signed script</td>
</tr>
</tbody>
</table>
### Scenario

- The required Codes indicating the specific nature of the DME being requested
- If a quote for the wheelchair being requested has been provided
- If a RESNA certification has been provided if custom seating is being requested.
- Whether a primary payer has issued a PA for the requested mobility devise/service that will deem the approval
- Whether required documentation is attached.

If the System cannot verify that the minimum required data elements and attachments are present, then the request is returned to the originating source and status of the request as returned for inadequate information is recorded in the System.

The System searches claims and other relevant databases, including the utilization management database supported by the System, to verify medical diagnosis codes related to stage of multiple sclerosis and any relevant history of wheelchair rental, purchase and/or repair and whether criteria for approving the PA request have been met.

Based on all available documentation, the System generates one of possible actions:
- The System generates a preliminary approval of the PA request when all criteria have been met based on submitted forms and verified claims.
- The System generates a preliminary denial based on certain criteria not being clearly met and forwards the denial to a queue for a second level of review.

For PA requests referred for second level review, a reviewer examines the available information compiled by the System and either verifies that a denial is in order; approval is warranted, perhaps with conditions; or additional information is required before a determination can be made.

The appropriate reviewer opens the queue, pulls up the forwarded PA request and takes action which may include:
- The reviewer reviews the preliminary determination that the System generates, and if in agreement, makes an indication to that effect with a reason for approval or denial. The System then generates a notice to the provider.
- If the reviewer determines that the PA request is justified based on certain conditions, the reviewer indicates in the System that the PA request is approved and notes conditions in the appropriate fields. The System generates a notice to the provider that the PA request is approved, along with conditions as appropriate.
- If the reviewer has reason to request further information that clarifies the PA request, an indication is made in the System that the request is pended and the PA request to send to a queue of pending requests. The system begins tracking time to resolution.
  - The reviewer opens the pending queue, views the dashboard of relevant information about the PA request, and initiates contact with the provider and/or conducts additional research to further clarify whether a request should be approved or denied.
  - The System tracks if and when additional information that has been requested is received, notifies the reviewer and flags the reviewer at prescribed intervals to make sure the PA request is processed within time limits.
  - The reviewer opens and reviews the updated information, indicates a determination, and the System generates an appropriate notice to the provider.
**USE CASE #2: PA REQUEST FROM OUT OF STATE PROVIDER FOR INPATIENT PROCEDURE/HOSPITALIZATION**

Based on the distribution of its population and health care resources, South Dakota Medicaid recipients often seek inpatient and specialty health care services from providers in border states. South Dakota Medicaid policy requires preauthorization for all inpatient hospitalizations and most outpatient services that are provided more than 50 miles outside of the State, except in Bismarck, North Dakota. Prior authorization does not guarantee payment; a provider must be enrolled South Dakota Medicaid provider and submit a timely and accurate claim. Out of state providers not currently enrolled in South Dakota Medicaid but seeking to serve a South Dakota Medicaid recipient must first obtain prior authorization and provide the service before their enrollment as a South Dakota Medicaid provider can be completed. *(See South Dakota Medicaid Prior Authorization Manual Out-of-State Services page 54)*

<table>
<thead>
<tr>
<th>Scenario</th>
<th>System Functionality</th>
</tr>
</thead>
</table>
| A request is received from an out of state hospital to authorize a surgical procedure and inpatient stay for a South Dakota Medicaid recipient. | The System receives a request through the provider portal or directly from the provider’s EHR, date and time stamps the electronic request, then verifies:  
  - Recipient Medicaid ID # and eligibility:  
    - If exempt aid category, Medicaid primary, pregnancy only, private health insurance  
    - Provider Medicaid ID # and participation  
      - Is the requesting provider a South Dakota PCP or specialist, or the out of state hospital?  
      - Is the requesting provider enrolled as a South Dakota Medicaid provider?  

  If the requesting hospital is not currently enrolled as a South Dakota Medicaid provider, the System will contact the DSS provider file to verify whether the provider has previously been enrolled, then flag the request and route it to a reviewer for follow up with the provider, including a notification informing the provider about conditions required for payment to be made if a prior authorization is approved i.e., SD enrollment and payment policies.  

  The System runs business rules against the information provided in the PA form submitted by the provider and verifies:  
  - The service codes in the PA request form are subject to PA  
  - Based on the location of the provider, PA is required  
  - Whether the procedure is categorized as experimental and PA is required  

  If PA is not required, the System issues a notification to the provider.  
  The System verifies whether information is available to run business rules and determine whether prior authorization criteria are met, including whether:  
  - PA form is complete, with requested specialties/procedures identified  
  - Relevant and required clinical records are attached and/or verified via MMIS or the UM database  
  - The System checks the UM database to verify and access records of any prior PA requests  
  - If, as part of stepped care protocols, in-state consultations and/or services are required prior to authorization of out of state services, the System verifies record of an in-state consultation, diagnostics, treatment and relevant services having occurred prior to the new out of state consultation/service being requested. *(See Use Case #3)*
Scenario | System Functionality
--- | ---
A first level review is conducted, and a determination is made to approve, deny or forward the PA request for a second level of review. | After running business rules, the System makes an initial determination:
- Required criteria are met and the PA request is approved.
- All required criteria cannot be fully verified, and a second level review is required.

If approved, the System generates a notification to the provider. If criteria specify a specific length of stay, this information is included in the notification and the System flags the case for concurrent review and potential re-authorization at a certain date.

If a second level review is required, the PA request is forwarded to a queue for second level review. The appropriate reviewer (RN) opens the PA request from the queue, reviews the dashboard of relevant information compiled by the System and makes one of several possible determinations. (See Use Case #1)
- The reviewer will consider information provided by the provider to justify the PA request and note any special circumstances.
- If the procedure is experimental the reviewer will:
  - Note whether additional supporting information is required from the requesting provider and indicate what information is needed as part of the notification to the provider that the System will generate.
  - Forward the PA request to a designated clinical specialist for 3rd level review.

Based on business rules, the System will flag the case for concurrent review on a certain timeframe.
- A designated RN will open the case from the queue.
- The System will display whether any information has been received from the hospital regarding discharge or transfer.
- The RN will contact the hospital to verify Medicaid recipient status and discharge planning and/or any potential for the need to authorize additional length of stay.
  - The reviewer will record notes in the Recipient’s record.
  - The System will capture updated LOS and flag for re-review.

The reviewer will take action in the System to:
- Preauthorize an additional length of stay and flag the case for ongoing concurrent review and/or refer the case for care management
  - The Recipient’s record will be updated with assignment to care management.
  - The System will send the case to care management queue.
  - A care manager will open and review dashboard of information regarding Recipient status and proceed with care coordination activities.

**USE CASE #3: VALIDATING STEPPED CARE PRIOR TO AUTHORIZATION OF TREATMENT**

According to South Dakota Medicaid policy, prior to authorizing certain treatments and procedures, there must be evidence that other more conservative evidence-based treatments have been tried and failed and that Medicaid recipients can benefit from the proposed treatment. Examples of such procedures include Botox for treatment of migraine headaches, breast reduction, bariatric surgery, and liver transplants. Required documentation would include information about history and outcomes of medication trials.
<table>
<thead>
<tr>
<th>Scenario</th>
<th>System Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>A request is received for prior authorization of bariatric surgery</td>
<td>The System verifies recipient and provider Medicaid eligibility and enrollment. <em>(See previous Use Cases).</em></td>
</tr>
<tr>
<td>After eligibility is determined, a first level system review determines whether required information is complete, and a second level review can be conducted.</td>
<td>If the PA request is for follow-up adjustments to a previously approved lap band/gastric banding procedure, the System verifies that the PA request is from the same surgeon or partner in the same practice who performed the original surgery, which is required by DSS protocol. If not, the request is returned to the provider with an appropriate notification. The System reviews the request form and whether all required fields are complete and required documentation relevant to bariatric surgery has been provided.</td>
</tr>
<tr>
<td>A DSS reviewer conducts a second level review, examining the information provided as part of the PA request in order to make a preliminary determination to approve, deny or pend a request for further information. A clinician with appropriate expertise (e.g., Medical Director, or Behavioral Health professional) conducts a third level review to verify a recommendation to approve or deny a PA request or</td>
<td>Based on configured business rules, the System will review the structured data provided and access and verify information contained in the MMIS and/or UM database, including diagnoses, lab data and other relevant medical reports relative to the pre-requisites in the DSS bariatric surgery protocol.</td>
</tr>
<tr>
<td></td>
<td>o BMI over 40, and age</td>
</tr>
<tr>
<td></td>
<td>o Diagnostic/claims codes for other systemic illness (CHF, HTN, CVI, hypoxemia, Type II diabetes, sleep apnea, drug/alcohol abuse, tobacco use</td>
</tr>
<tr>
<td></td>
<td>The System will apply business rules to determine whether evidence exists of pre-requisite non-surgical interventions required by the DSS UM bariatric surgery protocol.</td>
</tr>
<tr>
<td></td>
<td>o Physician supervised weight loss program</td>
</tr>
<tr>
<td></td>
<td>o Dietician consultation</td>
</tr>
<tr>
<td></td>
<td>o 4 consecutive visits with physician/care team that occurred with the 12 months prior to the PA request</td>
</tr>
<tr>
<td></td>
<td>If certain core components of the PA request are missing, the request will be returned to the Provider with a notification specifying the reason and requesting follow-up to forward a complete PA request.</td>
</tr>
<tr>
<td></td>
<td>If the PA request is determined to be complete and ready for second level review, it is sent to the appropriate queue. From the queue, a second level reviewer (e.g., RN) reviews the PA request checklist that the System provides as a “dashboard” of the PA request status, then conducts a more detailed review of certain pre-requisites for the surgery. These include:</td>
</tr>
<tr>
<td></td>
<td>Review of psychological assessment</td>
</tr>
<tr>
<td></td>
<td>Review of notes documenting the medical appropriateness of the surgery based on one of the required conditions being present, as outlined in the DSS Prior Authorization Manual (page 9).</td>
</tr>
<tr>
<td></td>
<td>The third level reviewer opens his or her queue, reviews the second level review recommendations and supporting record, and documents his/her determination</td>
</tr>
<tr>
<td></td>
<td>If agreeing with 2nd level review, notification of approval sent to provider</td>
</tr>
<tr>
<td></td>
<td>If PA request is denied, notification sent to provider including information regarding how to request a reconsideration.</td>
</tr>
</tbody>
</table>
## USE CASE #4: AUTHORIZING AND MONITORING PLACEMENT IN PSYCHIATRIC RESIDENTIAL TREATMENT FACILITIES

Psychiatric Residential Treatment is a placement for youth under the auspices of the DSS, Child Protective Services (CPS), who are unable to function in a family or group setting due to significant mental health challenges and require intense therapies in a highly structured and contained environment. Treatment is covered for Medicaid eligible youth under age 18 based on conditions being met, with the expectation that services to be provided will improve/stabilize the individual’s emotional and behavioral condition. A two-part review process is required to determine if a youth meets criteria for placement in Psychiatric Residential Treatment Facility (PRTF).

<table>
<thead>
<tr>
<th>Scenario</th>
<th>System Functionality</th>
</tr>
</thead>
</table>
| A referral is received (from a school, CPS, Dept of Corrections, Division of Behavioral Health, a provider or parents) recommending that a youth be placed in a PRTF and requesting DSS to approve placement | The referring entity completes and electronically submits the required form through either a recipient or provider portal or other route, and supporting information is uploaded to the System. In some cases, a referring entity may consult with the DSS PRTF coordinator and the coordinator will initiate the PA request. If a child is not currently Medicaid eligible, the PA request is still processed pending either the Recipient’s Medicaid eligibility determination or a provider’s enrollment. If a provider judges that an emergency placement is required, the youth will be admitted and the processes for certifying the stay will occur on the first working day following admission to the PRTF. The System verifies recipient and provider Medicaid eligibility and enrollment. (See previous Use Cases). Upon receipt of the request, a first level System review occurs to verify that information required for a State Review Team consideration of the request is complete. The System runs business rules and accesses the claims system to pull records including Medicaid claims history and verify that required documentation has been provided. Information required includes:  
  - Social history including past and current behaviors  
  - Psychological evaluation and diagnosis completed within the past 12 months  
  - Report from the school district summarizing the youth’s behaviors, if available  
  - Summary of outpatient services provided to date with outcomes and recommendations  
  - Alcohol and drug screening assessment, if available. The System notifies the PRTF coordinator that a request is pending. The coordinator opens the file and reviews information that the system has compiled to verify the adequacy of information provided. If information is missing, a notification is sent to the referring entity specifying information that is outstanding. This could include sending a link to parents through which they can provide information needed to complete the request. If all information is present, the Coordinator uses the System to schedules a review for the next available Monday morning meeting and sends a notification to the State Review Team members about receipt of a request and scheduled review. |
The DSS State Review Team meets to review the case (second level review) and make a recommendation about the appropriateness of the placement. A third level review then occurs by the South Dakota Foundation for Medical Care (SDFMC) to evaluate medical necessity and verify recommendations by the State Review Team, including time period for the placement.

The State Review Team consists of representatives from Departments of Social Services, Corrections, Human Services, and Education. In preparation for the meeting, members of the State Review Team access the System to review the Recipient's file and materials relevant to the PRTF request. During the meeting, recommendations regarding placement are recorded with notes relevant to the discussion. Possible determinations include:

- Yes/placement does not appear to be warranted, with a recommenced Length of Commitment based on needs.
- No/placement does not appear to be warranted.

The System sends an electronic notification to the SDFMC system about a referral for PRTF evaluation.

- The SDFMC system records the PA # that is tied to DSS MMIS/claims and alerts its reviewer.

A SDFMC reviewer completes a review of medical necessity criteria using MSG/InterQual criteria and enters result into SDFMC database.

Results may include:

- Verification of the State Review Team/second level review recommendations and authorization for placement over a specific time period.
  - The System forwards a notification to the referring provider and recipient's representative.
  - The System flags the case in MMIS for approved length of stay e.g., 30 days for evaluation, 60 days, or longer.
- Request for additional information prior to making a recommendation.
- Disagreement that the placement is medically necessary and a denial of the request for placement.

The System generates a notification to all parties in the format requested (information maintained in provider file and incorporated into business rules), along with information regarding how to file a request for reconsideration. Notification may include via portal, email, fax, hard copy.

Requests for continued stay are submitted to the System with an appropriate form and supporting information.

The System will conduct a first level review to determine if required information is present to enable the assessment to proceed.

- If so, the request will be forwarded directly to the SDFMC for consideration.
- If not, a notification will be sent to the referring provider requesting missing information before the review can be conducted.

A SDFMC reviewer will be notified about the review request and access the request and materials in the System.

- According to SDFMC protocols, a Reviewer will assess whether need remains for extended stay in a PRTF or whether a lower level of placement is now warranted.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>System Functionality</th>
</tr>
</thead>
</table>
| The DSS State Review Team meets to review the case (second level review) and make a recommendation about the appropriateness of the placement. | The State Review Team consists of representatives from Departments of Social Services, Corrections, Human Services, and Education. In preparation for the meeting, members of the State Review Team access the System to review the Recipient’s file and materials relevant to the PRTF request. During the meeting, recommendations regarding placement are recorded with notes relevant to the discussion. Possible determinations include:  
  - Yes/placement does not appear to be warranted, with a recommenced Length of Commitment based on needs.  
  - No/placement does not appear to be warranted.  
  The System sends an electronic notification to the SDFMC system about a referral for PRTF evaluation.  
    - The SDFMC system records the PA # that is tied to DSS MMIS/claims and alerts its reviewer.  
    A SDFMC reviewer completes a review of medical necessity criteria using MSG/InterQual criteria and enters result into SDFMC database.  
    Results may include:  
      - Verification of the State Review Team/second level review recommendations and authorization for placement over a specific time period.  
        - The System forwards a notification to the referring provider and recipient’s representative.  
        - The System flags the case in MMIS for approved length of stay e.g., 30 days for evaluation, 60 days, or longer.  
      - Request for additional information prior to making a recommendation.  
      - Disagreement that the placement is medically necessary and a denial of the request for placement.  
        The System generates a notification to all parties in the format requested (information maintained in provider file and incorporated into business rules), along with information regarding how to file a request for reconsideration. Notification may include via portal, email, fax, hard copy.  
        Requests for continued stay are submitted to the System with an appropriate form and supporting information.  
        The System will conduct a first level review to determine if required information is present to enable the assessment to proceed.  
          - If so, the request will be forwarded directly to the SDFMC for consideration.  
          - If not, a notification will be sent to the referring provider requesting missing information before the review can be conducted.  
            A SDFMC reviewer will be notified about the review request and access the request and materials in the System.  
              According to SDFMC protocols, a Reviewer will assess whether need remains for extended stay in a PRTF or whether a lower level of placement is now warranted. |
**Scenario** | **System Functionality**
---|---
The determination will be noted in the SDFMC system and forwarded to the referring provider and State Certification Team.

**USE CASE #5: AUTHORIZING BEHAVIORAL HEALTH/SUBSTANCE USE TREATMENT AND PROGRAMS**
Currently, the utilization management responsibilities related to behavioral health are divided between DSS divisions – the Division of Medical Services (DMS) and Division of Behavioral Health (DBH) – with support from the South Dakota Foundation for Medical Care (SDFMC), an external entity under contract to DSS. In addition to manual efforts by agency reviewers, UM/PA and care management activities conducted by each of these entities are supported to some extent by separate systems i.e., DMS uses an access database and the MMIS system, DBH uses the STARS provider network platform, and SDFMC utilizes its information system platform and interfaces with the DSS MMIS to acquire PA case numbers, then to share determinations and status reports.

These entities share a vision for leveraging the System’s UM/PA and CM functionalities to streamline and strengthen their UM/PA efforts related to substance abuse treatment and other “high intensity” behavioral health services as well as other care management efforts. Examples include expediting participation in appropriate, evidence-based programs by DBH clients (e.g., justice involved clients), and where appropriate, providing additional expert review and use of recognized, external standards to substantiate decisions about medical necessity. The following scenario illustrates several desired functionalities related to a client with behavioral health needs and services.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>System Functionality</th>
</tr>
</thead>
</table>
| A provider requests authorization for intensive methamphetamine treatment services. A first level System review is conducted to determine if all required elements are present in order to issue an approval. A second level review is conducted to authorize treatment services. | The provider accesses the Provider Portal to obtain information regarding covered benefits and services. The System receives a request form submitted through the provider portal. The System determines Recipient and provider eligibility (see use case #1). The System reviews data fields and attestations included in the authorization form submitted by the provider. - The System confirms that the request is complete with required information e.g., appropriate diagnoses, and validates past substance use treatment in the MMIS claims database. - Business rules identify that second level review is requires to authorize these services. A behavioral health reviewer opens the request from the queue and reviews the profile of relevant information compiled by the System that corresponds to the protocol for approving this treatment. - The reviewer verifies components of the protocol checklist that the System has auto-adjudicated and reviews relevant notes, attachments and health record. - Decision supports in the System based on the protocol for authorizing treatment guide the reviewer as to whether the request can be approved based on information contained in the health record. o If the behavioral health reviewer can authorize the request, this is done, the request is approved, and a notification generated and sent to STARS, which notifies the provider, including information regarding the approved treatment time period. - If the System decision supports guide the reviewer to determine that an additional level of clinical review is required, the reviewer forwards the request to the contracted external review entity (e.g., SDFMC) through an interface between the System and the SDFMC platform. (* Currently the
Scenario | System Functionality
--- | ---
A third level review is conducted to determine if requested treatment is authorized. | An appropriate clinical specialist opens and reviews the request and associated documentation and any issues that are flagged from the second review. The review uses his/her clinical judgement to make a determination, documenting notes and decision in the System and generating notification to DSS MMIS and the requesting provider. Potential options supported by the System include:

- The request is authorized for a certain time period based on protocol and business rules or denied. In either circumstance, rationale is provided with both structured data (checkbox) and free text added by the reviewer.
- Additional information is needed and requested. Based on protocol and business rules, the notification could include a message regarding if and how communication between reviewer and provider will occur to clarify outstanding questions (e.g., provider will be contacted).
- The request is approved, and based on factors in the case, the case is flagged for additional utilization care management and a request sent by the System to care management queue.
- MMIS is updated.

Near or after completion of inpatient treatment, participation in follow up Medication Assisted Treatment (MAT) will benefit the Recipient’s Recovery and return to the workforce. | If the Recipient has been assigned to a care manager, the System flags the care manager to review the status of the case and need for additional services post discharge from inpatient treatment.

- The care manager accesses System information regarding the “best practice” protocol for methamphetamine recovery and available SD resources, then contacts the Recipient and his providers regarding available and appropriate options.
- As agreed upon and documented in the Recipient’s file, the care manager completes a MAT authorization in the System. The System updates MMIS.
- On an ongoing basis, the System will flag the care manager to review the status of treatment.
  - The reviewer will open the file and the System will display a profile of current data including RX and provider utilization.
  - Using this information, the care manager will contact provider and member as appropriate.

If the Recipient is not in DSS care management, the Provider submits a request for program participation.

- The Provider accesses, completes and submits a request form via the Provider portal or STARS.
- System receives and conducts a first level review based on program referral protocols and information submitted.
- As appropriate, the System forwards the request to an appropriate DSS agency department/staff member for second level review.
- The System generates a notification to the program/provider authorizing participation, timeframe and required reporting.
USE CASE #6: MONITORING AND AUTHORIZING SERVICE LIMITS

Across DSS agencies, certain services do not require pre-authorization but are subject to service limits. In some cases, service limits can be extended if requested and approved. The System is expected to streamline the end to end process for providers and agencies, reducing unnecessary preauthorization requests and expediting timely adjudication of any requests for additional services beyond benefit limits. An example illustrated in this use case is mental health visits that extend beyond the coverage limit. This System functionality will also support the monitoring and authorization of other services, including EPSDT services for children.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>System Functionality</th>
</tr>
</thead>
</table>
| A mental health provider evaluates a new patient and determines that mental health treatment is needed. Near or at the end of service limits, the provider determines that the Recipient needs continuing services without disruption. If appropriate steps are taken to request prior authorization, additional services may be authorized. | The provider accesses information through the System portal to confirm benefit coverage and Recipient eligibility. The provider anticipates providing services within service limits, begins treatment and submits claims. The System tracks service utilization against service limits and provides updates to the Provider. The provider accesses the provider portal for information about requesting additional services. According to DSS policy (see SD Medicaid 2018 Pre-Authorization Manual page 47), a mental health provider must submit documentation and seek prior authorization of any service which will exceed the limits established by the department. If appropriate steps are taken to request prior authorization, additional services may be authorized. The provider has not previously submitted to the department the required PA documentation but out of concern for disrupting the Recipient’s treatment, the provider contacts the department and speaks to the appropriate behavioral health UM reviewer.  
  - Based on verbal review of information, the staff person authorizes the requested services but notes that verification of the verbal authorization enabling payment of claims for services will be contingent upon receiving required documentation.  
  The provider submits a prior authorization form to the System with attached documentation i.e., written treatment plan, diagnosis and planned treatment.  
  - The System conducts a first level review to determine that the request is complete with required documentation and routes the request to a review queue and specific reviewer (second level or third level i.e., SDFMC).  
  - The reviewer opens and reviews the request and documentation to determine that the additional services requested are justified based on the criteria specified in the PA Manual and UM protocol including:  
    - Consistent with recipient’s symptoms, diagnosis, condition or injury  
    - Recognized as prevailing standard consistent with generally accepted professional standards of the provider’s peer group;  
    - Responds to prevent death or disability, treat pain, injury, illness, and/or achieve physical or mental functioning etc.  
    - Not furnished primarily for convenience of the recipient or provider  
    - No other equally effective course of treatment available or suitable, which is more conservative or substantially less costly.  |
<table>
<thead>
<tr>
<th>Scenario</th>
<th>System Functionality</th>
</tr>
</thead>
</table>
| When the required information is received by the System, it flags the reviewer to open the file, review the documentation, and make a determination. Determinations may include: | When the required information is received by the System, it flags the reviewer to open the file, review the documentation, and make a determination.
- Additional services as requested are authorized. The reviewer verifies the previous verbal authorization in the System and the System updates MMIS and issues a notification to the provider.
- The case meets criteria for referral to care management for ongoing monitoring and care coordination. The reviewer verifies and refers, and the System sends to care management queue.
- Additional services are not authorized. The determination is noted in the System and a notification generated to the provider.
- Additional information must be submitted in order to authorize services. The System issues a notification to the provider with appropriate instructions, pends the request and flags the case for re-review. |

**USE CASE #7: LINKING DDD RECIPIENTS TO APPROPRIATE LEVELS AND SOURCES OF SUPPORT**

The Division of Developmental Disabilities (DDD) is seeking to expand an approach to authorizing programs and services that will achieve a “right sizing” i.e., the right supports are delivered to those most likely to benefit based on assessed need. At the same time, DDD is working to reduce access barriers to programs that will promote independence, autonomy and are cost effective. During 2019, DHS is implementing the Therap platform, starting with LTSS and eventually implementing it to support other HCBS/independent living support waiver programs. However, DDD is interested in using the DSS PA system to enhance eligibility determinations and ensure prerequisites are met by Recipients before they begin accessing services.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>System Functionality</th>
</tr>
</thead>
</table>
| A community agency working with a new DDD recipient and his family is requesting the Recipient’s placement in a setting that will provide an appropriate level of support. | The case worker accesses the DDD portal to review information regarding available levels of support in different settings and associated eligibility criteria and access an application/pre-authorization form.
A pre-authorization form is completed and submitted through the System’s DDD portal, providing required information that will be used to evaluate the extent to which the Recipient meets relevant criteria for various levels of support. Information will include but is not limited to:
- Client demographics
- Functional, cognitive, behavioral assessment findings
The System business rules generate a recommendation including:
- Types of supports required
- Appropriate setting e.g., ICF vs sharing living
- If there are outstanding issues requiring follow up, based on DDD eligibility protocols. |
| A first level System review is conducted to verify that required information has been submitted and if possible, make a recommendation regarding an appropriate setting. | The System generates a notification to DDD regarding the initial recommendation and resolve pending status of the preauthorization request.
- If there are no outstanding issues, DDD staff will direct the System notification to issue approval for the recommended level of care and setting accompanied by instructions regarding next steps. |
<p>| A second level review is conducted to verify recommendations and initiate follow up with Recipient. | |</p>
<table>
<thead>
<tr>
<th>Scenario</th>
<th>System Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>If there are outstanding issues, DDD staff will follow up with Recipient and Provider to clarify and potentially modify the recommendation and agree on a level of support/setting. When status of request is noted as verified by DDD, MMIS and Therap will be updated.</td>
<td><strong>USE CASE #8: ANALYSIS OF UTILIZATION AND COST DATA TO UNDERSTAND FINANCIAL LIABILITIES RELATED TO PRE-AUTHORIZED SERVICES</strong>&lt;br&gt;Robust analytics are critical for DSS and other agencies as part of overall accountability for the state’s public health and human services related expenditures. As part of its annual financial operations, DSS must account for all outstanding financial commitments under the Medicaid program. Ongoing analysis of utilization data is important for development of targeted policies and programs to optimize outcomes and contain costs. Additionally, the ability to collect and analyze data regarding certain pre-authorized but as not yet delivered services enables DSS to appropriately manage and report the budgetary implications of Recipient health trends and service utilization.</td>
</tr>
<tr>
<td>As part of its 4th quarter reporting, DSS is required to identify services authorized but not yet used as part of its overall budgetary accounting.</td>
<td>Based on input from DSS financial analysts, reporting templates are configured in the System. On a schedule to be determined, the System will support produce standardized and ad hoc reports requested by DSS analysts to analyze various factors related to Medicaid expenditures and project outstanding liabilities. The System’s analytic supports will enable examination of Medicaid utilization trends across services and populations including those that do and do not require pre-authorizations, and costs by type of pre-authorized service including:&lt;br&gt;• Analysis of historic pre-authorization and claims data to identify the expected scope and timeframe of services and claims for specific, known high-cost, open pre-authorized services.&lt;br&gt;• Identification of pre-authorizations considered to be &quot;open&quot; i.e., still in force, by type of service&lt;br&gt;• Projections of costs for services not yet delivered.</td>
</tr>
</tbody>
</table>
ATTACHMENT E – Future State Workflow

Purpose: The purpose of the prior authorization process is to determine medical necessity for appropriate claims payment.

<table>
<thead>
<tr>
<th>Member</th>
<th>Access Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Query System for info on PA policy/status</td>
</tr>
<tr>
<td></td>
<td>Submit required information</td>
</tr>
<tr>
<td></td>
<td>OK End</td>
</tr>
<tr>
<td></td>
<td>NO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Provider</th>
<th>Initiator through Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System receives electronic PA request</td>
</tr>
<tr>
<td></td>
<td>Recipient eligible?</td>
</tr>
<tr>
<td></td>
<td>Valid provider?</td>
</tr>
<tr>
<td></td>
<td>PA request complete?</td>
</tr>
<tr>
<td></td>
<td>Request returned for resubmission</td>
</tr>
<tr>
<td></td>
<td>Y Auto Adjudicate?</td>
</tr>
<tr>
<td></td>
<td>Y Send to Reviewer queue for PA determination</td>
</tr>
<tr>
<td></td>
<td>N Notify Provider</td>
</tr>
<tr>
<td></td>
<td>N Close</td>
</tr>
<tr>
<td></td>
<td>N Willing to enroll?</td>
</tr>
<tr>
<td></td>
<td>Y Send provider enrollment info/request to enroll</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Support Staff</th>
<th>Receive Faxed PA Request Form</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scan PA Request</td>
</tr>
<tr>
<td></td>
<td>Manual Notice Faxed to Provider</td>
</tr>
<tr>
<td></td>
<td>End</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reviewer: Registered Nurse (RN)</th>
<th>Open PA request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correctly Assigned?</td>
<td>PA Determination made</td>
</tr>
<tr>
<td>N Reassign</td>
<td>N Pended for additional review/guidance</td>
</tr>
<tr>
<td></td>
<td>Additional info/review/guidance?</td>
</tr>
<tr>
<td></td>
<td>Auto-deny after configured timeframe</td>
</tr>
<tr>
<td></td>
<td>System updates and acts on status of PA request</td>
</tr>
<tr>
<td></td>
<td>Provider notified via Portal and/or letter</td>
</tr>
<tr>
<td></td>
<td>Other UM and CM activities, tasks, and updates</td>
</tr>
</tbody>
</table>

End
The State hereby enters into a contract (the “Agreement” hereinafter) for consultant services with the Consultant. While performing services hereunder, Consultant is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

1. **CONSULTANT’S South Dakota Vendor Number is**.

2. **PERIOD OF PERFORMANCE:**
   A. This Agreement shall be effective as of MM/DD/YYYY and shall end on MM/DD/YYYY, unless sooner terminated pursuant to the terms hereof.

   B. Agreement is the result of request for proposal process, RFP #_____.

3. **PROVISIONS:**
   A. **The Purpose of this Consultant contract:**
      1. Does this Agreement involve Protected Health Information (PHI)?  YES ( )  NO ( X )
         If PHI is involved, a Business Associate Agreement must be attached and is fully incorporated herein as part of the Agreement (refer to attachment).

      3. The Consultant **will/will not** use state equipment, supplies or facilities.

   B. **The Consultant agrees to perform the following services (add an attachment if needed):**
      1. 

   C. **The State agrees to:**
      1. 

      2. Make payment for services upon satisfactory completion of services and receipt of bill. Payment will be in accordance with SDCL 5-26.

      3. Will the State pay Consultant expenses as a separate item?  YES ( )  NO ( X )
         If YES, expenses submitted will be reimbursed as identified in this Agreement.
D. Due to the subject matter of this Agreement, it requires the approval of the South Dakota Bureau of Information and Telecommunications ("BIT" hereinafter). The Consultant specifically agrees to the terms and conditions of the BIT Security Acknowledgement Form attached hereto as Exhibit A, the BIT supplementary contract clauses attached hereto as Exhibit B, the BIT Hosting, SaaS and Cloud Services State Technology Contract Template Terms attached hereto as Exhibit C and the Information Technology Security Plan (ITSP) attached hereto as Exhibit D, which Exhibits are collectively incorporated herein by reference and made a part hereof.

E. The TOTAL CONTRACT AMOUNT will not exceed $_________.

04/18
4. BILLING:
Consultant agrees to submit a bill for services within (30) days following the month in which services were provided. Consultant will prepare and submit a monthly bill for services. Consultant agrees to submit a final bill within 30 days of the Agreement end date to receive payment for completed services. If a final bill cannot be submitted in 30 days, then a written request for extension of time and explanation must be provided to the State.

5. TECHNICAL ASSISTANCE:
The State agrees to provide technical assistance regarding Department of Social Services rules, regulations and policies to the Consultant and to assist in the correction of problem areas identified by the State’s monitoring activities.

6. LICENSING AND STANDARD COMPLIANCE:
The Consultant agrees to comply in full with all licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance in which the service and/or care is provided for the duration of this Agreement. The Consultant will maintain effective internal controls in managing the federal award. Liability resulting from noncompliance with licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance or through the Consultant’s failure to ensure the safety of all individuals served is assumed entirely by the Consultant.

7. ASSURANCE REQUIREMENTS:
The Consultant agrees to abide by all applicable provisions of the following: Lobbying Activity, Byrd Anti Lobbying Amendment (31 USC 1352), Executive orders 12549 and 12689 (Debarment and Suspension), Drug-Free Workplace, Executive Order 11246 Equal Employment Opportunity, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, Title IX of the Education Amendments of 1972, Drug Abuse Office and Treatment Act of 1972, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Age Discrimination Act of 1975, Pro-Children Act of 1994, Hatch Act, Health Insurance Portability and Accountability Act (HIPAA) of 1996 as amended, Clean Air Act, Federal Water Pollution Control Act, Charitable Choice Provisions and Regulations, Equal Treatment for Faith-Based Religions at Title 28 Code of Federal Regulations Part 38, the Violence Against Women Reauthorization Act of 2013 and American Recovery and Reinvestment Act of 2009, as applicable; and any other nondiscrimination provision in the specific statute(s) under which application for Federal assistance is being made; and the requirements of any other nondiscrimination statute(s) which may apply to the award.

8. RETENTION AND INSPECTION OF RECORDS:
The Consultant agrees to maintain or supervise the maintenance of records necessary for the proper and efficient operation of the program, including records and documents regarding applications, determination of eligibility (when applicable), the provision of services, administrative costs, statistical, fiscal, other records, and information necessary for reporting and accountability required by the State. The Consultant shall retain such records for a period of six years from the date of submission of the final expenditure report. If such records are under pending audit, the Consultant agrees to hold such records for a longer period upon notification from the State. The State, through any authorized representative, will have access to and the right to examine and copy all records, books, papers or documents related to services rendered under this Agreement. State Proprietary Information retained in Consultant’s secondary and backup systems will remain fully subject to the obligations of confidentiality stated herein until such information is erased or destroyed in accordance with Consultant’s established record retention policies.

All payments to the Consultant by the State are subject to site review and audit as prescribed and carried out by the State. Any overpayment of this Agreement shall be returned to the State within thirty days after written notification to the Consultant.

9. WORK PRODUCT:
Consultant hereby acknowledges and agrees that all reports, plans, specifications, technical data, drawings, software system programs and documentation, procedures, files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, State Proprietary Information, as defined in the Confidentiality of Information paragraph herein, state data, end user data, Protected Health Information as defined in 45 CFR 160.103, and all information contained therein provided to the State by the Consultant in connection with its performance of service under this Agreement shall belong to and is the property of the State and will not be used in any way by the Consultant without the written consent of the State.
Paper, reports, forms, software programs, source code(s) and other materials which are a part of the work under this Agreement will not be copyrighted without written approval of the State. In the unlikely event that any copyright does not fully belong to the State, the State nonetheless reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, and otherwise use, and to authorize others to use, any such work for government purposes.

Consultant agrees to return all information received from the State to State’s custody upon the end of the term of this Agreement, unless otherwise agreed in a writing signed by both parties.

10. TERMINATION:
This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Consultant breaches any of the terms or conditions hereof, this Agreement may be terminated by the State for cause at any time, with or without notice. Upon termination of this Agreement, all accounts and payments shall be processed according to financial arrangements set forth herein for services rendered to date of termination.

11. FUNDING:
This Agreement depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for this purpose. If for any reason the Legislature fails to appropriate funds or grant expenditure authority, or funds become unavailable by operation of the law or federal funds reduction, this Agreement will be terminated by the State. Termination for any of these reasons is not a default by the State nor does it give rise to a claim against the State.

12. ASSIGNMENT AND AMENDMENTS:
This Agreement may not be assigned without the express prior written consent of the State. This Agreement may not be amended except in writing, which writing shall be expressly identified as a part hereof, and be signed by an authorized representative of each of the parties hereto.

13. CONTROLLING LAW:
This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota, without regard to any conflicts of law principles, decisional law, or statutory provision which would require or permit the application of another jurisdiction’s substantive law. Venue for any lawsuit pertaining to or affecting this Agreement shall be resolved in the Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

14. SUPERCESSION:
All prior discussions, communications and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement, and except as specifically provided herein, this Agreement constitutes the entire agreement with respect to the subject matter hereof.

15. IT STANDARDS:
Any software or hardware provided under this Agreement will comply with state standards which can be found at http://bit.sd.gov/standards/.

16. SEVERABILITY:
In the event that any provision of this Agreement shall be held unenforceable or invalid by any court of competent jurisdiction, such holding shall not invalidate or render unenforceable any other provision of this Agreement, which shall remain in full force and effect.

17. NOTICE:
Any notice or other communication required under this Agreement shall be in writing and sent to the address set forth above. Notices shall be given by and to the Division being contracted with on behalf of the State, and by the Consultant, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

18. SUBCONTRACTORS:
The Consultant may not use subcontractors to perform the services described herein without express prior written consent from the State. The State reserves the right to reject any person from the Agreement presenting insufficient skills or inappropriate behavior.
The Consultant will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Consultant will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance. The State, at its option, may require the vetting of any subcontractors. The Consultant is required to assist in this process as needed.

19. **STATE’S RIGHT TO REJECT:**
The State reserves the right to reject any person or entity from performing the work or services contemplated by this Agreement, who present insufficient skills or inappropriate behavior.

20. **HOLD HARMLESS:**
The Consultant agrees to hold harmless and indemnify the State of South Dakota, its officers, agents and employees, from and against any and all actions, suits, damages, liability or other proceedings which may arise as the result of performing services hereunder. This section does not require the Consultant to be responsible for or defend against claims or damages arising solely from errors or omissions of the State, its officers, agents or employees.

21. **INSURANCE:**
Before beginning work under this Agreement, Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement. The Consultant, at all times during the term of this Agreement, shall obtain and maintain in force insurance coverage of the types and with the limits listed below. In the event a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Consultant agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Consultant shall furnish copies of insurance policies if requested by the State.

   A. Commercial General Liability Insurance:
Consultant shall maintain occurrence-based commercial general liability insurance or an equivalent form with a limit of not less than $1,000,000 for each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this Agreement or be no less than two times the occurrence limit.

   B. Business Automobile Liability Insurance:
Consultant shall maintain business automobile liability insurance or an equivalent form with a limit of not less than $500,000 for each accident. Such insurance shall include coverage for owned, hired, and non-owned vehicles.

   C. Worker’s Compensation Insurance:
Consultant shall procure and maintain Workers’ Compensation and employers’ liability insurance as required by South Dakota law.

   D. Professional Liability Insurance:
Consultant agrees to procure and maintain professional liability insurance with a limit not less than $1,000,000.

   (Medical Health Professional shall maintain current general professional liability insurance with a limit of not less than one million dollars for each occurrence and three million dollars in the aggregate. Such insurance shall include South Dakota state employees as additional insureds in the event a claim, lawsuit, or other proceeding is filed against a state employee as a result of the services provided pursuant to this Agreement. If insurance provided by Medical Health Professional is provided on a claim made basis, then Medical Health Professional shall provide “tail” coverage for a period of five years after the termination of coverage.)

22. **CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:**
Consultant certifies, by signing this Agreement, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by the federal government or any state or local government department or agency. Consultant further agrees that it will immediately notify the State if during the term of this Agreement either it or its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.
23. **CONFLICT OF INTEREST:**
Consultant agrees to establish safeguards to prohibit employees or other persons from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Consultant expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.

24. **CONFIDENTIALITY OF INFORMATION:**
For the purpose of the sub-paragraph, “State Proprietary Information” shall include all information disclosed to the Consultant by the State. Consultant acknowledges that it shall have a duty to not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. Consultant shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this Agreement; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this Agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents or consultants except those who have agreed to obligations of confidentiality at least as strict as those set out in this Agreement and who have a need to know such information. Consultant is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. Consultant shall protect confidentiality of the State’s information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. State Proprietary Information shall not include information that (i) was in the public domain at the time it was disclosed to Consultant; (ii) was known to Consultant without restriction at the time of disclosure from the State; (iii) that is disclosed with the prior written approval of State’s officers or employees having authority to disclose such information; (iv) was independently developed by Consultant without the benefit or influence of the State’s information; (v) becomes known to Consultant without restriction from a source not connected to the State of South Dakota. State’s Proprietary Information shall include names, social security numbers, employer numbers, addresses and all other data about applicants, employers or other clients to whom the State provides services of any kind. Consultant understands that this information is confidential and protected under applicable State law at SDCL 1-27-1.5, modified by SDCL 1-27-1.6, SDCL 28-1-29, SDCL 28-1-32, and SDCL 28-1-68 as applicable federal regulation and agrees to immediately notify the State if the information is disclosure, either intentionally or inadvertently. The parties mutually agree that neither of them shall disclose the contents of the Agreement except as required by applicable law or as necessary to carry out the terms of the Agreement or to enforce that party’s rights under this Agreement. Consultant acknowledges that the State and its agencies are public entities and thus are bound by South Dakota open meetings and open records laws. It is therefore not a breach of this Agreement for the State to take any action that the State reasonably believes is necessary to comply with the South Dakota open records or open meetings laws. If work assignments performed in the course of this Agreement require additional security requirements or clearance, the Consultant will be required to undergo investigation.

25. **REPORTING PROVISION:**
Consultant agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to any person or property, or which may otherwise subject Consultant, or the State of South Dakota or its officers, agents or employees to liability. Consultant shall report any such event to the State immediately upon discovery.

Consultant's obligation under this section shall only be to report the occurrence of any event to the State and to make any other report provided for by their duties or applicable law. Consultant's obligation to report shall not require disclosure of any information subject to privilege or confidentiality under law (e.g., attorney-client communications). Reporting to the State under this section shall not excuse or satisfy any obligation of Consultant to report any event to law enforcement or other entities under the requirements of any applicable law.
26. AUTHORIZED SIGNATURES:
In witness hereto, the parties signify their agreement by affixing their signatures hereto.

______________________________                  __________________________
Consultant Signature                  Date

______________________________
Consultant Printed Name

______________________________                  __________________________
State - DSS Division Director William Snyder                  Date

______________________________                  __________________________
State - DSS Chief Financial Officer Laurie Mikkonen                  Date

______________________________                  __________________________
State – DSS Cabinet Secretary M. Gregory DeSautel, MD                  Date

State Agency Coding:

CFDA #  ____________  ____________  ____________  ____________  ____________
Company                                                
Account                                                
Center Req                                              
Center User                                              
Dollar Total                                            

______________________________
DSS Program Contact Person
Phone

______________________________
DSS Fiscal Contact Person                  Contract Accountant
Phone  605 773-3586

______________________________
Consultant Program Contact Person
Phone
Consultant Program Email Address

______________________________
Consultant Fiscal Contact Person
Phone
Consultant Fiscal Email Address

SDCL 1-24A-1 states that a copy of all consulting contracts shall be filed by the State agency with the State Auditor within five days after such contract is entered into and finally approved by the contracting parties. For further information about consulting contracts, see the State Auditor's policy handbook.
Consultant Contract Exhibit A - Security Acknowledgement

Please return agreement to your BIT Manager or Designated BIT Contact

All BIT employees and State contractors must sign; **Agreement to Comply with BIT Information Technology Security Policy (the “Policy”).** Users are responsible for compliance to all information security policies and procedures. **By signature below, the employee or contractor hereby acknowledges and agrees to the following:**

1. Employee is a State of South Dakota employee or contractor that uses non-public State of South Dakota technology infrastructure or information;
2. Employee or contractor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;
3. Employee or contractor agrees to follow state and federal regulations in regards to confidentiality and handling of data;
4. Employee or contractor has read and agrees to abide by the Policy;
5. Employee or contractor consents to discuss with a supervisor / State contact regarding Policy violations;
6. Employee or contractor shall abide by the policies described as a condition of continued employment / service;
7. Employee or contractor understands that any individual found to violate the Policy is subject to disciplinary action, including but not limited to, privilege revocation, employment termination or financial reimbursement to the State;
8. Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;
9. Access to the technology infrastructure of the State automatically terminates upon departure from the State of South Dakota employment or contract termination;
10. Employee or contractor shall promptly report violations of security policies to a BIT manager or State Contact and BIT Help Desk (605.773.4357);
11. The Policy may be amended from time to time. The State of South Dakota recommends employees and contractors for the State to regularly review the appropriate Policy and annual amendments.

**Information Technology Security Policy – BIT:** http://intranet.bit.sd.gov/policies/
**Information Technology Security Policy – CLIENT:** http://intranet.bit.sd.gov/policies/

Acknowledgement: State of South Dakota Information Technology Security Policy

Contractor: If the individual is signing for their entire company by signing this form the individual affirms that they have the authority to commit their entire organization and all its employees to follow the terms of this agreement.

____________________________________________________________
Employee or Contractor name and Company name in block capital letters
I. The following clauses are to be used at the agency’s discretion. These clauses apply to IT contracts based on:

**Clause:** Unresolved Breach of Agreement  
**Rationale:** Allows agency to recoup some costs associated with a project where the state alleges the consultant has not performed to project requirements and differences with the consultant cannot be resolved. The agency may have other methods for accomplishing this goal.  
**Usage:**  
**Optional Text:**  
**Initial Date:** base clause incorporated 5/26/2015  
**Date Modified:**

**UNRESOLVED BREACH OF THE AGREEMENT**  
In the event of an unresolved breach of this agreement, the parties acknowledge that damages from the breach will be difficult or impossible to measure or quantify. The parties agree that in the event of a breach, the Consultant shall pay, as liquidated damages, and not as a penalty, the sum of $________ or the amount paid by the State to the Consultant plus ___%, whichever is less which the parties agree is a fair and reasonable method of computing the damages caused by the breach.

**Clause:** Disposal of State Data  
**Rationale:** Federal regulations deal with the disposal of certain types of data: this clause requires the processes recommended by the National Institute of Standards and Technology which are the strictest methods known to BIT.  
**Usage:** Please consult your agency’s policy concerning the disposal of data. BIT strongly recommends use of this clause or one similar if any legally protected data is involved.  
**Initial Date:** base clause incorporated 10/15/2015  
**Date Modified:** 12/29/2016

**DISPOSAL OF STATE DATA**  
The Consultant, and Consultant’s Subcontractors, Agents, Assigns and/or Affiliated Entities shall securely dispose of all data in all forms, such as disk, CD/ DVD, backup tape and paper, when requested by the State. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods. Certificates of Destruction shall be provided to the State upon request.

**Clause:** Cyber Liability Insurance  
**Rationale:** Establishes the expectations for cyber liability insurance coverage if required  
**Usage:** Not required, but encouraged if the consultant can access, transmit, manipulate, or store any Personally Identifiable Information (PII), Family Educational Rights and Privacy Act (FERPA), Protected Heath Information (PHI), Federal Tax Information (FTI) or any information defined under state statute as confidential. Additional PII information may be found at http://intranet.bit.sd.gov/standards/PII.aspx. A 2013 study suggests the average cost to a business of a data breach is $188 per record with an average total cost of $5.4 million, not including punitive damages or fines. The cost of the insurance will vary significantly depending on the type of data, amount of data and the consultant’s security controls. There is no industry standard for the amount of coverage. Engage BIT in a conversation on this topic if it is an issue. Please consult your agency’s policy concerning PII, data protected by FERPA, PHI, FTI or information that is confidential under state law. The agency may already have preferred language that addresses some or all of the points included in the Security Incident and Data Breach Procedures, Handling of Data Breaches, and the Security Incident and Breach Responsibilities clause. If the language proposed by BIT conflicts with the agency preferred language, utilize the agency’s preferred language and inform BIT of the action.  
**Considerations:** If the agency elects to require the consultant to secure Cyber Liability Insurance, expect the cost to be passed on to the state. Encourage the consultant to check with their current insurance provider to determine whether they already have some or all the required coverage. This clause may be coupled with the Auditor’s insurance clause, number 6 in the Auditor’s Template. If no other insurance clause is included in the agreement, this clause can be coupled with the Security Incident and Data Breach Procedures, Handling of Data Breaches, and the Security Incident and Breach Responsibilities clauses  
**Optional Text:**  
**Initial Date:** base clause incorporated 5/26/2015  
**Date Modified:**
CYBER LIABILITY INSURANCE
The Consultant shall maintain cyber liability insurance with liability limits in the amount of ________ to protect any and all State data the Consultant receives as part of the project covered by this agreement including State data that may reside on devices, including laptops and smart phones, utilized by Consultant employees, whether the device is owned by the employee or the Consultant. If the Consultant has a contract with a third-party to host any State data the Consultant receives as part of the project under this agreement, then the Consultant shall include a requirement for cyber liability insurance as part of the contract between the Consultant and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include State data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-party Consultant. The cyber liability insurance shall cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this Agreement, the Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and which provide that such insurance may not be canceled, except on 30 days prior written notice to the State. The Consultant shall furnish copies of insurance policies if requested by the State. The insurance will stay in effect for ___ years after the work covered by this agreement is completed.

Clause: Domain Name Ownership
Rationale: Protects the website URL from misuse once the state no longer is using the site and allows the agency to retain ownership of the URL by paying the ongoing license fee.
Usage: Used if the agreement governs the development/use of a web site. An exception may be made if the website is used solely internally by the Consultant.
Optional Text: Retain, converting from red font to black, the final sentence if the project will include websites used internally by the Consultant.
Initial Date: base clause incorporated 5/26/2015
Date Modified:

DOMAIN NAME OWNERSHIP
Any website(s) that the Consultant creates as part of this project must have the domain name registered by and owned by the State. If as part of this project the Consultant is providing a service that utilizes a website with the domain name owned by the Consultant, the Consultant must give thirty (30) days’ notice before abandoning the site. If the Consultant intends to sell the site to another party the Consultant must give the State thirty days (30) notice and grant the State the right of first refusal. For any site or domain, whether hosted by the Consultant or within the State web infrastructure, any and all new web content should first be created in a development environment and then subjected to security scan before being approved for a move up to the production level. This paragraph does not include websites developed for the Consultant’s internal use.

Clause: Software Functionality and Replacement
Rationale: Protects the State against additional cost in the event the rights to the application are sold to another consultant who elects to discontinue the product and offers to license a similar application to the state at a higher cost. This preserves the state’s ability to determine whether the additional functionality in a different product is worth the additional investment.
Usage: Required for any project involving the acquisition/licensure of an application to be installed/operated in the state’s computing/networking environment.
Optional Text: The agency should replace the red text with a description of the general functionality of the application.
Initial Date: base clause incorporated 5/26/2015
Date Modified:

SOFTWARE FUNCTIONALITY AND REPLACEMENT
The software licensed by the Consultant to the State provides the following functionality:

Describe the broad functionality of software product licensed.

The Consultant agrees that:

A. If in the opinion of the State the Consultant reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or renamed product, the State shall be entitled to license such software product at no additional license or maintenance fee.
B. If in the opinion of the State the Consultant releases an option, future product, purchasable product or other release that has substantially the same functionality as the software product licensed to the State, and it ceases to provide maintenance for the older software product, the State shall have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the Consultant discontinues the licensed product and recommends movement to a new product as a replacement option regardless of any additional functionality the replacement product may have over the licensed product.

*** BIT Required

PROVISION OF DATA
Upon notice of termination by either party, the State will be provided by the Consultant all current State Data and End User Data in a non-proprietary form. Upon the effective date of the termination of the agreement, the State will again be provided by the Consultant with all current State Data and End User Data in a non-proprietary form.

THREAT NOTIFICATION
Upon becoming aware of a possible security threat(s) or exploit(s) with the Consultant’s product(s) and or service(s) being used by the State, the Consultant or any subcontractor suppling product(s) or service(s) to the Consultant needed to fulfill the terms of this Agreement will notify the State within two (2) business days of any such threat(s) or exploit(s). If the State requests, the Consultant will provide the State with information on the threat(s) or exploit(s).

SECURITY INCIDENTS REGARDING PROTECTED HEALTH INFORMATION
Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as defined in 45 CFR 164.304. The Consultant shall alert the State Contact within twelve (12) hours of a Security Incident and provide daily updates to the BIT contact at their request. The Parties agree that this alert does not affect the Consultant’s obligations under the Business Associate Agreement or the requirements of 45 CFR 164.410. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute a Security Incident, this Agreement constitutes notice by Consultant of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Consultant’s firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. The State can require the Consultant to conduct a review or investigation within the scope and methodology determined by the State. At the State’s discretion, the review or investigation may be performed by a third party at the Consultant’s expense.

Notwithstanding any other provision of this Agreement and in addition to any other remedies available to the State under law or equity, in the event the investigation or review determines that the consultant is responsible for the Security Incident, and where the State incurs any costs in the investigation, review or remediation of the Security Incident, the Consultant shall reimburse the State in full for all such costs. Costs include, but are not limited to, providing notification to regulatory agencies or other entities as required by law or contract. In the event the investigation or review determines that the consultant is responsible for the Security Incident, the Consultant shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident, and all costs associated with the remediation of the Consultant’s services and/or product(s).

BROWSER
The system, site, and/or application must be compatible with vendor supported versions of Edge, Chrome, Safari, Firefox and Internet Explorer browsers. Silverlight, QuickTime, PHP, Adobe ColdFusion, Adobe Flash and Adobe Animate CC will not be used in the system, site, and/or application.

SECURITY ACKNOWLEDGEMENT FORM
The Consultant will be required to sign the Security Acknowledgement form which is attached to this Agreement as Exhibit A. The signed Security Acknowledgement form must be submitted to the State and approved by the South Dakota Bureau of Information and Telecommunications and communicated to the Consultant by the State contact before work on the contract may begin. This form constitutes the agreement of Consultant to be responsible and liable for ensuring that the Consultant, Consultant’s employee(s), and Subcontractor’s, Agents, Assigns and or Affiliated Entities and all of their employee(s), participating in the work will abide by the
terms of the Information Technology Security Policy- Contractor (ITSP) attached to this Agreement as Exhibit D. Failure to abide by the requirements of the ITSP or the Security Acknowledgement form can be considered a breach of this Agreement at the discretion of the State. It is also a breach of this Agreement, at the discretion of the State, if the Consultant does not sign another Security Acknowledgement form covering any employee(s) and any Subcontractor’s, Agents, Assigns and or Affiliated Entities employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Consultant’s, Consultant’s employee(s) or Subcontractor’s, Agents, Assigns and or Affiliated Entities employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Consultant or Subcontractor’s, Agents, Assigns and or Affiliated Entities and in accordance with the Consultant’s or Subcontractor’s, Agents, Assigns and or Affiliated Entities personnel policies. Regardless of the actions taken by the Consultant and Subcontractor’s, Agents, Assigns and or Affiliated Entities, the State shall retain the right to require at its discretion the removal of the employee(s) from the project covered by this agreement.

BACKGROUND CHECKS
The State of South Dakota requires all employee(s) of the Consultant, Subcontractors, Agents, Assigns and or Affiliated Entities who write or modify State of South Dakota-owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo fingerprint-based background checks. These fingerprints will be used to check the criminal history records of the State as well as the Federal Bureau of Investigation’s criminal history records. These background checks must be performed by the State with support from the State’s law enforcement resources. The State will supply the fingerprint cards and prescribe the procedure to be used to process the fingerprint cards. Project plans should allow two (2) to four (4) weeks to complete this process. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the Consultant, Subcontractor’s, Agents, Assigns and or Affiliated Entities will be writing or modifying State of South Dakota owned software, altering hardware, configuring software of state owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas then, background checks must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Consultant to prohibit any employee, Subcontractors, Agents, Assigns and or Affiliated Entities from performing work under this Agreement whenever the State, in its sole discretion, believes that having a specific employee, subcontractor, agent assign or affiliated entity performing work under this Agreement is detrimental to the project or is considered by the State to be a security risk, based on the results of the background check. The State will provide the Consultant with notice of this determination.

PRODUCT INSTALLATION AND OPERATION
The State will install and operate the Consultant’s product on the State’s computing infrastructure. The State’s installation process and operation of the product will follow current State standards which can be found at http://bit.sd.gov/standards/. It is the Consultant’s responsibility to review these standards and alert the State if the costs enumerated in the agreement will change based on State standards. The State will not be responsible for added licensing or processing costs if the Consultant determines at a later date, that by following the standards in effect at the time of installation the State is or would be obligated to pay fines, additional rates, fees, license costs or charges of any type, additional charges of any type or character for Consultant’s or a third party’s intellectual property, or added support costs.

SECURITY
The Consultant shall take all actions necessary to protect State information from exploits, inappropriate alterations, access or release, and malicious attacks.

By signing this agreement, the Consultant warrants that:
A. All known security issues are resolved.
B. Assistance will be provided to the State by the Consultant in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. This investigation can include security scans made at the State’s discretion.
C. State technology standards, policies, and best practices will be followed. State technology standards can be found at http://bit.sd.gov/standards/.

LICENSE TO PERFORM SECURITY SCANNING
The Consultant will provide the State, at a time and for duration agreeable to both parties, access to the application and underlying hardware referenced in this Agreement for security scanning activities. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or the Consultant has with a third-party. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the state security scanning efforts discover security

04/18
issues, the State may collaborate, at the State’s discretion, with the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements the State has with the Consultant. The State will be indemnified and held harmless by the Consultant from all actions, lawsuits, damages (including all ordinary, incidental, consequential, and exemplary damages) or other proceedings that arise from security scanning, remediation efforts, and any after effects of security scanning or remediation. This indemnification includes all defense costs as well as reasonable attorneys’ fees the State of South Dakota is required to pay in any such proceedings. The State will not be charged for any costs incurred by Consultant in these remediation efforts unless agreed to by the State in advance in writing. In the event of conflicting language this clause supersedes any other language in this or any other agreement made between the State and the Consultant.

SECURITY SCANNING
At the State’s discretion, security scanning will be performed and or security settings put in place or altered during pre-production review for new or updated code. These scans and tests can be time consuming and should be accounted for in project planning documents and schedules. Products not meeting the State’s security and performance requirements will not be allowed into production and will be barred from User Acceptance Testing (UAT) until all issues are addressed to the State’s satisfaction. The discovery of security issues during UAT are automatically sufficient grounds for non-acceptance of a product even though a product may satisfy all other acceptance criteria. Any security issues discovered during UAT that require product changes will not be considered a project change chargeable to the State. The State urges the use of industry scanning/testing tools and recommends secure development other acceptance criteria. Any security issues discovered during UAT that require product changes will not be considered a project change chargeable to the State. The State urges the use of industry scanning/testing tools and recommends secure development methods are employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the Consultant producing or delivering an application to the State. Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing.

MALICIOUS CODE
A. The Consultant warrants that the licensed software contains no code that does not support an application requirement.
B. The Consultant warrants that the licensed software contains no malicious code.
C. The Consultant warrants that the Consultant will not insert into the licensed software or any media on which the licensed software is delivered any malicious or intentionally destructive code.
D. The Consultant warrants that the Consultant will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the licensed software before installation. In the event any malicious code is discovered in the licensed software delivered by the Consultant, the Consultant shall provide the State at no charge with a copy of the applicable licensed software that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this paragraph are in addition to other additional remedies available to the State.

DENIAL OF ACCESS OR REMOVAL OF AN APPLICATION AND OR HARDWARE FROM PRODUCTION
During the life of this Agreement the application and or hardware can be denied access to or removed from production at the State’s discretion. The reasons for the denial of access or removal of the application and or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption. Denial of access or removal of an application and or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the state determines are unacceptable results. The Consultant will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and or excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application and or hardware. At the discretion of the State, contractual payments may be suspended while the application and or hardware is denied access to or removed from production. The reasons can be because of the Consultant’s actions or inactions. Access to the production system to perform any remediying of the reasons for denial of access or removal of the software and hardware, and its updating and or patching will be made only with the State’s prior approval. It is expected that the Consultant shall provide the State with proof of the safety and or effectiveness of the remedy, update or patch proposed before the State provides access to the production system. The State shall sign a non-disclosure agreement with the Consultant if revealing the update or patch will put the Consultant’s intellectual property at risk. If the remedy, update or patch the Consultant proposes is unable to present software and or hardware that meets the State’s requirements, as defined by the State, which may include but not limited to security, functionality, unsupported third party technologies, to the State’s satisfaction within thirty (30) days of the denial of access to or removal from the production system and the Consultant does not employ the change management process to alter the project schedule or deliverables within the same thirty (30) days then at the State’s discretion the Agreement may be terminated.

MOVEMENT OF PRODUCT
The State operates a virtualized computing environment and retains the right to use industry standard hypervisor high availability, fail-over, and disaster recovery systems to move instances of the product(s) between the install sites defined with the Consultant within the provisions of resource and usage restrictions outlined elsewhere in the agreement. As part of normal operations, the State may also install the product on different computers or servers if the product is also removed from the previous computer or server within the provisions of resource and usage restrictions outlined elsewhere in the agreement. All such movement of product can be done by the State without any additional fees or charges by the Consultant.

**USE OF PRODUCT ON VIRTUALIZED INFRASTRUCTURE AND CHANGES TO THAT INFRASTRUCTURE**
The State operates a virtualized computing environment and uses software-based management and resource capping. The State retains the right to use and upgrade as deemed appropriate its hypervisor and operating system technology and related hardware without additional license fees or other charges provided the State assures the guest operating system(s) running within that hypervisor environment continue to present computing resources to the licensed product that conform with the terms of the license agreement. The computing resource allocations within the State’s hypervisor software-based management controls for the guest operating system(s) executing the product shall be the only consideration in licensing compliance related to computing resource capacity.

**LOAD BALANCING**
The State routinely load balances across multiple servers, applications that run on the State’s computing environment. The Consultant’s product must be able to be load balanced across multiple servers. Any changes or modifications required to allow the Consultant’s product to be load balanced so that it can operate on the State’s computing environment will be at the Consultant’s expense.

**BACKUP COPIES**
The State may make and keep backup copies of the licensed product without additional cost or obligation on the condition that:

A. The State maintains possession of the backup copies.
B. The backup copies are used only as bona fide backups.

**USE OF ABSTRACTION TECHNOLOGIES**
The Consultant’s application must use abstraction technologies in all applications, that is the removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services.

The Consultant warrants that hard-coded references will not be used in the application. Use of hard-coded references will result in a failure to pass pre-production testing or may cause the application to fail or be shut down at any time without warning and or be removed from production. Correcting the hardcoded references is the responsibility of the Consultant and will not be a project change chargeable to the State. If the use of hard-coded references is discovered after User Acceptance Testing the Consultant will correct the problem at no additional cost.

**LICENSE AGREEMENTS**
Consultant warrants that it has provided to the State and incorporated into this agreement all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software before execution of this agreement. Failure to provide all such license agreements, End User License Agreements, and terms of use shall be a breach of this agreement at the option of the State. The parties agree that neither the State nor its end users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Consultant agrees that it shall indemnify and hold the State harmless from any and all damages or other detriment, actions, lawsuits or other proceedings that arise from failure to provide all such license agreements, End User License Agreements, and terms of use or that arise from any failure to give the State notice of all such license agreements, End User License Agreements, and terms of use. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

**WEB AND MOBILE APPLICATIONS**
The Consultant’s application is required to:

A. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State’s business goals for the application;
B. encrypt data in transport and at rest using a mutually agreed upon encryption format;
C. close all connections and close the application at the end of processing;
D. the documentation will be in grammatically complete text for each call and defined variables (Use no abbreviations and use complete sentences, for example.) sufficient for a native speaker of English with average programming skills to determine the meaning and/or intent of what is written without prior knowledge of the application.
E. have no code not required for the functioning of application;
F. have no “back doors”, a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State;
G. permit no tracking of device user’s activities without providing a clear notice to the device user and requiring the device user’s active approval before the application captures tracking data;
H. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation;
I. fully disclose in the “about” information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s);
J. ask only for those permissions and access rights on the user’s device that are required for the defined requirements of the Consultant’s application;
K. access no data outside that which is defined in the “About” information for the Consultant’s application;
L. Your web site application produced for the State must conform to Web Content Accessibility Guidelines 2.0;

The Consultant is required to disclose all:
A. functionality;
B. device and functional dependencies; and
C. third party libraries used. (or; if the rest if the red text is used)
D. methods user data is being stored, processed or transmitted;
E. methods used to notify the user how their data is being stored, processed and or transmitted;
F. positive actions required by the user to give permission for their data to be stored, processed and or transmitted;
G. methods used to record the user’s response(s) to the notification that their data is being stored, processed and or transmitted;
H. methods used to secure the data in storage, processing or transmission; and
I. forms of authentication required for a user to access the application or any data it gathers stores, processes and or transmits;
J. methods used to create and customize existing reports;
K. methods used to integrate with external data sources;
L. methods used if integrates with public cloud provider;
M. methods and techniques used and the security features that protect data, if a public cloud provider is used;
N. formats the data and information uses.

If the application does not adhere to the requirements given above or the Consultant has unacceptable disclosures, at the State’s discretion, the Consultant will rectify the issues at no cost to the State.

OFFSHORE SERVICES
The Consultant will not provide access to State data to any entity or person(s) located outside the continental United States that are not named in this agreement or without the written permission of the State.

MULTIFACTOR AUTHENTICATION
The Consultant must adhere to the requirements of level 3 authentication assurance for multifactor authentication as defined in NIST 800-63 when performing work under this contract where the Consultant potentially has access to legally protected State data. The Consultant must require that and all its Subcontractors, Agents. Assigns, and Affiliated Entities who potentially have access to legally protected State data also adhere to level 3 authentication assurance as defined in NIST 800-63, and Consultant shall be in breach of this contract if Consultant fails to so require.
*** The following clauses are to be used at the agency’s discretion. These clauses apply to IT contracts based on:

---

**Clause:** Data Location  
**Rationale:** To ensure State and End User data is not stored in areas not under jurisdiction of US law.  
**Usage:**  
**Optional Text:**  
**Initial Date:** base clause incorporated 11/04/2016  
**Date Modified:**

**DATA LOCATION**  
The Consultant shall provide its services to the State and its End Users, as well as storage of State data and End User data solely from data centers in the continental United States. The Consultant will not allow any State or End User data to be provided to or accessed by any entity outside the continental United States. This restriction includes but is not limited to Consultant’s employees and contractors. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States. The Consultant shall not allow its employees or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at its data centers. The Consultant shall permit its personnel and contractors to access State data remotely only as required to provide technical support.

**Clause:** Data Protection  
**Rationale:** To put limits on how the state’s data can be used.  
**Usage:**  
**Optional Text:**  
**Initial Date:** base clause incorporated 11/10/2016  
**Date Modified:**

**DATA PROTECTION**  
Protection of personal privacy and data shall be an integral part of the business activities of the Consultant to ensure there is no inappropriate or unauthorized use of State’s data and or End User Data at any time. To this end, the Consultant shall safeguard the confidentiality, integrity and availability of State’s data and or End User Data and comply with the following conditions:

A. The Consultant shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Personal Health Information (PHI), Federal Tax Information (FTI) or any information that is confidential under state law. Such security measures shall be in accordance with recognized industry practice and not less protective than the measures the Consultant applies to its own non-public data.

B. At no time shall any data that either belong to or are intended for the use of the State or its officers, agents or employees—be copied, disclosed or retained by the Consultant or any party related to the Consultant for subsequent use in any transaction that does not include the State.

C. The Consultant will not use such data for the Consultant’s own benefit and, in particular will not engage in data mining of State’s data and or End User Data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State data.

**Clause:** Host Facility Physical Security  
**Rationale:** This may be required if there is a federal audit of data security. This clause while similar to the Faculties Inspection clause does provide more detail on the physical access requirements.
**HOST FACILITY PHYSICAL SECURITY**

The Consultant will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate physical security. This includes, at a minimum, centrally administered electronic locks that control entry and exit from all rooms where the hosted system resides. Any door security system must either be connected to the building’s power backup system as defined elsewhere or have internal battery power sufficient to last 24 hours in normal usage. Security events for the physical access system must be logged and the logs stored electronically in a secure location in a non-changeable format and must be searchable. Retention on the logs must be not less than 7 years. Log entries must be created for at least: successful entry and exit (indicating whether the access was to enter or exit the room) as well as all security related events such as, doors left open more than 30 seconds, forced entries, failed entry attempts, repeat entries without exit, repeat exits without entry, attempts to access doors for which access was not authorized. The Consultant agrees to provide, at the State’s request, full access to search the security logs for any access or security events related to any and all rooms and physical locations hosting the State’s system.

**Clause: Legal Requests for Data**

**Rationale:** This clause requires the consultant to notify the state if there are any legal requests for the state’s data.

**Usage:**

**Optional Text:**

**Initial Date:** base clause incorporated 11/21/16

**Date Modified:**

**LEGAL REQUESTS FOR DATA**

Except as otherwise expressly prohibited by law, the Consultant will:

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Consultant seeking State data and or End User Data maintained by the Consultant;

B. Consult with the State regarding its response;

C. Cooperate with the State’s requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request; and

D. Upon the State’s request, provide the State with a copy of both the demand or request and its proposed or actual response.

**Clause: eDiscovery**

**Rationale:** This clause requires the consultant to notify the state if there is any legal action that involves discovery of electronic data, usually emails.

**Usage:**

**Optional Text:**

**Initial Date:** base clause incorporated 11/21/16

**Date Modified:**

**EDISCOVERY**

The Consultant shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Consultant shall not respond to service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

**Clause: Access Attempts**
**Rationale:** This clause requires the consultant to keep a log of all access attempts to the system hosting state data. These access attempts do not necessarily need to be successful to be logged. Logs of access attempts are required by some federally protected data. If you have federally protected data you should check what your requirements are.

**Usage:**

**Optional Text:**

**Initial Date:** base clause incorporated 11/21/16

**Date Modified:**

---

### ACCESS ATTEMPTS

All access attempts, whether failed or successful, to any system connected to the hosted system which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity shall be logged by the Consultant. For all systems, the log must include at least: log-in page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 7 years in a searchable database in an electronic format that is un-modifiable. At the request of the state, access must be granted to search those logs as needed to demonstrate compliance with the terms of this contract, and any and all audit requirements related to the hosted system.

---

**Clause:** Annual Risk Analysis

**Rationale:** To make sure federal requirements for risk analysis are followed.

**Usage:** BIT suggests this be used wherever HIPAA data is involved unless this topic is covered in the agency’s Business Associate Agreement.

**Optional Text:**

**Initial Date:** base clause incorporated 2/16/2018

**Date Modified:**

---

### ANNUAL RISK ANALYSIS

The Consultant will conduct a risk analysis annually or when there has been a significant system change. The Consultant will provide verification to the State Contact upon request that the risk analysis has taken place. At a minimum the risk analysis will include a review of the:

(i) Penetration testing of the Consultant’s system.
(ii) Security policies and procedures.
(iii) Disaster recovery plan.
(iv) Security incident plan.
(v) Business Associates Agreements.
(vi) Inventory of physical systems, devices and media that store or utilize ePHI for completeness.

If the risk analysis provides evidence of deficiencies a risk management plan will be produced. A summary of the risk management plan will be sent to the State Contact. The summary will include completion dates for the plan’s milestones. Updates on the risk management plan will be sent to the State Contact upon request.

---

### THIRD PARTY HOSTING

If the Consultant has the State’s data and or End User’s Data hosted by another party the Consultant must provide the State the name of this party. The Consultant must provide the State with contact information for this third party and the location of their data center(s). The Consultant must receive from the third party written assurances that the state’s data and or End User Data will reside in the continental United States at all times and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party’s employees or contractors. If during the term of this agreement the consultant changes from the Consultant hosting the data to a third-party hosting the data or changes third-party hosting provider, the Consultant will provide the State with one hundred and eighty (180) days’ advance notice of this change and at that time provide the state with the information required above.

### SECURING OF DATA
All facilities used to store and process State’s data and or End User Data will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Consultant’s own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Consultant warrants that all State’s data and or End User Data will be encrypted in transmission (including via web interface) and storage at no less than AES256 level encryption with SHA256 or SHA2 hashing.

SECURITY PROCESSES
The Consultant shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Consultant. For example: virus checking and port sniffing.

IMPORT AND EXPORT OF DATA
The State shall have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Consultant. This includes the ability for the State to import or export data to/from other Consultants.

SCANNING AND AUDIT AUTHORIZATION
The Consultant will provide the State at no cost and at a date, time and for duration agreeable to both parties, authorization to scan and access to a test system containing test data for security scanning activities. The system and data provided to the State by Consultant for testing purposes will be considered a test system containing test data. The State will not scan any environment known by the State to be a production environment at the time the scan is performed by the State. Consultant provides their consent for the State or any third-party acting for the State to scan the systems and data provided as the State wishes using any methodology that the State wishes. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or that the consultant has with a third-party.

The Consultant will also allow the State at the State’s expense, not to include Consultant’s expenses, to perform up to two security audit and vulnerability assessments per year to provide verification of Consultant’s IT security safeguards for the system and its data. The State will work with the Consultant to arrange the audit at a time least likely to create workload issues for the Consultant and will accept scanning a test or UAT environment on which the code and systems are a mirror image of the production environment.

The Consultant indemnifies the State for ordinary, consequential and incidental damages to the Consultant’s computer system and the data it contains that is the result of scanning. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State’s security scans discover security issues the State may collaborate, at the State’s discretion with the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements between the State and Consultant. The State while engaged, and after, with the Consultant on remediation is indemnified and held harmless from all actions, lawsuits, damages (including all ordinary, consequential and incidental damages) or other proceedings that arise from security scanning, remediation efforts, and any after effects of security scanning or remediation. This indemnification includes all defense costs as well as reasonable attorneys’ fees the State of South Dakota is required to pay in such proceedings. The State will not be charged for any costs incurred by the consultant in these remediation efforts unless agreed to by the State in advance in writing.

In the event of conflicting language this clause supersedes any other language in this or any other agreement made between the State and the Consultant.

The Consultant agrees to work with the State to rectify any serious security issues revealed by the security audit and or security scanning. This includes additional security audits and security scanning that shall be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. It is required that any security audits must meet the requirements of the Payment Card Industry Data Security Standard (PCI DSS) irrespective of there being any PCI DSS data involved.

SUSPENSION OF SERVICES
The State may suspend, or terminate, or direct the Consultant to suspend or terminate, an End User’s access to services in accordance with the State’s policies an End User being . The State will assume sole responsibility for any claims made by End Users regarding the State’s suspension/termination or directive to suspend/terminate such service. The Consultant may suspend access to
services to an End User(s) immediately in response to an act or omission that reasonably appears to jeopardize the security or integrity of the Consultant’s services or the network(s) or facilities used to provide the services. Suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. The Consultant may suspend the State’s access to services if, after at least ____ days’ written notice to the State and subsequent good-faith, commercially reasonable efforts to resolve the matter with the State to the parties’ mutual satisfaction, the State remains in material breach of this Agreement. The suspension will be lifted immediately when the breach is cured. The Consultant may suspend access to services by an End User in response to a material breach by End User of any terms of use he or she has agreed to in connection with receiving the services. The Consultant will notify the State of any suspension of End User access to services.

SYSTEM UPGRADES
Advance notice of 30 days shall be provided the State of any major upgrades or system changes the Consultant will be implementing unless the changes are for reasons of security. A major upgrade is a replacement of hardware, software or firmware with a newer or improved version, in order to bring the system up to date or to improve its characteristics. The State reserves the right to scan the Consultant’s systems for vulnerabilities after a system upgrade. These vulnerability scan can include penetration testing of a test system at the State’s discretion.

PASSWORD PROTECTION
The website(s) and or service(s) that will be hosted by the Consultant for the State will be password protected. If the Consultant provides the user with a preset or default password that password cannot include any Personally Identifiable Information, data protected under the Family Educational Rights and Privacy Act, Personal Heath Information, Federal Tax Information or any information defined under state statute as confidential Information or fragment thereof.

MOVEMENT OF PROTECTED STATE DATA
Any State data that is protected by Federal or State statute or requirements or by industry standards must be kept secure. When protected State data is moved to any of the Consultant’s production or non-production systems, security must be maintained. The Consultant will ensure that that data will at least have the same level of security as it had on the State’s environment. The State’s security policies can be found in the Information Technology Security Policies (ITSP).
Consultant Contract Exhibit D - BIT Information Technology Security Plan (ITSP)

Included as separate document.
ATTACHMENT G – State of South Dakota Business Associate Agreement

1. Definitions

General definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the Provider, Consultant or entity contracting with the State of South Dakota as set forth more fully in the Agreement this Business Associate Agreement is attached.

(b) CFR. “CFR” shall mean the Code of Federal Regulations.

(c) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean South Dakota Department of Social Services.

(d) Designated Record Set. “Designated Record Set” shall have the meaning given to such term in 45 CFR 164.501.


(g) Protected Health Information. “Protected Health Information” or “PHI” shall mean the term as defined in 45 C.F.R. §160.103, and is limited to the Protected Health Information received from, or received or created on behalf of Covered Entity by Business Associate pursuant to performance of the Services under the Agreement.

2. Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware within five (5) business days of receiving knowledge of such use, disclosure, breach, or security incident;

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;
(e) Make available protected health information in a designated record set to the covered entity as necessary to satisfy covered entity’s obligations under 45 CFR 164.524. Business associate shall cooperate with covered entity to fulfill all requests by individuals for access to the individual’s protected health information that are approved by covered entity. If business associate receives a request from an individual for access to protected health information, business associate shall forward such request to covered entity within ten (10) business days. Covered entity shall be solely responsible for determining the scope of protected health information and Designated Record Set with respect to each request by an individual for access to protected health information;

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity’s obligations under 45 CFR 164.526. Within ten (10) business days following any such amendment or other measure, business associate shall provide written notice to covered entity confirming that business associate has made such amendments or other measures and containing any such information as may be necessary for covered entity to provide adequate notice to the individual in accordance with 45 CFR 164.526. Should business associate receive requests to amend protected health information from an individual, Business associate shall cooperate with covered entity to fulfill all requests by individuals for such amendments to the individual’s protected health information that are approved by covered entity. If business associate receives a request from an individual to amend protected health information, business associate shall forward such request to covered entity within ten (10) business days. Covered entity shall be solely responsible for determining whether to amend any protected health information with respect to each request by an individual for access to protected health information;

(g) Maintain and make available the information required to provide an accounting of disclosures to the covered entities necessary to satisfy covered entity’s obligations under 45 CFR 164.528. Business associate shall cooperate with covered entity to fulfill all requests by individuals for access to an accounting of disclosures that are approved by covered entity. If business associate receives a request from an individual for an accounting of disclosures, business associate shall immediately forward such request to covered entity. Covered entity shall be solely responsible for determining whether to release any account of disclosures;

(h) To the extent the business associate is to carry out one or more of covered entity’s obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the covered entity and / or the Secretary of the United States Department of Health and Human Services for purposes of determining compliance with the HIPAA Rules.

3. Permitted Uses and Disclosures by Business Associate

(a) Except as otherwise limited by this Agreement, Business Associate may make any uses and disclosures of Protected Health Information necessary to perform its services to Covered Entity and otherwise meet its obligations under this Agreement, if such use or disclosure would not violate the Privacy Rule if done by the covered entity. All other uses or disclosure by Business Associate not authorized by this Agreement or by specific instruction of Covered Entity are prohibited.

(b) The business associate is authorized to use protected health information if the business associate de-identifies the information in accordance with 45 CFR 164.514(a)-(c). In order to de-identify any information, Business Associate must remove all information identifying the individual including, but not limited to, the following: names, geographic subdivisions smaller than a state, all dates related to an individual, all ages over the age of 89 (except such ages may be aggregated into a single category of age 90 or older, telephone numbers, fax numbers, electronic mail (email) addresses, medical record numbers, account numbers, certificate/ license numbers, vehicle identifiers and serial numbers (including license plate numbers, device identifiers and serial numbers, web universal resource locators (URLs), internet protocol (IP) address number, biometric identifiers (including finger and voice prints), full face photographic images (and any comparable images), any other unique identifying number, and any other characteristic or code.
(c) Business associate may use or disclose protected health information as required by law.

(d) Business associate agrees to make uses and disclosures and requests for protected health information consistent with covered entity’s minimum necessary policies and procedures.

(e) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity except for the specific uses and disclosures set forth in (f) and (g).

(f) Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law.

(g) Business associate may provide data aggregation services relating to the health care operations of the covered entity.

4. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate’s use or disclosure of protected health information.

(b) Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate’s use or disclosure of protected health information.

(c) Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate’s use or disclosure of protected health information.

5. Term and Termination

(a) Term. The Term of this Agreement shall be effective as of and shall terminate on the dates set forth in the primary Agreement this Business Associate Agreement is attached to or on the date the primary Agreement terminates, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement.

(c) Obligations of Business Associate Upon Termination.

1. Except as provided in paragraph (2) of this section, upon termination of this agreement for any reason, business associate shall return or destroy all protected health information received from, or created or received by business associate on behalf of covered entity. This provision shall apply to protected health information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

2. In the event that business associate determines that returning or destroying the protected health information is infeasible, business associate shall provide to covered entity, within ten (10) business days, notification of the conditions that make return or destruction infeasible. Upon such determination, business associate shall extend the protections of this agreement to such protected health information and limit further uses and disclosures of such protected health information to those purposes that make the return or destruction infeasible, for so long as business associate maintains such protected health information.
(d) **Survival.** The obligations of business associate under this Section shall survive the termination of this Agreement.

6. **Miscellaneous**

(a) **Regulatory References.** A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) **Interpretation.** Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

(d) **Conflicts.** In the event of a conflict in between the terms of this Business Associate Agreement and the Agreement to which it is attached, the terms of this Business Associate Agreement shall prevail to the extent such an interpretation ensures compliance with the HIPAA Rules.

The Implementation contractor must comply with the following provisions:

1. Executive Order 11246, entitled "Equal Employment Opportunity," as amended by Executive Order 11375, and as supplemented by the Department of Labor Regulations (41 CFR Part 60): The Executive Order prohibits federal contractors and federally-assisted construction contractors and subcontractors who do over $10,000 in Government business in one year from discriminating in employment decisions on the basis of race, color, religion, sex, or national origin. The Executive Order also requires Government contractors to take affirmative action to ensure that equal opportunity is provided in all aspects of their employment.

2. The Clean Air Act, Section 306:
   a. No Federal agency may enter into any contract with any person who has been convicted of any offense under section 113(c) for the procurement of goods, materials, and services if such contract is to be performed at any facility at which the violation which gave rise to such conviction occurred, and if such facility is owned, leased, or supervised by such person. The prohibition in the preceding sentence shall continue until the Administrator certifies that the condition giving rise to such conviction has been corrected. For convictions arising under section 113(c)(2), the condition giving rise to the conviction also shall be considered to include any substantive violation of this Act associated with the violation of 113(c)(2). The Administrator may extend this prohibition to other facilities owned or operated by the convicted person.
   b. The Administrator shall establish procedures to provide all Federal agencies with the notification necessary for the purposes of subsection (a).
   c. In order to implement the purposes and policy of this Act to protect and enhance the quality of the Nation's air, the President shall, not more than 180 days after enactment of the Clean Air Amendments of 1970 cause to be issued an order (1) requiring each Federal agency authorized to enter into contracts and each Federal agency which is empowered to extend Federal assistance by way of grant, loan, or contract to effectuate the purpose and policy of this Act in such contracting or assistance activities, and (2) setting forth procedures, sanctions, penalties, and such other provisions, as the President determines necessary to carry out such requirement.
   d. The President may exempt any contract, loan, or grant from all or part of the provisions of this section where he determines such exemption is necessary in the paramount interest of the United States and he shall notify the Congress of such exemption.
   e. The President shall annually report to the Congress on measures taken toward implementing the purpose and intent of this section, including but not limited to the progress and problems associated with implementation of this section. [42 U.S.C. 7606]

3. The Clean Water Act:
   a. No Federal agency may enter into any contract with any person who has been convicted of any offense under Section 309(c) of this Act for the procurement of goods, materials, and services if such contract is to be performed at any facility at which the violation which gave rise to such conviction occurred, and if such facility is owned, leased, or supervised by such person. The prohibition in preceding sentence shall continue until the Administrator certifies that the condition giving rise to such conviction has been corrected.
   b. The Administrator shall establish procedures to provide all Federal agencies with the notification necessary for the purposes of subsection (a) of this section.
   c. In order to implement the purposes and policy of this Act to protect and enhance the quality of the Nation's water, the President shall, not more than 180 days after the enactment of this Act, cause to be issued an order:
      (1) requiring each Federal agency authorized to enter into contracts and each Federal agency which is empowered to extend Federal assistance by way of grant, loan, or contract to effectuate the purpose and policy of this Act in such contracting or assistance activities, and
      (2) setting forth procedures, sanctions, penalties, and such other provisions, as the President determines necessary to carry out such requirement.
d. The President may exempt any contract, loan, or grant from all or part of the provisions of this section where he
determines such exemption is necessary in the paramount interest of the United States and he shall notify the
Congress of such exemption.

e. The President shall annually report to the Congress on measures taken in compliance with the purpose and intent
of this section, including, but not limited to, the progress and problems associated with such compliance.

f. (1) No certification by a contractor, and no contract clause, may be required in the case of a contract for the
acquisition of commercial items in order to implement a prohibition or requirement of this section or a prohibition
or requirement issued in the implementation of this section.

(2) In paragraph (1), the term “commercial item” has the meaning given such term in section 4(12) of the Office of
Federal Procurement Policy Act (41 U.S.C. 403(12)).

4. The Anti-Lobbying Act: This Act prohibits the recipients of federal contracts, grants, and loans from using
appropriated funds for lobbying the Executive or Legislative Branches of the federal government in connection with a
specific contract, grant, or loan. As required by Section 1352, Title 31 of the U.S. Code and implemented at 34 CFR
Part 82 for persons entering into a grant or cooperative agreement over $100,000, as defined at 34 CFR Part 82,
Section 82.105 and 82.110, the applicant certifies that:

a. No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person
for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer
or employee of Congress, or an employee of a member of Congress in connection with the making of any federal
grant, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or
modification of any federal grant or cooperative agreement;

b. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or
attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of
Congress, or an employee of a member of Congress in connection with this federal grant or cooperative
agreement, the undersigned shall complete and submit Standard Form – LLL, “Disclosure Form to Report
Lobbying,” in accordance with its instructions;

c. The undersigned shall require that the language of this certification be include in the award documents for all sub-
awards at all tiers (including sub-grants, contracts under grants and cooperative agreements, and subcontracts)
and that all sub-recipients shall certify and disclose accordingly.

5. Americans with Disabilities Act: This Act (28 CFR Part 35, Title II, Subtitle A) prohibits discrimination on the basis of
disability in all services, programs, and activities provided to the public by State and local governments, except public
transportation services.

attempt to address the problems of drug abuse on the job. It is a fact that employees who use drugs have less
productivity, a lower quality of work, and a higher absenteeism, and are more likely to misappropriate funds or
services. From this perspective, the drug abuser may endanger other employees, the public at large, or themselves.
Damage to property, whether owned by this entity or not, could result from drug abuse on the job. All these actions
might undermine public confidence in the services this entity provides. Therefore, in order to remain a responsible
source for government contracts, the following guidelines have been adopted:

a. The unlawful manufacture, distribution, dispensation, possession or use of a controlled substance is prohibited in
the work place.

b. Violators may be terminated or requested to seek counseling from an approved rehabilitation service.

c. Employees must notify their employer of any conviction of a criminal drug statute no later than five days after such
conviction.

d. Although alcohol is not a controlled substance, it is nonetheless a drug. It is the policy of the Arkansas
Department of Health WIC Program that abuse of this drug will also not be tolerated in the workplace.

e. Contractors of federal agencies are required to certify that they will provide drug-free workplaces for their
employees.
7. Debarment, suspension, and other responsibility matters: As required by Executive Order 12549, Debarment and Suspension, and implemented at 34 CFR Part 85, for prospective participants in primary covered transactions, as defined at 34 CFR Part 85, Sections 85.105 and 85.110.

   a. The applicant certifies that it and its principals:

      (1) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal department or agency;

      (2) Have not within a three-year period preceding this application been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

      (3) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses enumerated in paragraph (1)(b) of this certification; and

      (4) Have not within a three-year period preceding this application had one or more public transactions (federal, state, or local) terminated for cause or default.

   b. Where the applicant is unable to certify to any of the statements in this certification, he or she shall attach an explanation to this application.

8. The federal government reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use, and to authorize others to use, for federal government purposes, the copyright in any work developed under a grant, sub-grant, or contract under a grant or sub-grant or any rights of copyright to which a contractor purchases ownership.

9. **Procurement Standards (Competition / Sole Source)**

   - SMM Section 11267
   - 45 CFR Part 95 Subpart F & 95.615
   - 45 CFR Part 95 & 92.36

   **Access to Records**

   - 42 CFR Part 433.112(b)(5) – (9)
   - 45 CFR Part 95 Subpart F & 95.615
   - SMM Section 11267

   **Software and Ownership Rights, Federal Licenses, Information Safeguarding, HIPAA Compliance, and Progress Reports:**

   - 45 CFR Part 95 Subpart F & 95.617
   - 42 CFR Part 431.300
   - 42 CFR Part 164

   **Independent Verification and Validation (IV&V)**

   - 45 CFR Part 95.626

10. **MITA 3.0**

ATTACHMENT I – BIT Security and Vendor Questionnaire

**Agencies:** The following questions help agencies acquire technology that meets state security and technology standards. BIT recommends that you contact your BIT Point of Contact to arrange a meeting if you have questions regarding this questionnaire or how it relates to your project.

It is rarely possible to know ahead of time the details of the technologies a vendor will propose. For this reason, you will get the best outcome if the questions remain as-is. Vendors are invited to mark those questions that do not apply to their set of technologies with NA (Not Applicable). In the rare case when there is detailed knowledge of what will be proposed beforehand, a narrowed set of questions may be possible, contact your BIT Point of Contact if you have questions about this.

**Vendors:** The following questions help the state determine the best way to assess your product or service technology for appropriate fit with the state’s technology needs. Some questions may not apply to the technology you use. In such cases, mark the question as NA (Not Applicable). Use the last column as needed to explain your answers. Questions with the Yes/No cells greyed out require you to explain your response. The more detailed the response, the better we can understand your product and/or service.

The “BIT” column corresponds to the branch that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact them on your behalf. DAT = Data Center; DEV = Development; TEL = Telecommunications; PMO = Project Management office

### Section A: System Security
The following questions are relevant for all vendors or third-parties engaged in this application or service, and pertain to relevant security practices and procedures for your system and coding.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>DAT</td>
<td>Is a user required to change their password? How often? What are the complexity requirements for the passwords? (BIT password requirements are available in Section 230.67.4.4 of the Information Technology Security Policy which can be supplied upon request).</td>
<td>YES</td>
</tr>
<tr>
<td>A2</td>
<td>DEV TEL</td>
<td>Will the system implement its own level of security?</td>
<td>NO</td>
</tr>
<tr>
<td>A3</td>
<td>DAT TEL x</td>
<td>Will the system provide Internet security functionality on public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?</td>
<td>NA</td>
</tr>
<tr>
<td>A4</td>
<td>TEL x</td>
<td>Will the system provide Internet security functionality on a public portal to include firewalls?</td>
<td>NA</td>
</tr>
<tr>
<td>A5</td>
<td>PMO</td>
<td>Will the system distinguish between local versus global administrators where local administrators have rights to user management only for the program area that they are associated with and global administrators have rights for the entire system?</td>
<td>NA</td>
</tr>
<tr>
<td>A6</td>
<td>DAT TEL</td>
<td>Does the application contain mitigations for risks associated to uncontrolled login attempts (response latency, re-Captcha, lockout, IP</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>A7</td>
<td>DAT</td>
<td>Are account credentials hashed and encrypted when stored?</td>
<td></td>
</tr>
<tr>
<td>A8</td>
<td>DAT TEL x</td>
<td>The protection of the State’s system and data is of upmost importance. Security scans must be done if:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>· An application will be placed on the State’s system;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>· The State’s system connects to another system;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>· The vendor stores or processes State data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The State would want to scan a test system; not a production system and will not do penetration testing.</strong> The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes. Is any of this an issue? If so, please explain.</td>
<td></td>
</tr>
<tr>
<td>A9</td>
<td>DAT</td>
<td>Will SSL traffic be decrypted and inspected?</td>
<td></td>
</tr>
<tr>
<td>A10</td>
<td>PMO x</td>
<td>Will organizations other than the State of South Dakota have access to our data?</td>
<td></td>
</tr>
<tr>
<td>A11</td>
<td>PMO</td>
<td>Will the State’s data be protected?</td>
<td></td>
</tr>
<tr>
<td>A12</td>
<td>DEV TEL</td>
<td>Describe the training your company offers related to defining security requirements, secure architecture and design, secure coding practices, and security testing.</td>
<td></td>
</tr>
<tr>
<td>A13</td>
<td>DEV TEL</td>
<td>Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?</td>
<td></td>
</tr>
<tr>
<td>A14</td>
<td>DEV</td>
<td>Are there some requirements for security that are “structured” as part of general releasability of a product and others that are “as needed” or “custom” for a particular release?</td>
<td></td>
</tr>
<tr>
<td>A15</td>
<td>TEL</td>
<td>What process is utilized by your company to prioritize security related enhancement requests?</td>
<td></td>
</tr>
<tr>
<td>A16</td>
<td>TEL</td>
<td>What threat assumptions were made, if any, when designing protections for the software and information assets processed?</td>
<td></td>
</tr>
<tr>
<td>A17</td>
<td>TEL</td>
<td>How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?</td>
<td></td>
</tr>
<tr>
<td>A18</td>
<td>TEL</td>
<td>What security criteria, if any, are considered when selecting third-party suppliers?</td>
<td></td>
</tr>
</tbody>
</table>
| A19 | TEL | How has the software been measured/assessed for its resistance to identified, relevant attack patterns such as Common Vulnerabilities &
<p>| A20 | TEL | Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available. |
| A21 | DAT | Are static or dynamic software security analysis tools used to identify weaknesses in the software that can lead to exploitable vulnerabilities? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results? |
| A22 | DAT | Has the product undergone any penetration testing? If yes, when, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated? |
| A23 | DEV | Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)? If yes, please explain. |
| A24 | DAT | Does your company publish a security section on its website? If so, do security researchers have the ability to report security issues? |
| A25 | DAT | Does your company have an executive-level officer responsible for the security of your company’s software products and/or processes? |
| A26 | DAT | Are security requirements developed independently of the rest of the requirements engineering activities? Or are they integrated into the mainstream requirements activities? |
| A27 | DAT | Does the software have any security critical dependencies or need additional controls from other software (e.g., operating system, directory service, application), firmware, or hardware? If yes, please describe. |
| A28 | DAT | What risk management measures are used during the software’s design to mitigate risks posed by use of third-party components? |
| A29 | DAT | Does your company perform background checks on members of the software development team? If so, are there any additional “vetting” checks done on people who work on critical application components, such as security? Explain. |
| A30 | DEV | Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle? Explain. |
| A31 | TEL | What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced? |
| A32 | DAT | Is two-factor authentication used for administrative control of all security devices and critical information systems? |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A33</td>
<td>DAT</td>
<td>Do you have an automated security event management system?</td>
</tr>
<tr>
<td>A34</td>
<td>DAT</td>
<td>Are security logs and audit trails protected from tampering or modification?</td>
</tr>
<tr>
<td>A35</td>
<td>DAT</td>
<td>It is State policy that if your system connects to another system providing SaaS, IaaS, or PaaS that this system has a security scan. The State would want to scan a test system; not a production system. Is this an issue? If so, please explain.</td>
</tr>
<tr>
<td>A36</td>
<td>DAT</td>
<td>A) Will the system support authentication?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B) Does the system give clues about valid username or password content or structure, for example when a user forgets their username or after a failed login attempt?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C) Are usernames and passwords generated by the system using user-specific information such as last name or birthdate?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If Yes to these, please explain.</td>
</tr>
<tr>
<td>A37</td>
<td>DEV</td>
<td>Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?</td>
</tr>
<tr>
<td>A38</td>
<td>TEL</td>
<td>What type of firewalls (or application gateways) do you use? How are they monitored/managed?</td>
</tr>
<tr>
<td>A39</td>
<td>TEL</td>
<td>What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?</td>
</tr>
<tr>
<td>A40</td>
<td>DAT TEL</td>
<td>What are your procedures for intrusion detection, incident response, and incident investigation/escalation?</td>
</tr>
<tr>
<td>A41</td>
<td>DAT TEL</td>
<td>How do you control physical and electronic access to the log files? Are log files consolidated to single servers?</td>
</tr>
<tr>
<td>A42</td>
<td>DAT TEL</td>
<td>Describe your security testing processes.</td>
</tr>
<tr>
<td>A43</td>
<td>DAT TEL</td>
<td>Do you have a BYOD policy that allows your staff to put any sort of sensitive or legally protected State data on their device personal device(s) or other non-company owned system(s)?</td>
</tr>
<tr>
<td>A44</td>
<td>DAT TEL</td>
<td>Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data? If yes, please explain your practices on multifactor authentication including the authentication level used as defined in NIST 800-63 in your explanation. If no, do you plan on going to multifunction authentication? If so, when?</td>
</tr>
<tr>
<td>A45</td>
<td>PMO</td>
<td>Will this system provide the capability to track data entry/access by the person, date and time?</td>
</tr>
</tbody>
</table>
## Section A: Data Encryption

Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.

## Section B: Device and Software Security

A47 DAT

- a. Do you have a SOC 2 audit report?
- b. Is the audit done annually?
- c. Does the audit cover all 5 of the trust principles?
- d. Does the audit include subservice providers?
- e. Has the auditor always been able to attest to an acceptable audit result?
- f. Will you provide a copy of your latest SOC 2 audit upon request, a redacted version is acceptable.

A48 DAT

Are you providing a device or software that is a part of the Internet of Things (IoT)? If yes, what is your process for ensuring the software on your IoT devices that are connected to the state's system, either permanently or intermittently, are maintained and/or updated?

### Section B: Hosting

Only for Vendor hosted applications, systems, databases, services and any other technology not hosted on the State's infrastructure. Mark the questions as “NA” if this is an application hosted by the State.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>PMO</td>
<td>Typically the State of South Dakota prefers to host all systems. In the event that the State decides that it would be preferable for the vendor to host the system, is this an option?</td>
</tr>
<tr>
<td>B2</td>
<td>PMO</td>
<td>Are there expected periods of time where the application will be unavailable for use?</td>
</tr>
<tr>
<td>B3</td>
<td>DAT</td>
<td>If you have agents or scripts executing on servers of hosted applications and what are the procedures for reviewing the security of these scripts or agents?</td>
</tr>
<tr>
<td>B4</td>
<td>DAT</td>
<td>What are the procedures and policies used to control access to the servers? How are audit logs maintained?</td>
</tr>
<tr>
<td>B5</td>
<td>DAT</td>
<td>Do you have a formal disaster recovery plan? Please explain what actions will be taken to recover from a disaster? Are warm or hot backups available?</td>
</tr>
<tr>
<td>B6</td>
<td>DAT</td>
<td>What are the set of controls to ensure separation of data and security information between different customers that are physically located in the same data center? On the same host server?</td>
</tr>
</tbody>
</table>
What are your data backup policies and procedures? How frequently are your backup procedures verified?

Are you or if the data is being hosted by a subservice provider are they FedRAMP certified?

If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with:
- Security for their I/T systems;
- Staff vetting;
- Staff security training?

If yes, summarize the contractual requirements.

If yes, how do you evaluate the third-party’s adherence to the contractual requirements?

If your application is hosted by you or a third party, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?

Do you use a security checklist when standing up any outward facing system?

Do you test after the system was stood up to make sure everything in the checklist was correctly set?

Will you provide the State with a copy of your checklist?

Are your Internet of Things (IoT) devices segmented from your network?

---

**Section C: Database**

Applies to any application or service that stores data, regardless of the application being hosted by the state or the vendor.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>DAT</td>
<td>Will the system require a database?</td>
<td>YES</td>
</tr>
<tr>
<td>C2</td>
<td>DAT</td>
<td>Will the system infrastructure require database replication?</td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>DAT</td>
<td>Will the system require transaction logging for database recovery?</td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td>DAT</td>
<td>How does data enter the system (transactional or batch or both)?</td>
<td></td>
</tr>
<tr>
<td>C5</td>
<td>PMO</td>
<td>Is the system data exportable by the user for use in tools like Excel or Access?</td>
<td></td>
</tr>
<tr>
<td>C6</td>
<td>PMO</td>
<td>Will user customizable data elements be exportable also?</td>
<td></td>
</tr>
<tr>
<td>C7</td>
<td>DAT</td>
<td>Will the State of South Dakota have access to the underlying data and data model for ad hoc reporting purposes? If yes, will the access be on-site or off-site?</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>BIT</td>
<td>Question</td>
<td>Response</td>
</tr>
<tr>
<td>----</td>
<td>-----</td>
<td>--------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>C8</td>
<td>DAT DEV</td>
<td>Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?</td>
<td></td>
</tr>
<tr>
<td>C9</td>
<td>DAT DEV</td>
<td>Will the system infrastructure require a Business Intelligence solution?</td>
<td></td>
</tr>
</tbody>
</table>

**Section D: Vendor Process**

The following questions are relevant for all vendors or third-parties engaged in this application or service and pertain to business practices. If the application is hosted by the vendor or the vendor supplies cloud services those questions dealing with installation or support of applications on the State’s system can be marked “NA”.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>DAT PMO</td>
<td>Will the vendor provide assistance with installation?</td>
<td></td>
</tr>
<tr>
<td>D2</td>
<td>DAT DEV PMO TEL</td>
<td>Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?</td>
<td></td>
</tr>
<tr>
<td>D3</td>
<td>TEL</td>
<td>In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?</td>
<td></td>
</tr>
<tr>
<td>D4</td>
<td>DEV</td>
<td>What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing and integrated testing)?</td>
<td></td>
</tr>
<tr>
<td>D5</td>
<td>TEL</td>
<td>Who and when are security tests performed on the product? Are tests performed by an internal test team, by an independent third party, or by both?</td>
<td></td>
</tr>
<tr>
<td>D6</td>
<td>DEV</td>
<td>Are misuse test cases included to exercise potential abuse scenarios of the software?</td>
<td></td>
</tr>
<tr>
<td>D7</td>
<td>TEL</td>
<td>What release criteria does your company have for its products with regard to security?</td>
<td></td>
</tr>
<tr>
<td>D8</td>
<td>DEV</td>
<td>What controls are in place to ensure that only the accepted/released software is placed on media for distribution?</td>
<td></td>
</tr>
<tr>
<td>D9</td>
<td>DAT DEV</td>
<td>Is there a Support Lifecycle Policy within the organization for the software in question? Does it outline and establish a consistent and predictable support timeline?</td>
<td></td>
</tr>
<tr>
<td>D10</td>
<td>DAT</td>
<td>How will patches and/or Service Packs be distributed to the Acquirer?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>1</strong></td>
<td><strong>DEV</strong></td>
<td>What services does the help desk, support center, or (if applicable) online support system offer and when are these services available?</td>
<td></td>
</tr>
<tr>
<td><strong>2</strong></td>
<td><strong>DAT</strong></td>
<td>How extensively are patches and Service Packs tested before they are released?</td>
<td></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td><strong>DAT</strong></td>
<td>Can patches and Service Packs be uninstalled? Are the procedures for uninstalling a patch or Service Pack automated or manual?</td>
<td></td>
</tr>
<tr>
<td><strong>4</strong></td>
<td><strong>DAT</strong></td>
<td>How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?</td>
<td></td>
</tr>
<tr>
<td><strong>5</strong></td>
<td><strong>DAT</strong></td>
<td>How do you set the relative severity of defects and how do you prioritize their remediation?</td>
<td></td>
</tr>
<tr>
<td><strong>6</strong></td>
<td><strong>DAT</strong></td>
<td>What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches?</td>
<td></td>
</tr>
<tr>
<td><strong>7</strong></td>
<td><strong>DAT</strong></td>
<td>Are third-party developers contractually required to follow your configuration management policies?</td>
<td></td>
</tr>
<tr>
<td><strong>8</strong></td>
<td><strong>DEV</strong></td>
<td>What policies and processes does your company use to verify that software components do not contain unintended, “dead,” or malicious code? What tools are used?</td>
<td></td>
</tr>
<tr>
<td><strong>9</strong></td>
<td><strong>DEV</strong></td>
<td>How is the software provenance verified (e.g. any checksums or signatures)?</td>
<td></td>
</tr>
<tr>
<td><strong>10</strong></td>
<td><strong>DEV</strong></td>
<td>Does the documentation explain how to install, configure, and/or use the software securely? Does it identify options that should not normally be used because they create security weaknesses?</td>
<td></td>
</tr>
<tr>
<td><strong>11</strong></td>
<td><strong>DAT</strong></td>
<td>Does your company’s defect classification scheme include security categories?</td>
<td></td>
</tr>
<tr>
<td><strong>12</strong></td>
<td><strong>DAT</strong></td>
<td>Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration following installation?</td>
<td></td>
</tr>
<tr>
<td><strong>13</strong></td>
<td><strong>DEV</strong></td>
<td>Does your company develop security measurement objectives for phases of the SDLC? Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?</td>
<td></td>
</tr>
<tr>
<td><strong>14</strong></td>
<td><strong>DEV</strong></td>
<td>How is the assurance of software produced by third-party developers assessed?</td>
<td></td>
</tr>
<tr>
<td><strong>15</strong></td>
<td><strong>DEV</strong></td>
<td>Does your company have a vulnerability management and reporting policy? Is it available for review?</td>
<td></td>
</tr>
<tr>
<td><strong>16</strong></td>
<td><strong>DAT</strong></td>
<td>What are the procedures for evaluating any vendor security alerts and installing patches and Service Packs?</td>
<td></td>
</tr>
<tr>
<td><strong>17</strong></td>
<td><strong>DAT</strong></td>
<td>Is testing done after changes are made to servers? What are your rollback procedures in the event of problems resulting from installing a patch or Service Pack?</td>
<td></td>
</tr>
<tr>
<td>D28</td>
<td>DAT</td>
<td>What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?</td>
<td></td>
</tr>
<tr>
<td>D29</td>
<td>DAT TEL</td>
<td>How are virus prevention, detection, correction, and updates handled for the products?</td>
<td></td>
</tr>
<tr>
<td>D30</td>
<td>DAT TEL</td>
<td>Do you perform regular reviews of system and network logs for security issues?</td>
<td></td>
</tr>
<tr>
<td>D31</td>
<td>DAT PMO</td>
<td>Do you provide security performance measures to the customer at regular intervals?</td>
<td></td>
</tr>
<tr>
<td>D32</td>
<td>DAT PMO</td>
<td>Is there an installation guide available and will you provide a copy to the State?</td>
<td></td>
</tr>
<tr>
<td>D33</td>
<td>DAT DEV PMO TEL</td>
<td>Will the implementation plan include user acceptance testing?</td>
<td></td>
</tr>
<tr>
<td>D34</td>
<td>DAT DEV PMO TEL</td>
<td>Will the implementation plan include performance testing?</td>
<td></td>
</tr>
<tr>
<td>D35</td>
<td>DAT DEV PMO TEL</td>
<td>What technical documentation will be provided to the State?</td>
<td></td>
</tr>
<tr>
<td>D36</td>
<td>DEV PMO</td>
<td>Will there be documented test cases for future releases including any customizations done for the State of South Dakota?</td>
<td></td>
</tr>
<tr>
<td>D37</td>
<td>PMO</td>
<td>Is the user manual electronically available and can the manual be printed?</td>
<td></td>
</tr>
<tr>
<td>D38</td>
<td>PMO</td>
<td>Describe your Support and on-line assistance options and any additional costs associated with the options.</td>
<td></td>
</tr>
<tr>
<td>D39</td>
<td>DAT PMO</td>
<td>Is there a method established to communicate availability of system updates?</td>
<td></td>
</tr>
<tr>
<td>D40</td>
<td>DEV PMO</td>
<td>If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?</td>
<td></td>
</tr>
<tr>
<td>D41</td>
<td>DEV PMO</td>
<td>Has your company ever conducted a project where your product was load tested?</td>
<td></td>
</tr>
<tr>
<td>D42</td>
<td>DEV PMO</td>
<td>Have you ever created a User Acceptance Test plan and test cases? If yes, what were the test cases? Do you do software assurance?</td>
<td></td>
</tr>
<tr>
<td>D43</td>
<td>PMO</td>
<td>Is there a strategy for mitigating unplanned disruptions and what is it?</td>
<td></td>
</tr>
<tr>
<td>D44</td>
<td>DAT</td>
<td>Please explain the pedigree of the software. Include in your answer who are the people, organization and processes that created the software.</td>
<td></td>
</tr>
<tr>
<td>D45</td>
<td>DAT</td>
<td>Explain the change management procedure used to identify the type and extent of changes allowed in the software throughout its lifecycle. Include</td>
<td></td>
</tr>
</tbody>
</table>
information on the oversight controls for the change management procedure.

| **D46** TEL | Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Provide a brief explanation. Will the supplier indemnify the Acquirer from these issues in the license agreement? Provide a brief explanation. |
| **D47** DEV | What are the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers) techniques, etc. used to produce and transform the software (brief summary response)? |
| **D48** DAT DEV | Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool? |
| **D49** DAT DEV TEL | What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review? |
| **D50** DEV | Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source. |
| **D51** DAT | Does the organization ever perform site inspections/policy compliance audits of its U.S. development facilities? Of its non-U.S. facilities? Of the facilities of its third-party developers? If yes, how often do these inspections/audits occur? Are they periodic or triggered by events (or both)? If triggered by events, provide examples of “trigger” events. |
| **D52** DEV | When does security testing occur during the SDLC (e.g., unit level, subsystem, system, certification and accreditation)? |
| **D53** DAT TEL | How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated? |
| **D54** DAT TEL | Do you perform penetration testing of the service? If yes, how frequently are penetration tests performed? Are the tests performed by internal resources or by a third party? |
| **D55** DAT | How frequently is the security tests performed? Are the tests performed by internal resources or by a third party? |
| **D56** DAT DEV | Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom. |
| **D57** DAT TEL | What is your process for ensuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated? |
It is State policy that all Vendor/Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Netscaler. Would this affect the implementation of the system?

The Vendors/Contractors are also expected to reply to follow-up questions in response to the answers they provided to the security questions. At the State’s discretion, a vendor’s answers to the follow-up questions may be required in writing and/or verbally. The answers provided may be used as part of the vendor selection criteria. Is this acceptable?

(For PHI only)

a. Have you done a risk assessment? If yes, will you share it?

b. If you have not done a risk assessment, would you be willing to do one based on the Health and Human Services assessment tool (https://www.healthit.gov/providers-professionals/security-risk-assessment-tool)? If yes, will you share it? The State is willing to sign a Non-disclosure Agreement before viewing any risk assessment.

c. If you have not done a risk assessment, when are you planning on doing one?

Will your web site and/or web application conform to the accessibility requirements of the Web Content Accessibility Guidelines 2.0? If not discuss what steps you take to make your web site and/or web application accessible. The guidelines can be found at http://www.w3.org/TR/WCAG20/.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
<th>Explain answer as needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>DEV PMO</td>
<td>What is the development technologies used for this system? Please indicate version as appropriate</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>ASP.Net</td>
<td>VB.Net</td>
<td>C#.Net</td>
<td>.NET Framework</td>
<td></td>
</tr>
<tr>
<td>Java/JSP</td>
<td>MS SQL</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**E2** DAT TEL  Is this a browser based User Interface?

**E3** DEV PMO  Will the system have any workflow requirements?

**E4** DAT  Can the system be implemented via Citrix?

**E5** DAT  Will the system print to a Citrix compatible networked printer?

**E6** TEL  If your application does not run under the latest Microsoft operating system, what is your process for updating the application?

**E7** DEV  Identify each of the Data, Business and Presentation layer technologies your product would use and provide a roadmap outlining how your release and or update roadmap aligns with the release and or update roadmap for this technology.

**E8** TELx  Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, JavaFX, Microsoft Silverlight, PHP or QuickTime? If yes, explain?

**E9** DEV  In order to connect to other applications or data, will the State be required to develop custom interfaces?

**E10** DEV  In order to fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?

**E11** DEV PMO  Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?

**E12** DAT  If the product is hosted at the State, will there be any third-party application(s) or system(s) installed or embedded to support the product (for example, database software, run libraries)? If so, please list those third-party application(s) or system(s).

**E13** DEV  What coding and/or API standards are used during development of the software?

**E14** DEV  Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?

**E15** DEV  How does the software’s exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>E16</td>
<td>DEV</td>
<td>Does the exception-handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E17</td>
<td>DEV</td>
<td>What percentage of code coverage does your testing provide?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| E18 | DAT | A) Will the system infrastructure involve the use of email?  
B) Will the system infrastructure require an interface into the State's email infrastructure?  
C) Will the system involve the use of bulk email distribution to State users? Client users? In what quantity will emails be sent, and how frequently? |   |   |
| E19 | TEL | A) Does your application use Java?  
B) If yes, is it locked into a certain version?  
C) Will it use the latest version of Java?  
D) If so, what is your process for updating the application? |   |   |
| E20 | DAT | Explain how and where the software validates (e.g., filter with white listing) inputs from untrusted sources before being used. |   |   |
| E21 | TEL | Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user)? Is it designed to isolate and minimize the extent of damage possible by a successful attack? |   |   |
| E22 | TEL | Does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)? |   |   |
| E23 | DEV | Do you use open source software or libraries? If yes, do you check for vulnerabilities in your software or library that are listed in:  
a. Common Vulnerabilities and Exposures (CVE) database?  
b. Open Source Vulnerability Database (OSVDB)?  
c. Open Web Application Security Project (OWASP) Top Ten? |   |   |

Section F: Infrastructure  
This pertains to how your system interacts with the State’s technology infrastructure. If the proposed technology does not interact with the State’s system the questions can be marked as “NA”.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>TEL</td>
<td>Is there a workstation install requirement?</td>
<td>YES</td>
</tr>
<tr>
<td>F2</td>
<td>DAT</td>
<td>Will the system infrastructure have a special backup requirement?</td>
<td></td>
</tr>
<tr>
<td>F3</td>
<td>DAT</td>
<td>Will the system infrastructure have any processes that require scheduling?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>F5</strong></td>
<td><strong>TEL</strong></td>
<td>Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines?</td>
<td></td>
</tr>
<tr>
<td><strong>F6</strong></td>
<td><strong>DAT</strong></td>
<td>It is State policy that all systems must be compatible with BIT’s dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?</td>
<td></td>
</tr>
<tr>
<td><strong>F7</strong></td>
<td><strong>TEL</strong></td>
<td>It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system? If yes, explain.</td>
<td></td>
</tr>
<tr>
<td><strong>F8</strong></td>
<td><strong>DAT</strong></td>
<td>It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. If need is determined by the State, would this affect the implementation of the system? If yes, explain.</td>
<td></td>
</tr>
<tr>
<td><strong>F9</strong></td>
<td><strong>DAT</strong></td>
<td>The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system? If yes, explain.</td>
<td></td>
</tr>
<tr>
<td><strong>F10</strong></td>
<td><strong>TEL</strong></td>
<td>It is State policy that all access from outside of the State of South Dakota’s private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system? If yes, explain.</td>
<td></td>
</tr>
<tr>
<td><strong>F11</strong></td>
<td><strong>TEL</strong></td>
<td>It is State policy that systems must support NAT and PAT running inside the State Network. Would this affect the implementation of the system? If yes, explain.</td>
<td></td>
</tr>
<tr>
<td><strong>F12</strong></td>
<td><strong>TEL</strong></td>
<td>It is State policy that systems must not use dynamic TCP or UDP ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would this affect the implementation of the system? If yes, explain.</td>
<td></td>
</tr>
<tr>
<td><strong>F13</strong></td>
<td><strong>DAT</strong></td>
<td>The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?</td>
<td></td>
</tr>
<tr>
<td><strong>F14</strong></td>
<td><strong>DEV</strong></td>
<td>Does your product run on Citrix Metaframe?</td>
<td></td>
</tr>
<tr>
<td>F15</td>
<td>PMO TEL</td>
<td>Please describe the types and levels of network access your system/application will require. This should include, but not be limited to: TCP/UDP ports used, protocols used, source and destination networks, traffic flow directions, who initiates traffic flow, whether connections are encrypted or not, and types of encryption used. Vendor should specify what access requirements are for user access to the system and what requirements are for any system level processes. Vendor should describe all requirements in details and provide full documentation as to the necessity of the requested access.</td>
<td></td>
</tr>
<tr>
<td>F16</td>
<td>PMO</td>
<td>List any hardware or software you propose to use that is not State standard, the standards can be found at <a href="http://bit.sd.gov/#">http://bit.sd.gov/#</a>.</td>
<td></td>
</tr>
<tr>
<td>F17</td>
<td>DAT</td>
<td>If your application is hosted on the State’s infrastructure, will it require a dedicated environment?</td>
<td></td>
</tr>
<tr>
<td>F18</td>
<td>DEV PMO</td>
<td>Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?</td>
<td></td>
</tr>
<tr>
<td>F19</td>
<td>DAT</td>
<td>Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?</td>
<td></td>
</tr>
<tr>
<td>F20</td>
<td>DAT</td>
<td>What are your policies and procedures for hardening servers?</td>
<td></td>
</tr>
<tr>
<td>F21</td>
<td>DAT TEL</td>
<td>Explain or provide a diagram of the architecture for the application including security mitigation.</td>
<td></td>
</tr>
<tr>
<td>F22</td>
<td>TEL x</td>
<td>What is your process for ensuring default remote login protocols and default passwords are disabled on Internet of Things (IoT) devices that are connected to your system either permanently or intermittently?</td>
<td></td>
</tr>
<tr>
<td>F23</td>
<td>DAT</td>
<td>Can the system be integrated with our enterprise Active Directory to ensure access is controlled?</td>
<td></td>
</tr>
<tr>
<td>F24</td>
<td>TEL x</td>
<td>It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies. Would this affect the implementation of the system?</td>
<td></td>
</tr>
<tr>
<td>F25</td>
<td>DAT x</td>
<td>Will the server-based software support:</td>
<td></td>
</tr>
<tr>
<td>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    &amp;n...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
F26 | TEL | All network systems must operate within the current configurations of the State of South Dakota’s firewalls, switches, IDS/IPS and desktop security infrastructure. Would this affect the implementation of the system?

F27 | DAT | It is State policy that all systems that require an email interface must leverage existing SMTP processes currently managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?

F28 | DAT | The State implements enterprise-wide anti-virus solutions on all servers and workstations as well as controls the roll-outs of any and all Microsoft patches based on level of criticality. Do you have any concerns in regards to this process?

F29 | DAT | What physical access do you require to work on hardware?

Section G: Business Process

These questions relate to how your business model interacts with and meets the State’s policies, procedures and practices. If the vendor is hosting the application or providing cloud services questions dealing with installation or support of applications on the State’s system can be marked “NA”.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1</td>
<td>DAT</td>
<td>If your application is hosted on a dedicated environment within the State’s infrastructure, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?</td>
<td></td>
</tr>
<tr>
<td>G2</td>
<td>PMO</td>
<td>Explain the software licensing model.</td>
<td></td>
</tr>
<tr>
<td>G3</td>
<td>DAT</td>
<td>Is on-site assistance available? If so, is there a charge?</td>
<td></td>
</tr>
<tr>
<td>G4</td>
<td>DEV</td>
<td>Will you provide customization of the system if required by the State of South Dakota?</td>
<td></td>
</tr>
<tr>
<td>G5</td>
<td>PMO</td>
<td>If yes, are there any additional costs for the customization?</td>
<td></td>
</tr>
<tr>
<td>G6</td>
<td>PMO</td>
<td>Will the source code for the system be put in escrow for the State of South Dakota? If yes, will you pay the associated escrow fees?</td>
<td></td>
</tr>
<tr>
<td>G7</td>
<td>PMO</td>
<td>Explain the basis on which pricing could change for the State based on your licensing model.</td>
<td></td>
</tr>
<tr>
<td>G8</td>
<td>PMO</td>
<td>Contractually, how many years price lock are you offering the State as part of your response? Also as part of your response, how many additional years are you offering to limit price increases and by what percent?</td>
<td></td>
</tr>
<tr>
<td>G9</td>
<td>PMO</td>
<td>Will the State of South Dakota own the data created in your hosting environment?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>G9</td>
<td>PMO</td>
<td>Will the State acquire the data at contract conclusion?</td>
<td></td>
</tr>
<tr>
<td>G10</td>
<td>PMO</td>
<td>Will the State’s data be used for any other purposes other than South Dakota’s usage?</td>
<td></td>
</tr>
<tr>
<td>G11</td>
<td>DAT</td>
<td>Has your company ever filed for Bankruptcy under U.S. Code Chapter 11? If so, please provide dates for each filing and describe the outcome.</td>
<td></td>
</tr>
<tr>
<td>G12</td>
<td>DAT</td>
<td>Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.</td>
<td></td>
</tr>
<tr>
<td>G13</td>
<td>DAT</td>
<td>Please summarize your company’s history of ownership, acquisitions, and mergers (both those performed by your company and those to which your company was subjected).</td>
<td></td>
</tr>
<tr>
<td>G14</td>
<td>DAT</td>
<td>Will you provide on-site support 24x7 to resolve security incidents?</td>
<td></td>
</tr>
<tr>
<td>G15</td>
<td>DEV</td>
<td>What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?</td>
<td></td>
</tr>
<tr>
<td>G16</td>
<td>DAT</td>
<td>Are help desk or support center personnel internal company resources or are these services outsourced to third parties?</td>
<td></td>
</tr>
<tr>
<td>G17</td>
<td>DAT</td>
<td>Are any of the services you plan to use located offshore (examples include data hosting, data processing, help desk and transcription services)?</td>
<td></td>
</tr>
<tr>
<td>G18</td>
<td>DAT</td>
<td>Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?</td>
<td></td>
</tr>
<tr>
<td>G19</td>
<td>DAT</td>
<td>What are your customer confidentiality policies? How are they enforced?</td>
<td></td>
</tr>
<tr>
<td>G20</td>
<td>DAT</td>
<td>Are you ISO 27001 certified? Is the certification done annually? Will you provide a copy of your certification report?</td>
<td></td>
</tr>
<tr>
<td>G21</td>
<td>DAT</td>
<td>(Use if PHI is involved) Are you HITRUST certified? Is the certification done annually? Will you provide a copy of your assessment?</td>
<td></td>
</tr>
<tr>
<td>G22</td>
<td>DAT</td>
<td>Will this application now or possibly in the future share PHI with other entities on other networks, be sold to another party or be accessed by anyone outside the US?</td>
<td></td>
</tr>
<tr>
<td>G23</td>
<td>DAT</td>
<td>If the product is hosted at the State, will there be a request to include an application to monitor license compliance?</td>
<td></td>
</tr>
<tr>
<td>G24</td>
<td>DAT</td>
<td>Is telephone assistance available for both installation and use? If yes, are there any additional charges?</td>
<td></td>
</tr>
</tbody>
</table>
Information Technology
Security Policy
Contractor Version 4.0
March 1, 2019
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center General-Data Center Security-Federal Tax Information</td>
<td>25</td>
</tr>
<tr>
<td>230.11.4.1. Federal Tax Information Returns and Return Information</td>
<td>26</td>
</tr>
<tr>
<td>230.11.4.2. What is Not Federal Tax Information</td>
<td>26</td>
</tr>
<tr>
<td>230.11.4.3. Safeguarding Federal Tax Information</td>
<td>26</td>
</tr>
<tr>
<td>230.11.4.4. Emailing Federal Tax Information</td>
<td>26</td>
</tr>
<tr>
<td>Data Center General-Procedural-Physical Access - Proximity Cards</td>
<td>26</td>
</tr>
<tr>
<td>230.58.4.1. Proximity Card for Non-BIT Employee Access</td>
<td>27</td>
</tr>
<tr>
<td>Data Center General-Data Center Security-Accounts Access Control and Authorization</td>
<td>27</td>
</tr>
<tr>
<td>230.67.4.1. Individual Access Authorization</td>
<td>28</td>
</tr>
<tr>
<td>230.67.4.2. Least Privilege</td>
<td>28</td>
</tr>
<tr>
<td>230.67.4.3. Password Requirements</td>
<td>28</td>
</tr>
<tr>
<td>230.67.4.4. Individual Access Termination</td>
<td>29</td>
</tr>
<tr>
<td>Data Center General-Payment Card Industry Data Security-Payment Card Industry Data Security Standard</td>
<td>29</td>
</tr>
<tr>
<td>230.72.4.1. Payment Card Industry Data Security Standard Requirements</td>
<td>30</td>
</tr>
<tr>
<td>Data Center General-Secure Information Technology Acquisition Policy-Secure Information Technology Acquisition Policy</td>
<td>30</td>
</tr>
<tr>
<td>230.73.4.1. Acquisition of Services Involving HIPAA Data</td>
<td>31</td>
</tr>
<tr>
<td>230.73.4.2. Security Scanning Requirements</td>
<td>31</td>
</tr>
<tr>
<td>230.73.4.3. Hardware Maintenance Agreements</td>
<td>31</td>
</tr>
<tr>
<td>Data Center General-Use of Production Data-Use of Production Data in a Non-Production Environment</td>
<td>31</td>
</tr>
<tr>
<td>230.74.4.1. Use of Production Data in a Non-Production Environment</td>
<td>32</td>
</tr>
<tr>
<td>230.74.4.2. Purging of Data</td>
<td>33</td>
</tr>
<tr>
<td>230.74.4.3. Compliance</td>
<td>33</td>
</tr>
<tr>
<td>Data Center General -Security Impacts-Data Classification</td>
<td>34</td>
</tr>
<tr>
<td>230.75.4.1. Data Classification System</td>
<td>34</td>
</tr>
<tr>
<td>230.75.4.2. Classification of Data Produced under Contract</td>
<td>35</td>
</tr>
<tr>
<td>230.75.4.3. Data Classification Responsibilities</td>
<td>35</td>
</tr>
<tr>
<td>Data Center General-Access to Confidential Data-Multi-Factor Authentication</td>
<td>36</td>
</tr>
<tr>
<td>230.76.4.1. Usage of Multi-Factor Authentication (MFA)</td>
<td>36</td>
</tr>
<tr>
<td>230.76.4.2. MFA Tokens</td>
<td>37</td>
</tr>
<tr>
<td>Data Center General-Approved Disposal of State Data-Media Sanitization</td>
<td>37</td>
</tr>
<tr>
<td>230.77.4.1. Sanitization of Media in a Contractor's Control</td>
<td>37</td>
</tr>
<tr>
<td>Data Center General-Transfer of Data-Secure Transfer of Data</td>
<td>38</td>
</tr>
<tr>
<td>230.78.4.1. Use of Secure File Transfer Protocol</td>
<td>39</td>
</tr>
<tr>
<td>Development-Application Security-Federal Tax Information</td>
<td>39</td>
</tr>
<tr>
<td>401.1.4.1. Allocation of Resources and Life Cycle Support</td>
<td>40</td>
</tr>
<tr>
<td>401.1.4.2. Information System Security Documentation</td>
<td>40</td>
</tr>
<tr>
<td>401.1.4.3. Software Usage Restrictions and User Installed Software</td>
<td>40</td>
</tr>
</tbody>
</table>
Development-Application Security-Security Assessments................................................................. 40
  401.3.4.1. Security Assessment ........................................................................................................... 41
  401.3.4.2. Assessment Report ............................................................................................................ 41
  401.3.4.3. Annual Review ................................................................................................................... 41
Development-Application Security-Data Encryption .......................................................... 42
  401.5.4.1. Data Encryption .................................................................................................................. 42
  401.5.4.2. Hashing Values ................................................................................................................... 42
  401.5.4.3. Tools .................................................................................................................................. 42
  401.5.4.4. Compliance Measurements ............................................................................................... 42
  401.5.4.5. Exceptions ........................................................................................................................ 43
  401.5.4.6. Non-Compliance ............................................................................................................... 43
Development-Application Security-Authentication and Authorization .......................... 43
  401.7.4.1. User Authentication and Authorization ........................................................................ 43
  401.7.4.2. Password Requirements .................................................................................................. 44
  401.7.4.3. Invalid Login Attempts for projects using Federal Tax Information ........................... 44
  401.7.4.4. reCAPTCHA .................................................................................................................... 44
  401.7.4.5. Tools .................................................................................................................................. 44
  401.7.4.6. Compliance Measurements ............................................................................................... 44
  401.7.4.7. Exceptions ........................................................................................................................ 44
  401.7.4.8. Non-Compliance ............................................................................................................... 44
Network-Service-Access Control......................................................................................... 45
  610.1.4.1. System Access Expectations ............................................................................................ 45
  610.1.4.2. Contractor Access ............................................................................................................ 46
  610.1.4.3. Modems ............................................................................................................................ 46
  610.1.4.4. Remote Access .................................................................................................................. 46
  610.1.4.5. Inspection and Review ....................................................................................................... 47
  610.1.4.6. Department of Social Services .......................................................................................... 47
Network-Concept-Security Domain Zones ........................................................................ 47
  610.3.4.1. Intranet ............................................................................................................................... 48
  610.3.4.2. DMZ .................................................................................................................................... 48
  610.3.4.3. Extranet .............................................................................................................................. 48
Network-Concept-Network Integrity....................................................................................... 48
  610.9.4.1. Responsibilities .................................................................................................................. 49
  610.9.4.2. Management ...................................................................................................................... 49
  610.9.4.3. Disabling Critical Components of Network Security Infrastructure ............................ 49
  610.9.4.4. Technical Asset or Contractor Connections ................................................................. 49
  610.9.4.5. Local Area Network .......................................................................................................... 49
  610.9.4.6. Wide Area Network ......................................................................................................... 49
610.9.4.7. Physical Controls ........................................................................................................................................ 49

Network-Communication-Internet .................................................................................................................................. 50
  610.11.4.1. Multiple Connections ................................................................................................................................. 50
  610.11.4.2. Interfaces .......................................................................................................................................................... 50
  610.11.4.3. Security ............................................................................................................................................................. 50
  610.11.4.4. Responsibilities .................................................................................................................................................. 50
  610.11.4.5. IPv4/IPv6 and Device Names .......................................................................................................................... 51

Security-Network Discovery-Probing-Exploiting .................................................................................................................... 51
  620.1.4.1. Limiting Tool Functionality ............................................................................................................................... 52
  620.1.4.2. Exploiting Security Controls of Information Systems .............................................................................................. 52
  620.1.4.3. Cracking Application or Passwords ....................................................................................................................... 52
  620.1.4.4. Exemptions ............................................................................................................................................................ 52

Security-Content Control-Internet Filtering ............................................................................................................................ 52
  620.5.4.1. Exemptions ............................................................................................................................................................ 53
  620.5.4.2. Appropriate Use of Administrator Access .......................................................................................................... 53
  620.5.4.3. DDN Content Filtering .......................................................................................................................................... 54
  620.5.4.4. DDN Intranet Content Filtering ............................................................................................................................. 54
  620.5.4.5. Filter Exemption Requests .................................................................................................................................. 54

TERMS....................................................................................................................................................................................... 55

ACRONYMS................................................................................................................................................................................. 63
<table>
<thead>
<tr>
<th>Policy Number</th>
<th>Policy Title</th>
<th>New</th>
<th>Revised</th>
<th>Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>220.1.4.3</td>
<td>Visibility of Server and Framework patching Status</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.74.4.1</td>
<td>Use of Production Data in a Non-Production Environment</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.67.4.6</td>
<td>Password Requirements</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.67.4.11</td>
<td>Non-Expiring Passwords</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.75.4.1</td>
<td>Data Classification System</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.76</td>
<td>Multi-Factor Authentication</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.77</td>
<td>Media Sanitization</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.78</td>
<td>Use of SFTP</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>401.5</td>
<td>Data Encryption</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>401.7</td>
<td>Authentication and Authorization</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>610.1</td>
<td>Access Control</td>
<td>03.01.2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.4.1</td>
<td>Background Checks</td>
<td>06.01.2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.67.4.2</td>
<td>User Privilege Capabilities</td>
<td>06.01.2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.74</td>
<td>Use of Production Data in a Non-Production Environment</td>
<td>06.01.2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>210.20</td>
<td>Disposition of Mainframe Output and Documentation</td>
<td>09.26.2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.9</td>
<td>Cloud Based Services and System Information</td>
<td>09.26.2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.67</td>
<td>Accounts Access Control and Authorization</td>
<td>09.26.2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.72</td>
<td>Payment Card Industry Data Security Standard</td>
<td>09.26.2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.74</td>
<td>Use of Production Data in a Non-Production Environment</td>
<td>09.26.2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>230.75</td>
<td>Data Classification</td>
<td>09.26.2018</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
General-Information Technology Security Policy-Introduction

1.1.1. Overview

This Information Technology (IT) Security Policy has been developed by the Bureau of Information & Telecommunications (BIT) of the State of South Dakota. The Information Technology Security Policy provides guidance regarding cyber security policies of the State relevant to the IT goals, beliefs, ethics, and responsibilities. Specific procedures that State employees and contractors must follow to comply with the security objectives are identified.

The objective of the Information Technology Security Policy is to provide a comprehensive set of cyber security policies detailing the acceptable practices for use of State of South Dakota IT resources. The security policies and procedures set forth are to accomplish the following:

- Assure proper implementation of security controls within the BIT environment.
- Assure government data is protected regardless of hosting location.
- Demonstrate commitment and support to the implementation of security measures by BIT and Executive management.
- Avoid litigation by documenting acceptable use of State IT resources.
- Achieve consistent and complete security across the diverse technology infrastructure of the State and hosted State data.

The Information Technology Security Policy, when combined with individual, specific security procedures, provides a comprehensive approach to security planning and execution to ensure that State managed assets are afforded appropriate levels of protection against destruction; loss; unauthorized access, change, or use; and disruption or denial of service.

BIT is responsible for maintaining and updating this policy. An updated version of the Information Technology Security Policy will be posted to the Intranet annually the first of March. The Commissioner of BIT or the Chief Information Security Officer can authorize an out of cycle or special edition to be released.

Information Technology Security is based on three principles:

- Confidentiality
- Integrity
- Availability

Confidentiality - ensuring that only permitted individuals are able to view information pertinent to apply defined responsibilities.

Integrity - the information is accurate because nothing has been changed or altered.

Availability - the technology infrastructure and services built upon that infrastructure are not intentionally disrupted and are available for use by the clientele in a dependable and reliable manner.

Each individual policy defined herein falls within one or more of these guiding principles.

Information Technology security requires on-going vigilance, and employees should understand the importance of cyber security in the protection of State data and technology resources along with the personal/home computing/data assets of every individual. Guardianship of State data, infrastructure, and applications is a critical...
priority for BIT. The effort is complicated by the balance needed between usability/service and meaningful protection.

BIT Mission Statement

The Bureau of Information and Telecommunications (BIT) strives to partner and collaborate with clients in support of their missions through innovative information technology consulting, systems, and solutions.

Vision

Through our highly motivated staff - we will be a Leader and valued partner in providing technology solutions, services, and support that directly contribute to the success of our clients.

Goals:

**Provide a Reliable, Secure and Modern Infrastructure.**
Provide a well-designed and architected secure computing and communications environment to ensure optimal service delivery to business. Architecture and process will be optimized to support agile and reliable computing and communication services.

Technology assets must be high performing and dependable to ensure services are available whenever needed. Centralization, standardization, and collaboration are vital to efficiently leverage investments. To maintain public trust, we must secure data and technology assets through leading security tools, policies, and practices.

**Deliver Valuable Services at Economical Costs.**
Develop innovative and cost-effective solutions through collaboration, cooperation, and in partnership with our clients. The solution sets include developing customized business solutions, efficient project management services, and productive relationships with clients.

Regarding our citizens interacting with their government: "People should be online, not waiting in line."

**Build and Retain a Highly Skilled Workforce.**
Improve the effectiveness, productivity, and satisfaction of employees in order to attract (and retain) a highly qualified workforce to foster individual innovation and professional growth. Appropriate training and tools will be provided to enhance and improve career skills in the workforce.

Information technology systems are critical, valuable assets. Policies relating to the valuable assets are important to ensure that all entities receive adequate information to enable the department, office, and agency to provide a basic level of protection to the technology systems.

**Security is not accomplished at a single point or by a single individual! (Or in a single point in time!)**

Instead of relying on one person or a firewall or anti-virus software or some other single piece of hardware or software, a series of assets and entities together build a safe computing environment. Technically, a layered approach is taken to accomplish security within the State which is called the Information Technology (IT) Security Model. A foundation is established; additional layers may build on the previous layer or may also act independently to provide separate security measures. Each point of accessibility into the wired and wireless network creates security concerns. Security is not limited to technology. A critical portion of cyber security is the human aspect.

**Information Technology Security Model**

The different technology layers of the Information Technology Security Model create opportunities for implementing security:
• **User Education** involves the training of employees to ensure that proper awareness is brought to the topic of security including steps to take when incidents occur that are outside of the scope of the daily work routine.

• **Physical Access** is taking appropriate steps to physically safeguard technical equipment such as outlining procedures to prevent workstations from being stolen which can include limiting access to a particular room or locking up the device in a cabinet.

• **Network Access** includes protecting the State Network from unauthorized access via internal methods and from outside our physical offices. Because technology can be manipulated by individuals or workstations to create a detrimental outcome, safeguards must be implemented to prevent, thwart, and repel workstation attacks from inside State Government and the Internet; access protection is not limited to workstations, it includes smartphones, Internet of Thing devices, environmental controls, and network - network connectivity.

• **Workstation Platform** means taking advantage of the inherent feature sets of workstation platforms. For example, user id and password capabilities must be used as intended within the workstation platform.

• **Cyber Strength Evaluation** of business software must apply across in-house developed and third party built or supplied software applications. New applications must be tested before being placed into service and existing applications must be re-evaluated on a regular basis.

• **Cyber security language** is incorporated within all information technology (I/T) requests for proposals and I/T contracts.

• **Information System security** entails designing the necessary security features and permissions to ensure that only legitimized staff have proper resource access. The design must consider areas such as viewers of departmental data to individuals that can add data or update records.

• **Data security** is the protection of the asset; often referred to as the "money in the vault". Insuring that data is only accessible by permitted applications and personnel is the core of the security model. The data could be credit card numbers, social security numbers, health records, or financial information.

**Partners**

The IT Security model goal is to ensure that the hardware, software, and data technology assets of the State are protected in a reasonable and prudent manner. Planning, cooperation, and assistance from many different entities is required to meet the goal. The State has various partners in cyber security efforts. BIT must continue to evolve relationships with:

- State government of South Dakota branches departments, and constitutional offices
- Internet Service Providers
- Multi-State Information and Sharing Center (MS ISAC)
- Department of Homeland Security
- State Fusion Center
- Federal Bureau of Investigation (FBI) - InfraGard program
- National Association of State Technology Directors (NASTD)
- National Association of Chief Information Officers (NASCIO)
- SysAdmin, Audit, Networking, and Security (SANS)
- Microsoft, Inc.
- Symantec, Inc.
- US CERT
- A variety of hardware and software contractors.

All of these organizations contribute to the development of cyber security information sharing, policies, procedures, and metrics. In return, specific reporting is distributed amongst the partners.

**Roles and Responsibilities**
In the application of information technology, BIT is responsible for providing leadership, policy, and technical support to all agencies of the Executive branch of the State of South Dakota. Also, various levels of support are provided to the Judicial branch, constitutional offices of government, K-12 education, and higher education. In addition to data center operations and related end user and customer support services, the broad statement of roles and responsibilities encompasses major information resource functions such as development, delivery, administration of voice, data, and video, applications - to include services, software, hardware selection, installation, and support.

Individual roles and responsibilities are defined herein; the following responsibilities are shared by all:

- Participate in information security awareness program activities.
- Read, understand, and follow the policies defined in the Information Technology Security Policy.
- Report all violations, security incidents, suspected, and/or attempted security incidents to BIT.

BIT Commissioner:

The Commissioner of the Bureau of Information & Telecommunications for the State of South Dakota is responsible for ensuring that:

- Reasonable security measures are taken to protect sensitive files and information.
- Enforceable security rules are created and disseminated.
- System resources are managed and monitored to ensure prudent and legitimate usage.
- Alleged security violations are addressed, and problems are investigated.
- Designated individuals are responsible for design, configuration, and support of technology resources.

Employees and Contractors are responsible for:

- Taking the time to read, understand, and ask questions if necessary to clarify the policies defined herein.
- Fully adhering to these policies defined herein.
- Agreeing that use of State technologies which includes equipment, applications, and resources are for work-related purposes.
- Applying recommended password policies.
- Safeguarding sensitive information whether employee / contractor is in the office or traveling for the State.
- Reporting any unusual requests for information or obvious security incidents to the BIT Help Desk.
- Immediately reporting loss of any State technology devices or data.
- Understanding that everyone is a potential target of nefarious individuals seeking 'social engineering' information to be used for illegally accessing State of South Dakota systems and technologies; Hence, be aware that any information provided to outside entities can be dangerous.
- Protecting information technology assets by following policies and procedures.
- Ensuring each individual is authorized to use a given technical asset.
- Understanding and complying with the policies, procedures, and laws related to conditions of use authorizing access to BIT systems and data.
- Not subverting or attempting to subvert security measures.

Department, Office, Division, or Group Managers are responsible for:

- Creating, disseminating, and enforcing conditions of use for technology and applications in areas of responsibility.
- Responding to concerns regarding alleged or real violations of this policy.
- Ensuring that their employees understand security responsibilities.
- Monitoring the use of South Dakota technology resources by observing usage.
• Determining the access requirements of staff, and ensuring completion of the appropriate forms, including all required authorizations for the application(s) requested by insuring only legitimate staff have access to the set of functions needed to perform defined tasks.
• Communicating terminations and status changes of individuals immediately to the Bureau of Human Resources (BHR) through BHR-defined procedures so that BIT is notified to ensure proper deletion or revision of user access is performed.
• Ensuring a secure physical environment for the staff use of State equipment, information systems, and data.

Bureau of Information & Telecommunications (BIT) is responsible for:

• Taking reasonable action to assure the authorized use and security of data, networks, applications, and communications amongst these technologies.
• Promptly responding to client questions on details relating to appropriate use of technical resources.
• Providing advice regarding the development of conditions of use or authorized use and procedures through work order requests.
• Ensuring that investigations into any alleged personal workstation or network security compromises, incidents, or problems are conducted.
• Ensuring that appropriate security controls are enabled and are being followed in coordination with BIT staff that are responsible for security administration.
• Verifying and authorizing individuals for an appropriate level of access to only the resources required to perform one's responsibilities.
• Overseeing that an individual has the necessary security authorizations in order for the person to perform assigned duties or tasks.
• Cooperating with appropriate departments, branches, agencies, and law enforcement officials in the course of investigation of alleged violations of policy or law.
• Overseeing the administration of BIT employee and contractor access to BIT facilities.
• Coordinating disaster recovery and testing exercises.

Data Owners

All data files, information, and applications belong to the State. Authorized users or agents of the data are the State of South Dakota departments, agencies, and offices. Files in central systems belong to the account owner. Data owners are responsible for:

• Tracking the data owned/managed by the agency and agency staff.
• Providing BIT notification within 24 hours of any notices regarding federal/state/or industry audits related to any aspects of an agency data, electronic communications, or data processing.
• Working with BIT to ensure access to the data and application(s) is limited to individuals with a legitimate need for the resource access.
• Ensuring that security measures and standards are implemented and enforced in a method consistent with BIT security policies and procedures.
• Establishing measures to ensure the integrity of the data and applications found within the owner's area of responsibility.
• Authorizing individual's appropriate security access rights for accessing the data and applications that are assigned to the data owner for administration.
• Periodically reviewing access rights to determine that the level is still appropriate for authorized users or the level needs to be changed.
• Assuring a process is in place to retain or purge information according to record retention schedules as set by the Records Management office of the Bureau of Administration or other entities.
• Determining the sensitivity and criticality of the data and application based on established Federal, State, and organizational definitions.
Compliance with system security and integrity; noncompliance and enforcement; reservation of authority and rights is expected of all employees and contractors.

- All State and contractor personnel utilizing information technology resources shall cooperate fully with the cyber security policies of the State.
- The State reserves the right to take all necessary actions to prevent the State network and computing infrastructure from being used to attack, damage, harm, or improperly exploit any internal or external systems or networks.
- The State reserves the right to take all necessary actions to protect the integrity of the State network, the systems attached to the State network, and the data contained therein.
- Violations of federal, State regulations, or any laws respecting information technology will be considered serious matters that may warrant loss of applicable privileges, fines, or more serious action as necessary, to include but not limited, appropriate disciplinary action.

Individuals with questions concerning the policies described herein should be directed to either an immediate State supervisor or the BIT Help Desk for assignment to the most pertinent BIT Division.

Compliance and Enforcement:

All managers and supervisors are responsible for enforcing the Security Awareness policy.

Any disclosure of regulated data is subject to the Human Resource Policies of BHR.

1.1.2. Purpose

This Information Technology Security Policy contains information technology security policies to ensure that employees and contractors are familiar with the laws and regulations that govern use of IT systems and the data those systems contain.

1.1.3. Scope

The Information Technology Security Policy is intended to address the range of cyber security related topics. Detailed policies are listed and explained throughout the document. Security topics included are workstation, server, network, applications development, mobile, administrative, operational, and other IT areas.

The clientele served by BIT is very diverse. Including the Executive and Judicial branches of State government, local - municipal - county governments, K-12 schools, technical schools, and colleges and universities. Different policies will have a different set of impacted clienteles.

1.1.3.1. Scope Assumptions

The security policies listed within the Information Technology Security Policy apply to State employees and contractors working on or with State of South Dakota IT equipment, data, or services. All are expected to comply with BIT cyber security policies.

1.1.3.2. Scope Constraints

Contractors are not given any special privileges or dispensations regarding policies listed herein. Contractors are expected to follow all policies designated as an employee would follow them. Third party hosting companies also have a set of policies applicable to them. This set of policies is normally a subset of the entire BIT catalog of policies.
1.1.4. Policy

1.1.4.1. General
The policy of BIT is that information is considered a valuable asset and must be appropriately evaluated and protected against all forms of unauthorized access, use, disclosure, modification, or destruction. Security controls must be sufficient to ensure the confidentiality, integrity, availability, and accountability of sensitive and critical information processed and stored on BIT resources and other hosting parties.

In addition to implementing the necessary safeguards, each State department, office, and agency is required to determine that the proper levels of protection for the information for that entity exists to include information that is under the control of the department, office, or agency. The security controls that must be applied will be consistent with the classification or value of the information and associated processes that the security controls are designed to protect. Information that is considered by management to be sensitive, critical, or sensitive and critical requires more stringent controls.

1.1.4.2. Chief Information Security Officer
The Commissioner of BIT shall appoint a Chief Information Security Officer (CISO) to implement the information technology security program for the State. The CISO shall seek to assure that information technology is secure at the State and shall be responsible for the following duties:

- Enforcing the provisions of the Information Technology Security Policy.
- Providing for and implementing, in cooperation with the Data Center, Development, and Telecommunications Divisions of BIT, a written process to investigate any violations or potential violations of this policy or any policy regarding system security and integrity, individually or in cooperation with any appropriate State law enforcement or investigative official.
- Implementing training and education programs to ensure government employees are aware of the risks and expected behaviors towards cyber security.
- Keeping a record of system integrity problems and incidents.
- Maintaining and updating the Information Technology Security Policies.
- Taking such emergency action as is reasonably necessary to provide system control where security is deemed to have been lost or jeopardized.
- Performing periodic security surveys.
- Providing for network security by seeking to preclude misuse of the network of the State to gain or attempt to gain unauthorized access to any system.
- Performing checks of information systems to assess system security and integrity, as well as to determine the use or placement of illegal or improper software or equipment.
- Coordinating the cyber security activities across BIT to ensure technology services and IT policies are effective in balancing security requirements vs. client needs.
- Ensuring processes are in place to remove all data before equipment is disposed or redeployed.
- Coordinating and consulting with the BIT Security Infrastructure Team (SIT), Executive Working Group on Cyber Security, other State departments, Board of Regents, K-12 community, federal Department of Homeland Security, and Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Implementing decisions of the State concerning information technology security.
- Providing reports directly to the Office of the Governor where any serious security violation or potential challenge to security occurs.
- Leading the BIT Security Infrastructure Team.
- Leading the Executive Working Group on Cyber Security.

1.1.4.3. Security Infrastructure Team (SIT)
The SIT shall, in coordination with the CISO, recommend technology solutions, written policies, and procedures necessary for assuring the security and integrity of State information technology. The SIT shall coordinate with the CISO in creating and implementing a written system to investigate any violations or potential violations of this policy or any policy regarding system security and integrity.
The CISO shall appoint the Security Infrastructure Team members.
The SIT shall be chaired by the CISO.
At a minimum, the SIT communicates internally every two weeks, via a scheduled bi-weekly meeting or via email, the current security posture of the State.
The SIT shall consist of at least one member from each of the BIT information technology divisions.
The recommendation is that membership include multiple representation from development, systems integration, desktop support, networking.
K-12, Regental, Judicial, Legislative, and other government entities can be invited at the discretion of the CISO.

1.1.4.4. Security Operations Team (SOT)
The Security Operations Team (SOT) shall be appointed by the CISO. The SOT meets daily to review any cyber security findings or issues with the State Infrastructure within the previous day. The SOT includes members of the Telecommunications, Data Center, and Development divisions.

- Logs are fed into the State security information and event management system and are monitored by the SOT daily. These logs include firewall, intrusion detection, intrusion prevention, desktop protection, audit logs, etc.
- The SOT meets daily to review any findings or issues.
- Plans of action are established with assignments established based on the deficiencies.

The SOT can make recommendations and suggestions to the SIT for operational considerations.

1.1.4.5. BIT Executive Working Group on Cyber Security
The Executive Working group shall be informed and educated on matters regarding cyber security. They shall offer their perspective and feedback on technology, policies and other important matters.

- At the CISO's discretion, the members of the Working group shall come from the Executive, Judicial, Legislative branches of State government, constitutional offices, K-12 public schools and higher education, and other qualified individuals.

The Group shall meet quarterly at a minimum.

Administrative -I/T Asset Protection-Background Checks

10.1.1. Overview
As a condition of employment, all current and prospective Bureau of Information and Telecommunications (BIT) employees and Information Technology contractors desiring to work for the State shall be screened thoroughly including verification of qualifications.

Prospective employees and contractors will be notified that a background check will be done as part of the recruiting and selection process.

These verifications must be performed at least once every ten years.

10.1.2. Purpose
Ensure that current and prospective BIT employees and Information Technology contractors do not have a criminal history that would raise suspicion as to the integrity of their employment.
10.1.3. Scope

Background checks shall be limited to criminal history available through State and Federal resources.

10.1.3.1. Scope Assumptions

The scope includes BIT employees and prospective BIT employees of the Administration, Data Center, Development, and Telecommunications Divisions, South Dakota Public Broadcasting studio engineers, field engineers, and network operations center staff as well as current and prospective Information Technology contractors desiring to work for the State.

10.1.3.2. Scope Constraints

Background checks are not performed for financial or credit information.

10.1.4. Policy

10.1.4.1. Background Checks

BIT requires all current and prospective BIT employees, State Technology contractors, and the South Dakota Public Broadcasting Engineering group who write or modify State of South Dakota-owned software, alter hardware, configure software of State-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo Federal fingerprint-based background checks and to have these background checks repeated at least once every ten years. Failure to comply with a federal background investigation may result in disciplinary action up to and including termination of employment or the rescinding of a conditional offer of employment.

These background checks must be fingerprint-based and performed by the State with support from the State's law enforcement resources. Under provisions set forth in Title 28, Code of Federal Regulations (CFR), Section 50.12, the prospective employees and contractors will be provided written notification that their fingerprints will be used to check the criminal history records of the State and the Federal Bureau of Investigation (FBI). Identification records obtained from the FBI may be used solely for the purpose requested and may not be disseminated outside the receiving department, related agency, or other authorized entity. BIT will supply the fingerprint cards and the procedure that is to be used to process the fingerprint cards.

Individuals should plan on the background check taking two to four weeks.

The steps to process the background checks are found in procedures document ITSP 1010.1 Background Checks Procedures.

10.1.4.2. Disqualifying Criteria

SDCL 1-33-63 allows the Commissioner of BIT to require a Federal background investigation be performed on any current or prospective BIT employee or Information Technology contractor that has access to confidential data or information. To implement these provisions, BIT must determine and memorialize its Disqualifying Criteria policy - the specific criminal activity that operates to disqualify a person from having access to the confidential data.

For purposes of this Policy, the terms "employee or contractor" means "potential or current BIT employee or Information Technology contractor."

A. An employee or contractor may not have access to confidential data if the individual has been convicted of a felony within 5 years of the date of the most recent criminal background check or any time thereafter.
1. Employees or contractors involved with technology associated with the division of the South Dakota Lottery must meet the qualifications defined in SDCL 42-7A-14. Primarily, this extends the period beyond completing felony sentencing to 10 years, rather than 5 as defined in A. above.

B. If the employee or contractor has been convicted of a crime not included in Paragraph A, the employee or contractor is not automatically disqualified from having access to confidential data. The determination of whether such an employee or contractor may have access to confidential data will be made on an individual basis. The considerations will include but not be limited to:
   1. The nature of the conviction, particularly if it is a crime of dishonesty, a financial crime, an identity crime, or a crime involving the misuse of confidential information.
   2. The length of time between the offense and the employment decision.
   3. The number of offenses.
   4. The relatedness of the conviction to the duties and responsibilities of the position.
   5. The efforts at maintaining a clean record.
   6. The number of crimes committed.

C. The determination required by Paragraph B will be made by the BIT Chief Information Security Officer (CISO) in consultation with the applicable Division Director.

D. Under no circumstances may an employee or contractor have access to confidential data if the individual is disqualified by this policy.

E. If a position within the BIT requires an employee or contractor to have access to confidential data as an essential part of the job function, the individual's failure to undergo or to successfully pass a criminal background check may result in termination of the employee or contractor.

F. After the adoption of this policy, no employee or contractor may be hired by BIT unless the individual undergoes and successfully passes a criminal background check pursuant to this policy.

10.1.4.3. Noncriminal Agency Coordinator (NAC)
The CISO is designated as a Noncriminal Agency Coordinator (NAC) to act as the primary contact person for BIT.

10.1.4.4. Local Agency Security Officer (LASO)
The CISO is appointed as a Local Agency Security Officer (LASO) to act as liaison with the South Dakota Division of Criminal Investigation (SDDCI) to ensure the BIT follows security procedures.

10.1.4.5. Background Check Interpretation
When an explanation of a charge or disposition is needed, the BIT NAC will communicate directly with the agency (SDDCI) that furnished the data to the FBI.

10.1.4.6. Not Guilty Presumption
An individual should be presumed not guilty of any charge/arrest for which there is no final disposition stated on the record or otherwise determined.

10.1.4.7. Background Check Information Challenge
An opportunity to challenge and discuss the disqualification due to information found in the criminal history records of the FBI will be provided to the applicant for five days, if requested. Due to the confidential nature of the criminal history records of the FBI and the restrictions on disclosure of the records, it may be discussed that the applicant was disqualified because of criminal history information; however, the specific FBI results may not be disclosed to the applicant, neither in writing nor verbally.

Under provisions set forth in Title 28, CFR, Section 50.12, if the information on the record is used to disqualify an applicant, the official making the determination of suitability for licensing or employment shall provide the applicant the opportunity to complete, or challenge the accuracy of, the information contained in the FBI Identification record. The deciding official should not deny the license or employment based on the information in
the record until the applicant has been afforded a reasonable time to correct or complete the information or has declined to do so.

10.1.4.8. Corrective Action
If the applicant wishes to correct the record as it appears in the FBI's Criminal Justice Information Services (CJIS) Division Records System, the applicant should be advised that the procedures to change, correct, or update the record are set forth in Title 28, CFR, Section 16.34.

10.1.4.9. Training
BIT will comply with mandatory training requirements as outlined in the South Dakota Division of Criminal Investigation Guide for Noncriminal Justice Agencies. All personnel directly associated with accessing, maintaining, processing, dissemination, or destruction of Criminal History Record Information (CHRI) shall be trained.

10.1.4.10. Emailing Background Check Information
It is prohibited to mail criminal history background check information either as an email or as an attachment to email. Individuals are prohibited from opening any email that contains background check information. They must report the occurrence to their supervisor and delete the email.

**Administrative - I/T Asset Protection-Confidentiality**

10.3.1. Overview
All BIT employees and contracted technology professionals shall be granted appropriate access to information, agency documents, records, programs, files, diagrams, and pertinent data resources needed to fulfill the job responsibilities of an individual or a contractual agreement. In return, it is expected that such data is treated as a trade secret and individuals will not modify data or disclose data to others without proper authorization. Products resulting from employment or custom-built solutions for government agencies are the property of the State.

10.3.2. Purpose
To ensure that employees are familiar with the laws that govern use of information technology systems and the data contained within those systems and that employees and contractor comply with such laws.

10.3.3. Scope
This policy applies to BIT and technology contractors of the State. It includes the protection of sensitive data in addition to the work products built under State guidance.

Individuals shall maintain confidentiality and data integrity of documents, records, configurations, programs, and files and understand that work products resulting from such efforts are the property of the State.

10.3.3.1. Scope Assumptions
The confidentiality and data integrity responsibility of BIT employees and contractors extends to, but is not limited to systems, software, data, configurations, architectures / designs, documentation, and infrastructure information developed on its own or acquired from third parties. Customized work products including specific-built software solutions are the property of the State.

10.3.3.2. Scope Constraints
Agencies will have their own data protection and confidentiality agreements. Leased and licensed software is exempt from this policy.

10.3.4. Policy

10.3.4.1. Confidentiality Agreement
The individual must not, at any time, use or disclose any trade secrets or confidential information of the State to anyone, include agencies or contractors that have business with the State, without written permission from the BIT Commissioner, except as required to perform duties for the State.

The individual agrees to adhere to all data processing and technology policies governing the use of the technology infrastructure of the State.

The individual agrees that all developments made and works created by the individual in connection with the contractual agreement of the State shall be the sole and complete property of the State, and all copyrights and other proprietary interest, therein, shall belong to the State.

Upon the request of the State to include the termination of the employment of the person, the individual will leave all reports, messages, programs, diagrams, documentation, code, memoranda, notes, records, drawings, manuals, flow charts, and any other documents whether manual or electronic pertaining to the State, including all copies thereof, with BIT to include all data resources whether manual or electronic involving any trade secrets or confidential information of the State to include agencies or contractors that have business with the State.

Complying with Legal Obligations

Employees and contractors are subject to Federal, State and local laws governing the use of information technology systems and the data contained in those systems.

- BIT shall comply with all applicable laws and take measures to protect the information technology systems and the data contained within information systems. Agencies must take the initiative to comply with applicable laws and regulations pertaining to their field of business.
- BIT shall ensure that all BIT employees and technology contractors are aware of legal and regulatory requirements that address the use of information technology systems and the data that reside on those systems.
- Agencies shall ensure that each public employee and other agency authorized users are provided with a summary of the legal obligations that apply to that agency such as HIPAA, etc.

10.3.4.2. Security Acknowledgement and Access
Once chosen, contractors must identify all individual contractors that will be participating in work for the State and begin participating after the work has begun.

Contractors working with the State shall be required to sign the Security Acknowledgement form (http://intranet.bit.sd.gov/forms/).

All BIT employees and contractors need to have a copy signed and filed. Contractor access to the technology infrastructure of the State is closely managed and limited.

Contractors do not have the same degree of access nor privileges given to State employees.

At the sole discretion of BIT, access for a contractor to the technology infrastructure of the State can be amended or terminated.

Mainframe-Mainframe Security-Mainframe Accounts
210.3.1. Overview

This policy covers the mandatory use of individual User IDs to control access to specific mainframe resources.

210.3.2. Purpose

To protect mainframe resources from unauthorized or inappropriate access unique User IDs are used. Rights are granted case-by-case allowing for auditing of both successful and unsuccessful access attempts that can be tracked for security audits.

210.3.3. Scope

Mainframe security requirements apply all those who have access to or use mainframe resources administered by BIT.

210.3.3.1. Scope Assumptions

This policy applies to those who use or wish to use and/or have access to mainframe resources.

210.3.3.2. Scope Constraints

This policy applies to only to those who wish or do use or access any mainframe resources. It does not necessarily apply to resources on Windows, Unix, or AS/400 platforms.

210.3.4. Policy

210.3.4.1. Unique Account Requirement

All mainframe resources are protected by one or more mainframe security systems. Each individual that requires access to mainframe resources must have a unique User ID which allows for viewing, updating, creating or deleting of protected resources controlled by least one of the security systems.

210.3.4.2. Requests for Mainframe User IDs

Access to mainframe systems and data is granted only when a specific business need is proven, as defined by BIT client departments and BIT Mainframe Security Administration. All access for department personnel must be requested in writing to the BIT Help Desk using the Employee Request Form (New/Move) at the BIT Intranet http://intranet.bit.sd.gov/forms. All requests must be made by department personnel authorized to make such requests and access will be assigned based on the principle of least privilege, which requires that a user be given no more privilege than necessary to perform a job.

210.3.4.3. Responsibility for Mainframe UserIDs and Passwords

All client user access to mainframe resources is identified by assigned mainframe User IDs and authenticated by passwords. Individuals that have been assigned an individual mainframe User ID are considered the owner of the ID and are responsible for securing and protecting its password. Individuals must not write the password on paper, post the password on terminals, save the password in computer files or allow the password to be known by other individuals. Individuals on record as being the owner of an ID are responsible for all valid or invalid access made by that ID. Unauthorized access to State or Federally protected data may be prosecuted by State and Federal authorities.

Mainframe-Mainframe Security-Mainframe Accounts
210.4.1. Overview

This policy covers the mandatory use of individual User IDs to control access to specific mainframe resources.

210.4.2. Purpose

To protect mainframe resources from unauthorized or inappropriate access unique User IDs are used. Rights are granted case-by-case allowing for auditing of both successful and unsuccessful access attempts that can be tracked for security audits.

210.4.3. Scope

Mainframe security requirements apply to all those who have access to mainframe resources administered by BIT.

210.4.3.1. Scope Assumptions

This policy applies to those who use or wish to use and/or have access to mainframe resources.

210.4.3.2. Scope Constraints

This policy applies to only to those who wish to or do use or access any mainframe resources. It does not apply to resources on Windows, UNIX or mobile devices.

210.4.4. Policy

210.4.4.1. Mainframe User ID Revocation

Mainframe user IDs will be disabled if they are not used within forty-five days and will need to be reset by the BIT Help Desk.

Mainframe-Mainframe Security-Mainframe Access

210.25.1. Overview

This policy covers requirements that must be met before physical access will be granted to the BIT Computer Room.

210.25.2. Purpose

The purpose of this policy is to protect physical mainframe resources from unauthorized access through the use of physical access requirements.

210.25.3. Scope

These security requirements apply those who have a need to gain physical access to the location that houses mainframe hardware administered by the BIT.

210.25.3.1. Scope Assumptions
The policy applies to those who wish to gain physical access to the BIT Computer Room.

210.25.3.2. Scope Constraints

This policy applies to only those who wish to access the BIT Computer Room. It does not necessarily apply to other facilities or rooms administered by BIT personnel.

210.25.4. Policy

210.25.4.1. Mainframe Access

For security reasons, BIT maintains what is referred to as a "closed" computer room. No individuals, other than BIT Operations personnel, are permitted in the mainframe computer room unless the person can show a need to be in the room, provide a form of photo identification, and sign in and sign out. Individuals who meet these requirements must also be escorted by Data Center staff at all times.

Server-Server Security-Server Maintenance and Administration

220.1.1. Overview

Servers require maintenance. Failure to maintain a server exposes the State to unacceptable security risks. Allowing server patching status to be visible outside a network can also expose the network to unacceptable risk. Out-of-date systems that are accessible from the Internet may have vulnerabilities related to the application servers or the application framework. There can be design flaws or implementation bugs. Hackers look for evidence of weak links in cyber defenses. A successful exploitation may result in data loss, bad reputation, loss of credibility, or financial problems.

220.1.2. Purpose

This empowers BIT to manage State enterprise servers and provide for secure server maintenance on any network State data and applications reside.

220.1.3. Scope

This policy covers BIT managed enterprise servers, Contractor managed servers connecting to the State network, and Contractor managed networks that host State data and/or applications.

220.1.3.1. Scope Assumptions

A server is connected to the State network or hosts state data and/or applications.

220.1.3.2. Scope Constraints

This only applies to the State's enterprise distributed system that hosts state data and/or applications. This policy does not include the State mainframe, AS/400, desktop, and mobile devices.

220.1.4. Policy

220.1.4.1. Visibility of Server and Framework Patching Status

The server patch status will not be visible outside a network hosting State data and/or application. This policy applies to both the State network and Contractor networks that host State data or applications.
Server-Server Security-File Transfer Protocol

220.7.1. Overview

The State supported FTP server is meant for short term storage only and is not meant as a permanent data store. The FTP service should be used for applications uploading or downloading files that have a limited lifespan, transfer of files of large size, and temporary placement for files to be downloaded outside the technology infrastructure of the State. The FTP server is not backed up and all files placed on the server have a lifespan of seven days. If the files are not removed after seven days, the data will be automatically deleted. The FTP server is secured to the Internet; in order for outside entities to get into the FTP server, an FTP username and password is required. In addition, the FTP server is secured from internal clients of the State though the configuration of the permissions for the device. By default, all State users have Read, Write and Delete access while internet users have no access.

- All access will require a user id and password. Anonymous FTP is not acceptable.
- Retention period on all files will be limited to seven calendar days. Individual files will be deleted after seven days of storage.

220.7.2. Purpose

To limit the volume of data storage on the FTP server and assure the FTP server serves the purpose for which it is intended, namely a reliable way to temporarily store data that is being transferred into our out of the state.

220.7.3. Scope

The scope is the use of the State's FTP server within the State domain.

220.7.3.1. Scope Assumptions

This policy only covers only the State's FTP server within the State domain.

220.7.3.2. Scope Constraints

This policy only applies to the State's FTP server and its use as a temporary storage location. It does not apply to any other data storage locations or data-transfer processes.

220.7.4. Policy

220.7.4.1. Use of File Transfer Protocol Server

Internet users shall use the available FTP software to get to the FTP server. The FTP server is meant for short term storage only and is not meant as a permanent data store. Copying or retrieving files from the FTP server by Internet clients is not allowed unless an account is created for the individual or company. Contact the BIT Help Desk to request access to the available FTP software and/or the steps, costs, and authorizations required to create an FTP account for a non-State user.

Server-Server Security-Assurance HIPAA Regulations are Met

220.10.1. Overview
BIT will establish and maintain the security and privacy of electronic Health Insurance Portability and Accountability Act (HIPAA) information created, used, transmitted, stored, and destroyed by State employees and/or the State in accordance with Federal laws and regulations.

220.10.2. Purpose


220.10.3. Scope

This policy applies to those who access or create HIPAA data on systems managed by BIT.

220.10.3.1. Scope Assumptions

You use HIPAA data in electronic form, electronic Personal Information (ePHI).

220.10.3.2. Scope Constraints

This policy only applies to users of HIPAA data in electronic form (ePHI).

220.10.4. Policy

220.10.4.1. The Data User is Responsible for Adhering to HIPAA Regulations

Each user with access to HIPAA data is responsible for understanding federal requirements for data handling and security and accountable for any actions they take that may compromise the security or confidentiality of HIPAA data. BIT will work with HIPAA authorized agency staff and authorized federal audit staff as well as written federal rules and regulations to assure security and access controls are in place to meet 45 CFR Part 160 and Part 164 and other applicable rules and regulations relating to electronic HIPAA information created, used, transmitted, stored, and destroyed on technology managed by BIT. Where deficiencies are determined to exist, BIT will work with the appropriate resources within the State and the applicable federal audit group to address those.

Data Center General-Data Center Security-Cloud Based Services and System Information

230.9.1. Overview

Cloud-based technology providers rely on a wide range of technologies and business models to offer and maintain their services. The security, reliability, portability, resilience, and long-term viability of any given service offering is largely dependent on the technologies and business models in use and the manner in which those technologies and business models are implemented, maintained, and managed.

However, it is impossible to know what the nature of the underlying technologies or business practices may be without a collaborative, detailed, and thoughtful review with the cloud-based technology provider.

BIT must approve and be a signatory to all cloud-based and remote technology service and system agreements.

230.9.2. Purpose
Define BIT’s authority to review, approve, and be a signatory to cloud based systems and technology services agreements used or contracted for by client agencies.

230.9.3. **Scope**

The scope of this policy includes all executive branch technology acquisitions that use any cloud-based system or service that originates from outside the direct physical or logical control and management of BIT.

230.9.3.1. **Scope Assumptions**

This policy applies to any cloud-based system or services used or acquired by an agency that originates from outside the direct physical or logical control and management of BIT.

230.9.3.2. **Scope Constraints**

This policy does not apply to third party systems or services that are hosted at the state on BIT managed infrastructure and/or managed by BIT. This policy does not apply to systems or services for the State’s K-12 or clients.

230.9.4. **Policy**

230.9.4.1. **Responsibility for Cloud Based Services and Systems.**

As the approving entity for all statewide IT services and systems, including cloud-based services and systems, BIT must review, approve, and be a signatory to all agreements for acquiring or using cloud-based types of systems or services. Cloud-based technology providers include, but are not limited to, any entity that uses technologies and business processes to store, access, or manipulate state or citizen data from outside the direct physical or logical control and management of BIT managed systems.

It is critical to plan ahead for the purchasing of these services from an IT or cloud provider. Agencies must factor in the time required for BIT staff to perform a detailed review and assessment to determine whether approval can be granted.

Data Center General-Secure Information Technology Acquisition Policy-
Secure Information Technology Acquisition Policy

230.10.1. **Overview**

Secure information technology acquisition is the methodology the State uses to acquire information technology goods and services. The goal is to acquire I/T goods and services that meet security and technology standards as inexpensively as possible. To that end there must be processes that filter out insecure technology that does not meet State standards, identify solutions that are technological unsound and discover all cost associated with the acquisition. These processes must work in conjunction to accomplish those ends. This must be accomplished while recognizing the sometimes-unique needs of BIT’s clients and encouraging their full participation in the process.

230.10.2. **Purpose**

The purpose is to acquire I/T goods and services as securely as possible.

230.10.3. **Scope**
These policies cover the acquisition of I/T goods and services by the executive branch and any other branch or entity acquiring technology that will be used on or with the State’s I/T infrastructure.

230.10.3.1. Scope Assumptions

These polices assume that you are acquiring I/T related goods and/or services.

230.10.3.2. Scope Constraints

These policies only apply to the acquisition of I/T goods and services.

230.10.4. Policy

230.10.4.1. Hardware Maintenance Agreements

Any hardware acquired must include a commitment by the supplier to keep the hardware’s associated software and firmware patched and up-to-date as well as providing a hardware maintenance agreement. BIT will scan all hardware and the software and firmware associated with the hardware for security vulnerabilities on a regular basis and will apply vendor-supplied mitigation for any vulnerabilities found. When a hardware reaches the vendor's end-of-life date, BIT will continue scanning the hardware and will mitigate any new vulnerabilities found, up to and including replacing the hardware if the vulnerability is severe enough and if there is no other mitigation available.

Data Center General-Data Center Security-Federal Tax Information

230.11.1. Overview

This policy covers safeguarding Federal Tax Information (FTI). Special handling instructions must be in place when working with FTI including the prohibition of remote access to FTI without using multi-factor authentication. This policy documents what is FTI, what is not, and what safeguards must be implemented specific to files that contain FTI.

230.11.2. Purpose

To define FTI as well as the safeguards that must be in place when receiving, handling, or sharing FTI.

230.11.3. Scope

This policy applies to all FTI obtained directly from the Internal Revenue Service (IRS) or from an official IRS form.

230.11.3.1. Scope Assumptions

It is assumed that individuals receiving and/or accessing FTI have a legitimate business need to do so, and have obtained the necessary permissions from the IRS to transfer information of this nature to State-owned servers and/or to access information of this nature.

230.11.3.2. Scope Constraints

This policy applies only to Federal Tax Information. This policy does not apply to information that is not FTI.
230.11.4. Policy

230.11.4.1. Federal Tax Information Returns and Return Information
A return is any tax or information return, estimated tax declaration or refund claim to include amendments, supplements, supporting schedules, attachments or lists required by, and filed with the IRS by, on behalf of, or with respect to any person or entity. Examples of returns include forms filed on paper or electronically, such as Forms 1040, 941, 1120, and other informational forms, such as 1099 or W-2. Forms include supporting schedules, attachments or lists that are supplemental to or part of such a return.

Information collected or generated by the IRS regarding a person's Internal Revenue Code liability or potential liability includes but is not limited to:

- Information, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense.
- Information extracted from a return, including names of dependents or the location of business, the taxpayer's name, address, and identification number.
- Information collected by the IRS about any person's tax affairs, even if identifiers such as name, address, and identification number are deleted.
- FTI may include PII. FTI may include the following PII elements, the:
  - Name of a person with respect to whom a return is filed.
  - Mailing address.
  - Taxpayer identification number.
  - Email addresses.
  - Telephone numbers.
  - Social Security Numbers.
  - Bank account numbers.
  - Date and place of birth.
  - Mother's maiden name;
  - Biometric data (e.g., height, weight, eye color, fingerprints).
  - Any combination of the preceding.

If the preceding information needs clarification or should ever come in question, BIT will review and define FTI as Federal Tax Information as defined within the tax codes of the United States of America by accessing www.irs.gov to search for Tax Code, Regulations and Official Guidance. For the purpose of BIT security planning anything stored on mainframe media is treated as if the media contains FTI.

230.11.4.2. What is Not Federal Tax Information
FTI does not include information provided directly by the taxpayer or third parties. If the taxpayer or third party subsequently provides returns, return information or other PII independently, the information is not FTI as long as the IRS source information is replaced with the newly provided information.

230.11.4.3. Safeguarding Federal Tax Information
Safeguarding FTI is critically important so confidential taxpayer information is continuously protected as required by federal law. Access to FTI is permitted only to individuals who require the FTI to perform their official duties and as authorized under the IRC. FTI must never be indiscriminately disseminated, even within State government.

230.11.4.4. Emailing Federal Tax Information
It is prohibited to email FTI either as an email or as an attachment to an email. Do not open any email that contains FTI but report the occurrence to your supervisor and delete the email.
230.58.1. Overview

This policy addresses the issuance, use, and monitoring of proximity cards which provide access to BIT facilities.

230.58.2. Purpose

Physical access to equipment facilities controlled by BIT must be restricted to authorized personnel only.

230.58.3. Scope

Authorized personnel may be BIT employees, BIT contractor personnel, or other State personnel that have equipment located in BIT facilities.

230.58.3.1. Scope Assumptions

Staff and visitors have a legitimate business need for entering BIT facilities.

230.58.3.2. Scope Constraints

This policy does not apply to locations equipped with proximity card readers that are not maintained by BIT.

230.58.4. Policy

230.58.4.1. Proximity Card for Non-BIT Employee Access

Temporary Guest Access

On occasion, situations may exist where a contractor needs to have temporary access to a secured environment. Authorized visitors must provide their escort with a photo ID and the guest and escort must jointly sign in using the sign in sheets located inside the door of each equipment facility. The individuals are guests of the State and must be monitored at all times by an authorized employee of BIT. The individuals cannot be left alone in a secured location without supervision. Only BIT employees with access privileges to the secured facility being accessed are authorized to be an escort for visitors.

Permanent Access Procedures for Non-BIT Employees

Contractors and other agency personnel that have been issued a proximity card are considered trusted partners. However, trusted partners do not have the authority to sign in visitors that have not been issued a proximity card.

Access to the state campus tunnel system

All agencies follow the process and policies regarding tunnel system access on the state campus as set and managed by the Department of Public Safety (DPS). BIT shall support the policy and follow its requirements and processes as defined and as directed by DPS.

Data Center General-Data Center Security-Accounts Access Control and Authorization

230.67.1. Overview

All devices that can connect to the State domain and/or managed by BIT as well as their peripheral devices will have security policies established and implemented to restrict unauthorized activities. Authorization for individuals to access programs, databases, and related technologies will be enforced. Access must be based on least privilege. Individual accounts are created for those with a need to access State IT resources. Access must end
when the manager of an employee or contractor determines access is no longer required or when job responsibilities change, and privileged access must be adjusted. Only authorized personnel will be allowed to change passwords and they must have proper credentials to prove who they are.

There are policies for thresholds for lockouts, duration of lockouts, and resets specific to the Department of Human Services (DHS), Department of Revenue (DOR), Department of Social Services (DSS), and the Department of Labor and Regulation (DLR).

230.67.2. Purpose

This policy provides the forms and processes to authorize, create, maintain and terminate accounts.

230.67.3. Scope

This policy covers all State IT resources managed by BIT.

230.67.3.1. Scope Assumptions

Employee and contractor access are authorized by an immediate supervisor or higher-level manager. Security administrators will conduct periodic reviews to verify that only access needed by an individual's job duties have been assigned. When a supervisor or manager determines access needs to be changed, they must notify BIT using the Employee Request Form (New/Move/Change Responsibilities).

230.67.3.2. Scope Constraints

This policy does not apply to the mainframe, the AS/400s, or IT resources which are not managed by BIT. The lockout threshold, lockout duration, and reset requirements apply only to DHS, DOR, DSS, or DLR workstations.

230.67.4. Policy

230.67.4.1. Individual Access Authorization

The Employee Request Form (New/Move/Change Responsibilities) is used to request access to State IT resources and it must be filled out by an authorized manager. This form must be used when a contractor starts, a new employee is hired, an employee transfers positions, or when an employee's or a contractor's duties change. If the change in duties is enough to regard the change as a new position or requires a new or amended contract the Security Acknowledgement form must also be signed.

230.67.4.2. Least Privilege

Access privileges must be layered to reflect job functions and separation of duties, and minimal security privileges or only the security privileges required for an individual to perform work duties must be assigned.

230.67.4.3. Password Requirements

Must:

- Be changed every ninety days.
- Be at least eight characters.
- Contain at least three of the following four-character groups:
  - English uppercase characters (A through Z).
  - English lowercase characters (a through z).
  - Numerals (0 through 9).
Non-alphabetic characters (such as !, $, #, %).

- Must not be one of the twenty-four most recent passwords;
- Must not have been changed within the last seven days.
- Does not contain first name, last name, username.
- Does not contain Social Security Number.
- Does not contain permutations of "password".
- Cannot be a dictionary word.

User accounts with no administrative rights will need to change their passwords every 90-days. User accounts with administrative rights will need to change their passwords every 60-days. Where existing State technology products can support multiple expiration password policies for individual administrators' accounts that have administrative access rights without altering the general 90-day expiration password policy for individual users' accounts that do not have administrative access rights, the expiration password policy shall be set to 60-days for such administrators' accounts that have administrative access rights. Contractor passwords that provide access to the State's system or devices must expire after 60-days. Contractor(s) must not share passwords with other contractor(s).

230.67.4.4. Individual Access Termination

Access privileges must be terminated immediately when authorization ends for a user identified by the individual's manager. When an employee or contractor employment is terminated, the manager is responsible for completing the Exiting Employee Request form. If the termination is immediate, the BIT Help Desk (605-773-4357) must be notified without delay so that access and authorization assigned to the individual can be disabled. In all departing employee situations, managers must take reasonable steps to ensure no assets of the State including data, software, or hardware are taken, shared, inappropriately modified, or destroyed by the individual.

Data Center General-Payment Card Industry Data Security-Payment Card Industry Data Security Standard

230.72.1. Overview

Payment Card Industry Data Security Standard (PCI) requirements are set by the Payment Card Industry Security Standards Council to protect cardholder data. The standards govern all merchants and organizations that store, process, or transmit this data, and include requirements for software developers and manufacturers of applications and devices used in the transaction process. Compliance with the PCI security standards is enforced by the major payment card brands who formed the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The requirements apply to all payment methods, including retail (in person), mail/telephone order, and e-commerce. Failure to adhere to PCI standards can result in the State not being able to use payment cards and can result in fines.

230.72.2. Purpose

The purpose is to ensure the State complies with PCI security standards.

230.72.3. Scope

These policies cover the servicing of payment cards for goods and/or services provided by the State.
230.72.3.1. **Scope Assumptions**

Payment cards are used to reimbursement the State for goods and/or services provided by the State.

230.72.3.2. **Scope Constraints**

This policy covers payments made to the State not use of the State of payment cards to acquire goods and services.

230.72.4. **Policy**

230.72.4.1. **Payment Card Industry Data Security Standard Requirements**

The State is required by the payment card association to follow the PCI security standards. These standards assure a secure environment for our customers, protecting them against both loss and fraud. The State must comply with PCI requirements for securely processing, storing, transmitting, and disposing of cardholder data. Annually all payment card service providers (such as banks) that perform card processing for the State must be certified as PCI compliant. The service providers must submit a letter to BIT confirming compliance with PCI standards.

230.73.1. **Overview**

Secure information technology acquisition is the methodology the State uses to acquire information technology goods and services. The goal is to acquire I/T goods and services that meet security and technology standards as inexpensively as possible. To that end there must be processes that filter out insecure technology that does not meet State standards, identify solutions that are technologically unsound and discover all cost associated with the acquisition. These processes must work in conjunction to accomplish those ends. This must be accomplished by recognizing the unique needs of BIT’s clients and encouraging their full participation in the process. BIT acquisition resources can be found on the BIT Technology Review webpage.

230.73.2. **Purpose**

The purpose is to acquire I/T goods and services as securely as possible.

230.73.3. **Scope**

These policies cover the acquisition of I/T goods and services by the executive branch and any other branch or entity acquiring technology that will be used on or with the State’s I/T infrastructure.

230.73.3.1. **Scope Assumptions**

These polices assume that you are acquiring I/T related goods and/or services.

230.73.3.2. **Scope Constraints**

These policies only apply to the acquisition of I/T goods and services.
230.73.4. Policy

230.73.4.1. Acquisition of Services Involving HIPAA Data
Any contractor providing services that potentially can expose HIPAA data to the contractor, must sign the BIT business associate agreement before the work can start. If having the contractor sign a BIT business associate agreement is not possible or if it is thought that a business associate agreement is not needed, permission to proceed with the work must be obtained from the BIT Chief Information Security Officer before any work can proceed. There also must be a risk assessment performed by the BIT Chief Information Security Officer or a designee. There are no exceptions to these policies.

230.73.4.2. Security Scanning Requirements
Applications installed on the State's system or service(s) hosted by a contractor such as SaaS, PaaS or IaaS, must be scanned for security vulnerabilities. For any application, installed on either the State's infrastructure or the Contractor's, where a contract has not been signed, an authorization to scan must be signed before scanning can be done. Any exceptions to this policy must be approved by the BIT Chief Information Security Officer and may require a signed release by the agency recognizing the risks involved.

230.73.4.3. Hardware Maintenance Agreements
Any hardware acquired must include a commitment by the supplier to keep the hardware's associated software and firmware patched and up-to-date as well as providing a hardware maintenance agreement. BIT will scan all hardware and the software and firmware associated with the hardware for security vulnerabilities on a regular basis and will apply vendor-supplied mitigation for any vulnerabilities found. When a hardware reaches the vendor's end-of-life date, BIT will continue scanning the hardware and will mitigate any new vulnerabilities found, up to and including replacing the hardware if the vulnerability is severe enough and if there is no other mitigation available.

Data Center General-Use of Production Data

230.74.1. Overview
Precautions must be taken when copying data from a production environment to a non-production environment. A non-production environment can be, but is not limited to, staging, development, or test environments. State employees must store State data in non-production environments securely and must have approval before they move any protected production data to a non-production environment.

230.74.2. Purpose
This policy states how protected production data should be handled outside of production environments. The testing of applications can be enhanced with the use of live data. Precautions must be taken to ensure that the protected data is safeguarded.

230.74.3. Scope
This policy includes all non-production environments that store, or process protected production data on State systems and the movement of State data to and from a contractor infrastructure. Movement of data on infrastructure completely outside the State's control by a Contractor is not covered by this policy. Movement of data on infrastructure outside the State’s control by a Contractor will be governed by any agreements made between the State and the Contractor.

Approval is obtained by using the BIT Moving Live Data Request Form. Any data protected under Federal or State regulation or statute or industry standard is considered protected data. Protected data includes but is not
limited to Personally Identifiable Information (PII), Protected Heath Information (PHI), Federal Tax Information (FTI), Family Educational Rights and Privacy Act (FERPA), Criminal Justice Information System data (CJIS), The Federal Parent Locator Service (FPLS), and Payment Card Industry data (PCI). Protected production data that is masked, deidentified or aggregated is no longer considered to be protected data. Information on what is legally protected data that is Personally Identifiable Information (PII) is found [here](#).

### 230.74.3.1. Scope Assumptions

This policy assumes State employees and contractors are authorized to work with the data and need to move protected production data into:

- A non-production State environment.
- A Contractor environment.
- From a Contractor environment to a State environment.

### 230.74.3.2. Scope Constraints

This policy only covers State production data that will be moved into a non-production environment.

### 230.74.4. Policy

#### 230.74.4.1. Use of Production Data in a Non-Production Environment

Approval must be obtained before moving protected production data to a non-production environment. The non-production environment must have the same level of security as the production environment. The BIT [Moving Live Data Request Form](#) must be used for approval. Contractors can obtain the form from their agency contact.

Approval for moving protected production data is valid for six months. If the data is needed in the non-production environment longer than the approval period, another BIT Moving Live Data Request Form must be filled out and approved before the last approval expires. An expedited approval can also be requested through the Moving Live Data Request Form for data that will only be in the non-production environment for two-business days or less. All data must be purged before either approval expires.

Prior to moving production data from the State's environment to the Contractor's system there must be a security scan. This scan must be done by the State or a BIT approved third-party. This scan can be done up to three-months before the data is moved. If there is a third-party scan the scan results must be provided to the State contact. An acceptable security scan report of the data must consist of at least:

- The system that was evaluated (URL if possible, mask if needed);
- The categories that were evaluated (for example SQL injection, cross site scripting, etc.);
- What were the general findings (for example how many SQL injection issues were found and the count per category);
- Technical details of each issue found including, where it was found, web address, what was found, and the http response if possible.

The infrastructure scan report must include at least:

- What software, platform and framework were used to perform the scan;
- What general categories were evaluated, host discovery, vulnerability scan, external vulnerability scan or compliance checks;
- Explain the exact details of the test run with those categories;
- General findings or summary report;
- Technical findings, including the exact details of what was found and their severity.
The use of Federal Tax Information (FTI) in non-production environments requires authorization from the IRS Office of Safeguards by filling out the IRS Live Data Testing Notification Form. A copy, or link, to the approved IRS form must be attached to the BIT Moving Live Data Request Form. The use of FTI production data in a non-production environment is limited to tax administration or other authorized IRS purposes including:

- Testing new systems.
- Validation of Federal data load.
- Data matching between state and federal forms.
- Testing audit selection.

FTI data may only be disclosed to those requiring the data to perform their official duties. The requester may also be required to sign a form, provided by the data owner, prior to obtaining access to the production FTI. IRS approved sanitization methods must be used after the data is no longer needed.

The FPLS can be a secondary source of FTI. FTI from the FPLS is treated as if the FTI was from the IRS. Other forms of data that have unique requirements are:

- CJIS data can only be moved by the Office of Attorney General (ATG), it cannot be moved by BIT. The ATG must notify the CISO when CJIS data is moved, provide the location of that data, and inform the CISO if dual authorization is required before disposal of the data. After the CJIS data is no longer needed it must be disposed of as stated in ITSP 230.68. The documentation and verification of the disposal of the data will be completed by the ATG.
- PCI data may not be used in non-production environments.

Contractors with access to protected data must sign the Security Acknowledgement Form and have passed a background check before they can have access to the data.

Protected State data cannot be moved outside the United States of America or its territories.

The Data Center may be requested to verify compliance using, but not limited to, business tool reports, internal, and external audits. The request to verify can be made by the data owner or CISO.

**230.74.4.2. Purging of Data**

If there is unapproved protected production data in a non-production environment, the data must be purged. Any protected production data on a BIT-developed system that was moved to a non-production environment prior to this policy going into effect must be approved or purged. Any protected production data on BIT-hosted Contractor-developed system that was moved to a non-production environment prior to this policy going into effect must be approved by November 7, 2018 or purged.

Protected production data must be purged from the non-production environment before the BIT Moving Live Data Request Form approval has expired or it must be re-approved. It is the responsibility of the requestor of the data move to verify that the data has been purged.

**230.74.4.3. Compliance**

If an individual finds unapproved, unmasked protected production data in a non-production environment, they must:

1. Notify her or his manager.
2. The manager must notify the Development Director and CISO.
3. The data must be purged.
4. The Development Director and CISO will be notified when it is purged.
If unapproved, unmasked, protected production data is found in a non-production environment, the CISO will decide if it is a security incident. The individual(s) responsible for unapproved unmasked protected production data in a non-production environment may be subject to disciplinary action up to and including dismissal. The placing of unapproved unmasked FTI, HIPAA, or FPLS data on a non-production environment may subject the responsible individual to legal action as stated in IRS 1075 or The American Recovery and Reinvestment Act of 2009.

Data Center General -Security Impacts-Data Classification

230.75.1. Overview

Data classification establishes the agency and BIT responsibilities for handling, maintaining, and meeting required levels of security control for the data.

230.75.2. Purpose

The purpose of this policy is to provide data classification for confidentiality, integrity, and availability.

230.75.3. Scope

These policies include all State data located on State infrastructure or Contractor infrastructure. These policies also include data owned by Contractors if the data is used by an agency and resides on BIT managed systems. An example is Geographic Information System data. While the data may be owned by the Contractor the agency is considered the data owner for the purposes of these policies. If the data is owned by the Contractor and there are data handling requirements in the contract, the contractual data handling requirements preempts these policies.

230.75.3.1. Scope Assumptions

These policies cover all state data residing on the State's or a Contractor's system and Contractor data residing on State systems. Contractor owned data on a Contractor's system is not included.

230.75.3.2. Scope Constraints

These policies are limited to data and does not cover applications.

230.75.4. Policy

230.75.4.1. Data Classification System

Each agency shall serve as a classification authority for the data and information for which it is considered the data owner. BIT is not the data owner of data it collects or maintains for another state agency to fulfill that agency’s mission; the State agency is the data owner.

Data classification is based on three objectives:

- Confidentiality
- Integrity
- Availability

There are four risks associated with each objective:
Starting March 31, 2019, all State hosted data must be classified using Application Portfolio Management (APM). Starting June 30, 2019, all Contractor hosted data will be classified using APM. Starting March 1, 2019 all contracts must use the Data Classification Table to assess the contracts risks. This information will be entered on the Contract MOU Review Checklist and Summary. Both the Data Classification Table and the checklist can be found on the Templates: Technology Contracts webpage.

Any data that is Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), Health Information Portability and Accountability Act (HIPAA), or any information defined under State or Federal statute as confidential is automatically considered to be highly confidential. Examples risk assessments are:

- Public Assistance Records- High Risk.
- Pistol Permits Records- Medium Risk.
- Inventory of Emergency Vehicles- Low Risk.

Further information on protected information can be found in the ITSP Terms and Acronyms Directory and http://intranetbit.sd.gov/standards/PII.aspx.

All data on the State's mainframe system is automatically treated by BIT as being high risk for confidentiality, integrity and availability.

230.75.4.2. Classification of Data Produced under Contract
As part of the contract process the data owner is required to document the classification of all data produced or utilized by the project. The data classification is recorded on the Contract MOU Review Checklist and Summary provided by BIT. A copy of which will be kept by BIT and included with a copy of the contract. This includes State data that resides on a Contractor's system or data that the Contractor generates as part of a project. Also included is any State data utilized by a Contractor while providing Software as a Service (SaaS). The checklist can be found on the Templates: Technology Contracts webpage.

230.75.4.3. Data Classification Responsibilities
It is the data owner's responsibility to:

- Choose a systematic decision process to classify the data.
- Document the classification.
- Determine whether existing laws, regulations or agreements limit or regulate the collection, use, disclosure, access, retention and disposal of their state data. Agencies shall use all applicable published requirements, guidelines and limitations.
- Educate agency staff on the data classification procedures, requirements and guidelines.
- Based upon the results of the agency's data classification, establish data maintenance guidelines and communicate them to BIT.
- Establish a process to regularly review the appropriateness of the assigned data classifications and to adjust classifications in the event of:
  - Regulatory changes affecting an agency's management of information under its control.
  - Technologies for which data classification policies do not yet exist.

If the data is Protected Health Information (PHI) BIT recommends that the data owner perform a risk assessment as well as data classification.
It is BIT’s responsibility to:

- Assure that proper access controls are implemented, monitored and audited for building, floor and/or cage access in accordance with the data classification labels assigned by the data owner.
- Submit audit results to the data owners as required by law or regulation.
- Perform regular backups of state data.
- Validate data integrity.
- Restore data from backup media.
- Fulfill the data requirements specified in agency security policies, standards and guidelines pertaining to information security and data protection.
- Retain records of data activity that include information on who accessed the data and what data was accessed as considered appropriate by the federal regulatory agency responsible for establishing security controls for the data.
- Provide appropriate security controls for contractor hosted services according to the data classification labels assigned by the data owners.

**Data Center General-Access to Confidential Data-Multi-Factor Authentication**

**230.76.1. Overview**

The implementation of Multi-Factor Authentication (MFA) improves authorization access to technology systems and enhances cyber security.

MFA provides an additional layer of protection towards the access control aspect of cyber security. MFA is an authorization technology based on at least two pieces of information. This is one additional step in the authentication process beyond the standard set of user id and passwords.

**230.76.2. Purpose**

The purpose of this policy is to provide direction on MFA use within State government.

**230.76.3. Scope**

This policy applies to remote access to the State's network.

**230.76.3.1. Scope Assumptions**

The usage of MFA will meet / fulfill all audit findings against the State. The solution will meet the MFA needs of protected data, equipment and sensitive applications.

**230.76.3.2. Scope Constraints**

This policy applies to remote access of State data, equipment, and applications.

**230.76.4. Policy**

**230.76.4.1. Usage of Multi-Factor Authentication (MFA)**
Remote access is any access to a State information system by a user communicating through an external network, for example, the Internet. MFA will be required for remote access of State data, equipment and applications.

**230.76.4.2. MFA Tokens**

If a user has a mobile device enrolled in the State's standard Mobile Device Management System to gain access to State resources, that mobile device is their second factor of authentication and the user will not be issued a hard token.

Mobile device authentication is the preferred method of secondary authentication.

Hard tokens are only allowed as a user's second factor of authentication if the user does not have a mobile device enrolled in the State's standard Mobile Device Management System. A user may receive and use a hard token as their alternative second factor of authentication upon approval from BIT and at the agency's expense.

**Data Center General-Approved Disposal of State Data-Media Sanitization**

230.77.1. **Overview**

There can be a significant risk when sensitive data is collected and kept on media. This media must be appropriately sanitized when no longer needed. Media sanitization methodology is dependent on the confidentiality of the data. Effective sanitization requires knowing where the data is, what the data is, and how the data needs to be protected. Any sanitization must also be checked and documented.

230.77.2. **Purpose**

The purpose of this policy is to ensure State data is properly sanitized when it is out of the State's control.

230.77.3. **Scope**

Any media containing State data in a Contractor's control. Media is any material on which data is on or may be recorded on, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical disks. This includes both portable media and media that is installed on devices like workstations, servers, laptops, tablets, and phones.

230.77.3.1. **Scope Assumptions**

Electronic media with State data must be securely sanitized. The methods used are dependent on the confidentiality of the data.

230.77.3.2. **Scope Constraints**

Mainframe electronic media is out of scope, it has its own IRS policy requirements. Any media that is in BIT's control is also out of scope. Only media in a Contractor's control is in scope.

230.77.4. **Policy**

230.77.4.1. **Sanitization of Media in a Contractor's Control**

The required sanitization method is dependent on the data's classification, see ITSP 230.75.4.1. The data owner is responsible for classifying their data. Contractors are responsible for either sanitizing media in their care or returning it to the State as agreed to in their contract. There are two approved sanitization methods, purge or
destroy see NIST 800-88:

**Purge**- A method of sanitization by applying physical or logical techniques that renders target data recovery infeasible using state of the art laboratory techniques.

**Destroy**- A method of sanitization that renders target data recovery impossible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Using the data security classification table which can be found on this webpage, classify the confidentiality of the data. The data's status will be based on the risks associated with the data. Any data classified as no risk does not have to be sanitized. No risk data in a contractor's care is still subject to any adverse event notification requirements agreed to in their contract.

These are the media sanitization requirements:

**Low confidentiality status:**
- Purge

**Moderate confidentiality status:**
- Media is not reused - Destroy
- Media is reused - Purge

**High confidentiality status:**
- Destroy

In some cases, a Contractor is legally required to keep highly confidential State data intact or otherwise cannot sanitize the data. These circumstances are dealt with in the Contractor's contract with the State. The inability to sanitize data must be included in any response to a Request for Proposals and the data owner must be informed before any contract is signed.

Following sanitization, a Certificate of Media Sanitization should be completed for each piece of media that has been sanitized, the certificate can be found on this webpage. This certificate must be sent to the State Contact who will pass it on to Data Center Director.

### Data Center General-Transfer of Data-Secure Transfer of Data

#### 230.78.1. Overview

Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which allows data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. This term is also known as SSH File Transfer Protocol

The SFTP makes sure data is securely transferred using a private and safe data stream. The SFTP's main purpose is to transfer data but can also be used to access an FTP server. The SFTP protocol runs on a secure channel, the client user must be authenticated by the server and no clear text passwords or file data are transferred.

#### 230.78.2. Purpose
The purpose of this policy is to ensure that State data is securely transferred.

230.78.3. Scope

The policy covers any transfer of State data.

230.78.3.1. Scope Assumptions

This policy assumes that State data needs to be sent to or from outside the State's network or between non-State networks.

230.78.3.2. Scope Constraints

The policy does not cover non-State data.

230.78.4. Policy

230.78.4.1. Use of Secure File Transfer Protocol

SFTP must be used when State data is being sent outside the State's network, from another network to the State or is being sent between non-State networks.

Development-Application Security-Federal Tax Information

401.1.1. Overview

The acquisition, development, installation, and operation of all information systems must meet federal requirements necessary to protect Federal Tax Information (FTI).

401.1.2. Purpose

The purpose of this policy is to meet federal security requirements to safeguard FTI on any information system that is acquisitioned or developed by BIT.

401.1.3. Scope

The scope of this policy includes all information systems developed by BIT, contractors, or any third party that is involved in receiving, processing, storing, or transferring Federal Tax Information (FTI).

401.1.3.1. Scope Assumptions

This policy assumes that if the information system receives, processes, stores, or transfers FTI, it will be capable of being security scanned.

401.1.3.2. Scope Constraints

The policy only applies to information systems that receive, process, store, or transfer FTI. Security scans are not conducted on mainframe applications and desktop applications. Due to software licensing requirements, some vendor hosted solutions do not allow for BIT to conduct security scans. Vendor hosted solutions must still comply with federal requirements to protect FTI and must meet BIT security requirements specified in contact terms.
401.1.4. Policy

401.1.4.1. Allocation of Resources and Life Cycle Support
As part of the capital planning and investment control process, BIT will determine, document, and allocate the resources required to adequately protect information systems. Security assessments will be performed as part of the Software Development Life Cycle (SDLC) process.

401.1.4.2. Information System Security Documentation
BIT will obtain, protect as required, and make available to authorized personnel, security assessment documentation for the information system. Any newly developed or acquired software, hardware, application, or website will be required to pass a security scan:

- Prior to being moved into production.
- After a significant change.
- Prior to any updates being moved into production.

A report specifying each area reviewed or audited during the assessment process will be completed and filed. The report will include all deficiencies discovered during the assessment. A solution for each deficiency will be noted and a due date for the solution to become effective will be documented. All information regarding security assessments and official records of such will be recorded in the Pegasus system.

If BIT is unable to conduct a security scan on a vendor hosted solution, the vendor must meet all security audit and vulnerability assessment requirements deemed appropriate by BIT and provide documentation of such to BIT as specified in contract terms.

401.1.4.3. Software Usage Restrictions and User Installed Software
To safeguard FTI, BIT will comply with software usage restrictions, impose and enforce limitations on user installed software on BIT workstations. Preventing unauthorized installation of non-standard software on BIT workstations and verifying that licensing requirements are met ensures that security controls implemented by BIT are not circumvented. Software and associated documentation will be used in accordance with software contract agreements and copyright laws. BIT will track the use of software and associated documentation that is protected by quantity licenses to control copying and distribution. BIT will control and document the use of peer-to-peer file sharing technology to ensure that it is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work. Prior to installation on BIT workstations, open source software must go through the BIT moratorium process that includes, but is not limited to, a security assessment. Only authorized individuals are permitted to install software.

401.1.4.4. Developer Configuration Management
BIT requires that information system developers and integrators perform configuration management during information system SDLC and operation as well as manage and control changes to the information system to include:

- Documentation of approved changes to the information system and potential security impacts of the changes.
- Track security flaws and flaw resolution within the system.
- Implementation of only BIT approved changes.

Development-Application Security-Security Assessments

401.3.1. Overview
To ensure applications developed by BIT, contractors, or any third-party are protected and monitored to prevent unauthorized use, modification, disclosure, destruction, or denial of access to assets of the State.
401.3.2. Purpose

The purpose of this policy is to ensure that no hosted application, software, or website may be moved into production without passing a security assessment.

401.3.3. Scope

This policy applies to any software, application, or website developed by BIT, contractors, or by any third-party.

401.3.3.1. Scope Assumptions

This policy assumes that if the software, application, or website hosts any type of state government data, it will be capable of being security scanned. The security assessment will include active penetration testing and analysis of an application which can include, but is not limited to, the latest Top 10 categories of the OWASP (Open Web Application Security Project) and NIST (National Institute of Standards and Technology) standards.

401.3.3.2. Scope Constraints

Constraints on this policy include mainframe applications and desktop applications. Desktop applications are only scanned for connections to an unauthorized location or if it opens up dangerous ports.

401.3.4. Policy

401.3.4.1. Security Assessment

Configurations and installation parameters on all State applications must comply with BIT security management policies, procedures, and standards. All BIT developed software, third-party applications, internally hosted websites, and externally hosted websites must pass a security assessment prior to being accepted into production. The originator of the request to transfer to production will bear the responsibility of verifying that a security assessment has been performed. Written verification from the BIT Security Infrastructure Team (SIT) (BIT.ENTNETWORKSEC@state.sd.us) that the software, application, or website has passed the security assessment must be provided. Security assessments will be performed as part of the SDLC (Software Development Life Cycle) process. A security assessment of all applications supporting the needs of the Medical Management Information System (MMIS) and the Medicaid eligibility determination system will be conducted annually. For additional information on how to initiate a security assessment see 1451.5 Security Assessment Procedure.

401.3.4.2. Assessment Report

A report specifying each area reviewed or audited during the assessment process will be completed and filed. To view the report form, see Audit findings template follow up. The reports shall be reviewed by the BIT SIT on a quarterly basis to ensure all deficiencies have been resolved in a timely manner.

401.3.4.3. Annual Review

BIT will form an annual assessment team comprised of individuals who have been identified as having the knowledge and skills to properly assess the requirements for security controls, assessing risk, and understanding the various user needs of the system. These individuals shall also understand the consequences of non-adherence to security controls and processes. The BIT assessment team will conduct an annual assessment of security controls for applications and systems. This assessment will be performed concurrently with annual security discussions and will verify:

- The extent to which security controls are implemented correctly.
- Security controls are operating as intended.
• Security controls meet the life cycle and level of risk security requirements of the applications, websites, software, and systems.

Development-Application Security-Data Encryption

401.5.1. Overview

This policy covers rules for storing sensitive data used by applications and systems.

401.5.2. Purpose

The purpose of this policy is to outline what encryption algorithms and encryption tools are approved to use to encrypt columns in the State databases. The policy defines the minimum level of data that is required to be encrypted.

401.5.3. Scope

All data required to be encrypted must comply with this policy by June 30, 2024.

401.5.3.1. Scope Assumptions

This policy does not apply to Mainframe systems. Mainframe data is encrypted at rest which complies with IRS 1075.

401.5.3.2. Scope Constraints

This policy applies to applications and/or systems that have been developed or rewritten by BIT, contractors employed by BIT, and/or third-party vendors contracted by the State.

401.5.4. Policy

401.5.4.1. Data Encryption

All High Impact Personally Identifiable Information (PII) Data is required to be encrypted at both at rest and in transit. High Impact PII includes, but is not limited to, Social Security Numbers (SSNs), Federal Tax Information (FTI), and Protected Health Information (PHI). See BIT PII Storage Standards http://intranetbit.sd.gov/standards/PIIstorage.aspx. Other data may be recommended or required to be encrypted depending on the results of Software Development Life Cycle (SDLC) security reviews.

401.5.4.2. Hashing Values

Only values that are not going to be decrypted can use a hashing algorithm, all other values must use one of the encryption tools or algorithms listed above. Data that cannot be hashed includes, but is not limited to, Protected Health Information (PHI), Federal Tax Information (FTI), and Personally Identifiable Information (PII).

401.5.4.3. Tools


401.5.4.4. Compliance Measurements

The BIT Development Enterprise Team will verify compliance to this policy through various methods including, but not limited to, business tool reports, and internal and external audits.
401.5.4.5. Exceptions
Any exceptions to this policy must be approved in advance by the BIT Development Enterprise Team Manager.

401.5.4.6. Non-Compliance
Applications that do not meet the requirements of this policy will not be permitted into a production environment until the requirements of this policy have been satisfied.

Development-Application Security-Authentication and Authorization

401.7.1. Overview
This policy defines how authentication and authorization is implemented on websites, applications, and systems for the protection of State data.

401.7.2. Purpose
The purpose of this policy is to set the minimum requirements for how to work with and create applications, websites, and systems that require user authentication and role-based authorization of users.

401.7.3. Scope
This policy applies to all new applications, websites, and system rewrites.

401.7.3.1. Scope Assumptions
The applications, websites, or systems referred to in this policy include new development and those being rewritten. Any application, website, or system that receives, possesses, stores, or transfers Federal Tax Information (FTI) must follow the policy sections for FTI.

401.7.3.2. Scope Constraints
The applications, websites, or systems referred to in this policy must have been developed or rewritten by the Development division of BIT, contractors employed by BIT, and/or third-party vendors contracted by the State. This policy does not apply to applications or websites hosted by contractors or third-party vendors.

401.7.4. Policy

401.7.4.1. User Authentication and Authorization
If your project uses authentication and authorization of users with different roles it must include the following requirements.

- Web applications for sd.gov services that require a logon screen for user authentication must use mySD single sign on (SSO) authentication.
- Desktop applications that require user authentication functionality must use Active Directory or SSO for logon and role management, if possible.
- Mainframe systems that require user authentication functionality must use Resource Access Control Facility (RACF).
- Shared use of User Accounts is not permitted. When user accounts are created, they must be created for an individual - not for a group.
If custom authentication is required, it must be approved before the project begins, unless an exception has already been granted.

401.7.4.2. **Password Requirements**
The following password requirements must be built into your project.

1. Enforce a minimum password complexity of:
   - Eight-character minimum and a maximum of 64 characters.
   - At least one numeric and at least one special character.
   - A mixture of at least one uppercase and at least one lowercase letter.
   - Storing and transmitting only encrypted representations of passwords.
2. Enforce password minimum lifetime restriction of one day
3. Prohibit Password reuse for 24 generations
4. Allow the use of a temporary password for system logon requiring an immediate change to a permanent password
5. Password-protect system initialization (boot) settings
6. Allow passwords to be copied and pasted into the login.
7. No passwords hint.
8. No knowledge-based authentication. (For example, what was the name of your first pet?).

If your project involves FTI it must include the following requirements, in addition to those listed above.

- Enforce non-privileged account passwords to be changed at least every 90 days.
- Enforce privileged account passwords to be changed at least every 60 days.

401.7.4.3. **Invalid Login Attempts for projects using Federal Tax Information**
If your project involves FTI, it must include the following requirements.

- Enforce a limit of three consecutive invalid login attempts by a user during a 120-minute period by automatically locking the account for a period of at least 15 minutes.
- Prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.
- Retain the session lock until the user reestablishes access using established identification and authentication procedures.
- The information system must automatically terminate a user session after 30 minutes of inactivity.

401.7.4.4. **reCAPTCHA**
ReCAPTCHA will be required on all login pages and public facing form submissions unless they are protected by a login page that already uses reCAPTCHA. For more details on how to implement reCAPTCHA, see Procedure 1451.3.

401.7.4.5. **Tools**
For instructions on how to use mySD in your application, visit mySD.sd.gov and click Developer Toolkits.

401.7.4.6. **Compliance Measurements**
The BIT Development Enterprise Team will verify compliance to this policy through various methods including, but not limited to business tool reports and internal and external audits.

401.7.4.7. **Exceptions**
Any exceptions to this policy must first be approved in advance by the Development Enterprise Team Manager.

401.7.4.8. **Non-Compliance**
Network-Service-Access Control

610.1.1. Overview

Access to the technology infrastructure of the State is essential to maintaining a productive workforce. With this access comes the risk and responsibility of approving, monitoring, and securing the users, workstations, and systems being accessed to protect their confidentiality, integrity, and availability. Controlling access to State technology systems is paramount to avoid damages. Such damages include loss of sensitive or confidential data, destruction or theft of intellectual property, harm to public image, disruption of or damage to public safety activities, and fines or financial liabilities incurred as a result of the damage.

610.1.2. Purpose

The purpose of this policy is to establish rules, guidelines and expectations surrounding access to State technology resources.

610.1.3. Scope

BIT is responsible for designing, configuring and maintaining access to technology systems owned by or operated for the State and its citizens. To supply reliable and secure access, standards and policies for limiting and controlling technology access are established in this policy.

- All State employees and contractors with a State-owned or non-State-owned workstation used to connect to the State network or State infrastructure;
- Remote access connections, to include but not limited to the Internet, used to complete tasks on behalf of the State, including email access and viewing Intranet resources;
- All workstations and devices utilized, and the technical implementations of access used to connect to State networks;
- Communication - originating from and to - DDN Intranet and DMZ.

610.1.3.1. Scope Assumptions

BIT has standardized access control methods and technologies. Only users, workstations, accounts and services compliant with or outlined in this policy are permitted within the DDN. An Agency specific clause is documented in the policy section. The policy applies to the Department of Social Services systems and applications referenced. The policy assumes that Department of Social Services systems and applications referenced are supported or maintained by developers and support staff who have access to remote connections.

610.1.3.2. Scope Constraints

While this policy applies to BIT managed technology systems at our K-12 and Higher Education client locations, this policy does not apply to users and workstations managed and operated by those institutions on their local networks.

610.1.4. Policy

610.1.4.1. System Access Expectations
All access for user and/or system level rights must be granted, reviewed and approved by BIT for accuracy and adequacy to ensure that the appropriate level of access for the intended functions is granted. All access methods utilized to connect to State networks must be implemented through approved combinations of hardware and software security tools that have:

- Unique identification or UID for each user.
- System level identification for each system (e.g. Active Directory accounts).
- Capability to restrict access to specific nodes or network applications.
- Access control software or hardware that protects stored data and the security system from tampering. Audit trails of successful and unsuccessful log-in/access attempts.
- Account credentials must not be stored in unencrypted fashion on any workstation or storage platform.

If a system requires access control methods that fall outside of the listed requirements, the agency sponsoring or requesting that system must work with their BIT Point of Contact to engage BIT in a review of this system. If an exemption would be required, the Security Exemption Request Form at the BIT Intranet (http://intranet.bit.sd.gov/forms) must be submitted to the BIT HELP Desk (773-4357) for exemption considerations. Unrestricted access into or out of the DDN Intranet and/or DMZ is prohibited. Systems or applications that must call out to a remote system or "call home" for any reason must be vetted and approved by BIT prior to their installation within State infrastructure.

### 610.1.4.2. Contractor Access

Access to the DDN Intranet and DMZ by contractors is rigorously controlled and managed. The following rules apply to any contractors connecting to State infrastructure:

- Requests for contractor access to technology infrastructure must be approved by BIT. A Security Exemption Form, located at the BIT Intranet (http://intranet.bit.sd.gov/forms), submitted to the BIT HELP Desk (773-4357) is required to gain any level of access to State technology systems.
- Contractor access will be limited to the bare-minimum number of systems necessary to accomplish BIT-approved tasks and procedures. This access will be controlled by any number of mechanisms, to include, but not limited to, user accounts, firewall policies, Group Policy, scheduled lockdown and maintenance windows, and/or Skype for Business remote access with BIT personnel monitoring and controlling the access.
- Contractors will not have any access to State workstations without explicit authorization from the BIT Commissioner or BIT Chief Information Security Officer. A Security Exemption Form, located at the BIT Intranet (http://intranet.bit.sd.gov/forms), submitted to the BIT HELP Desk (773-4357) is required to request access.
- Administrative accounts on State technology systems must be fully vetted by BIT, periodically reviewed for accuracy and necessity, and limited to the minimum level of systems and access necessary. Domain, enterprise, or similar administrative access levels are strictly prohibited for contractors.

### 610.1.4.3. Modems

Dial-in or dial-out telephony modems are not allowed to be connected to servers or any other technical assets of the State for any use. Digital Subscription Lines (DSL), cellular and cable modems managed by BIT are not considered telephony modems under this policy.

### 610.1.4.4. Remote Access

Remote access to the DDN Intranet and DMZ, to include all data files and applications, must be BIT managed, secured and encrypted. Any remote access where Federal Tax Information (FTI) and or Criminal Justice Information System (CJIS) data is accessed over the remote connection must be performed using multi-factor authentication. Supported forms for remote access are:

- Secure Sockets Layer (SSL) - an Internet Web Browser with a minimum of 256-bit encryption.
- CSG - the Citrix Secure Gateway of the State.
• NetMotion - a VPN client maintained by BIT.
• Horizon View (VDI).
• Skype for Business - a collaboration system operated by BIT, can be used if and only if a BIT staffer monitors and manages the access during all remote access sessions.

SSL VPNs are not permitted under any circumstances. There is no direct remote access using Remote Desktop Protocol (RDP) allowed from the Internet to the State network or to any cloud-based resource with access to the State network. Indirect RDP access from the Internet is only allowed if it goes through a BIT-approved remote access service.

610.1.4.5. Inspection and Review
BIT will verify compliance to this policy through a number of methods, including but not limited to: periodic walk-throughs, video monitoring, internal and external audits, automated systems processes, business tool reports, and inspections. Feedback will be provided to the required entities.

610.1.4.6. Department of Social Services
In November of each year, a review will be conducted of all personnel with remote access to a major system supporting the needs of the Medicaid Management Information System (MMIS).

• A document will be generated and filed containing the names of personnel with remote access and privileged functions.
• If a determination is made that an individual no longer requires remote access to MMIS, then the remote access will be terminated.

In November of each year, a review will be conducted of all personnel with remote access to a major system supporting the needs of the Division of Child Support.

• A document will be generated and filed containing the names of personnel with remote access and privileged functions.
• If a determination is made that an individual no longer requires remote access to the Division of Child Support System, then the remote access will be terminated.

Network-Concept-Security Domain Zones

610.3.1. Overview
All devices connected to any technology infrastructure of the State must be protected. The connections must be designed and implemented to ensure compliance with the access control policies for each connected system.

610.3.2. Purpose
Different areas or zones of the State network require different levels of protection and security. This policy will define the different zones and expectations for each zone.

610.3.3. Scope
Links to external networks, including but necessarily not limited to, the Internet, federal agencies, and third-party companies must be managed by BIT to ensure the security of the technology infrastructure of the State.

610.3.3.1. Scope Assumptions
All individuals that utilize the DDN must work with BIT to define business practices or align connectivity into one of the three security domain zones which are the Intranet Zone, De-Militarized Zone (DMZ), and Extranet Zone. BIT will not always be able to allow devices and assets to communicate amongst the Security Domain Zones for security reasons, which can include Federal requirements.

610.3.3.2. Scope Constraints

Networks outside of the control of BIT, such as the local university networks operated by Higher Education are outside of the scope of this policy.

610.3.4. Policy

610.3.4.1. Intranet

The Intranet zone is the private, internal network that contains traditional clients of the State and internal business systems. To access the Intranet from external locations, such as the Public Internet, a Firewall Modification Request Form must be completed at the BIT Intranet (http://intranet.bit.sd.gov/forms). Only approved methods and technologies can be used to traverse into the Intranet from other network zones.

610.3.4.2. DMZ

The DMZ is the portion of the DDN that provides limited security services and is designed to support services and systems that are utilized by external users. In most situations, the external users require access to resources in the DMZ from the Public Internet. All services and systems that need to be publicly accessible must be placed within the DMZ zone. Access to the DMZ from external locations will require an approved Firewall Modification Request Form completed at the BIT Intranet (http://intranet.bit.sd.gov/forms).

610.3.4.3. Extranet

The Extranet zone is segmented from the Intranet zone and the DMZ zone to support network connections for agencies that are not part of the infrastructure of the State Intranet due to business situations. Access to the Extranet from external locations will require an approved Firewall Modification Request Form completed at the BIT Intranet (http://intranet.bit.sd.gov/forms).

Network-Concept-Network Integrity

610.9.1. Overview

The DDN is a complex network containing a multitude of inter-dependent systems, connections, and roles. Adequate security measures must be in place to protect the technical assets of the State - physically and logically - from damage, theft, vandalism, and other forms of threats to maintain the integrity of the network.

610.9.2. Purpose

This policy is to establish the baselines of how network integrity is maintained through technology standards and personnel practices. Adequate security measures must be in place through these standards to protect the technical assets of the State.

610.9.3. Scope

Technologies, contracts, and practices, to include hardware, software or circuits, must be physically and logically protected against theft, damage, and misuse.

610.9.3.1. Scope Assumptions
By maintaining accurate accountability of property and instituting appropriate countermeasures to safeguard property, the opportunity for loss, theft or pilferage of valuable technical resources can be greatly diminished. Clients that request the construction of a local or wide area network will work with BIT for the design, implementation, and support matrix of the proposed network segment.

610.9.3.2. Scope Constraints

While this policy applies to BIT managed equipment at BIT’s higher education client locations, this policy does not include the internal networks of BIT’s higher education clients.

610.9.4. Policy

610.9.4.1. Responsibilities
BIT is responsible for providing secure and reliable network connectivity through approved and managed platforms for agencies. This responsibility encompasses local networks, wide-area networks, wireless networks, cellular networks, secure remote access networks, and relevant security components.

610.9.4.2. Management
BIT will manage network connectivity platforms for agencies. This responsibility encompasses local networks, wide-area networks, wireless networks, cellular networks, secure remote access networks, and relevant security components.

610.9.4.3. Disabling Critical Components of Network Security Infrastructure
Critical components of the BIT network security infrastructure must not be disabled, bypassed or turned off without prior approval from the Director of the Division of Telecommunications or their designee(s).

610.9.4.4. Technical Asset or Contractor Connections
Connection of any contractor and/or their equipment to the DDN or any subsystem requires prior approval from the BIT Commissioner or their designee(s). To request any equipment to be installed or connected to the DDN, requestors will begin by submitting a request to the BIT HELP Desk (773-4357) and must provide two weeks' notice. The request must include the dates, times, duration of connection, and the reasons for the connectivity. The requestor must be ready to provide the technical device, any available documentation, and technical contacts to BIT.

610.9.4.5. Local Area Network
All LANs must follow the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard for wired Ethernet networks. State wireless networks operate only in accordance to the wireless policy. Devices and systems in use must meet the specifications laid out by IEEE, to include but not necessarily limited to: 802.1x, 802.3x full duplex, 802.3, 802.3z 1000BASE-LX, 802.3ab 1000BASE-T, 802.3z 1000BASE-X, 802.3ae 10GbE LAN-PHY, 802.1w RSTP, 802.1s, 802.3ad with LACP support, 802.1Q. Wired network ports that are not individually identified as in use by a State employee, such as those in conference rooms or public areas, will remain disabled unless specifically requested via the BIT HELP Desk (773-4357). Requests must include the dates and times these ports will be used by State employees.

610.9.4.6. Wide Area Network
To assure privacy through carrier networks, all carrier-based services utilize private virtual links in a fashion determined and maintained by BIT. This can include, but is not necessarily limited to, carrier managed Multiprotocol Label Switching (MPLS) networks, Metro Ethernet (MEF) networks, dark fiber networks, or IPSec secured virtual private networks (VPNs) over commercial Internet services. Secure socket layer (SSL) VPNs are not allowed in any location on the network.

610.9.4.7. Physical Controls
All line junction points to include cable and line facilities must be located in secure areas or an area that is locked with a key or similar allowed system. Devices to include but not limited to firewalls, servers, switches, hubs, routers, and wireless access points, must be protected from unauthorized physical access.

Network-Communication-Internet

610.11.1. Overview

All devices connected to any technology infrastructure of the State must be protected. BIT is responsible for defining and managing the method, services, and providers used to access the Internet. The Internet is a tremendous tool to be utilized by the State, but the open-system architecture of the Internet creates risks that must be mitigated; BIT does not control the Internet. All Internet access to or originating from the DDN must be approved through the BIT HELP Desk (773-4357).

610.11.2. Purpose

Access to and access from the Internet is approved, managed, and maintained by BIT.

610.11.3. Scope

This policy establishes acceptable expectations for connections from a State office or connected entity to the public Internet. It establishes rules and regulations for the types of, ownership of, and equipment involved in public Internet connections and the DDN.

610.11.3.1. Scope Assumptions

Devices or networks connected to the DDN are expected to comply with this policy.

610.11.3.2. Scope Constraints

Networks not fully under the management of BIT, such as the local county government networks in a courthouse, are out of scope for this policy.

610.11.4. Policy

610.11.4.1. Multiple Connections

No entity or device that participates on the DDN may maintain or install an Internet connection on a network that is also connected to the DDN. Devices are not permitted to be dual-homed (connected to the DDN and the public Internet simultaneously). All traffic destined to the Internet from a DDN-connected entity or arriving from the Internet to the DDN must be through BIT managed solutions. K-12 schools or Post-Secondary Educational institutions that are connected to the DDN are not allowed to have a connection to a public ISP.

610.11.4.2. Interfaces

Establishing a direct, real-time connection between the DDN and external organizations networks, such as Federal Government, contractor support, or any other public or private network, must be approved by BIT. Additional tasks may be required from BIT to determine what additional suitable security measures can be implemented for the connection. All real-time, external connections to the technology infrastructure of the State must pass through a firewall or a similar technology entry point.

610.11.4.3. Security
Only services that are explicitly authorized by BIT will be permitted inbound and outbound between the DDN Intranet and the Internet. BIT is responsible for periodically reviewing the implemented security rules for devices that manage inbound and outbound connections. Depending on vulnerabilities and other security risks identified, access to the Internet and from the Internet to the DDN can be restricted and/or expanded without notice. Individuals may not probe security mechanisms at any DDN site, State facility or Internet location without specific, written permission that has been obtained from an authoritative person from each of the affected entities. Similarly, any scanning or security probing activity against a DDN site or State facility requires written permission from the BIT Chief Information Security Officer before such an activity is performed. Unauthorized behavior will be referred to the appropriate law enforcement agency.

610.11.4.4. Responsibilities
Devices connected to the DDN may not be used to make unauthorized connections, to break into, or adversely affect the performance of any asset on the DDN or the Internet. All equipment of the State, including but not limited to, workstations, email system, Internet access tools, and other information systems, are restricted to official State business use only.

610.11.4.5. IPv4/IPv6 and Device Names
BIT is responsible for the management of the DDN public IPv4/IPv6 address space which has components used by the State to include the assignment of device names. Workstations and servers are required to use Dynamic Host Configuration Protocol (DHCP) for the assignment of IPv4/IPv6 addresses. Requests for an exemption from DHCP must be submitted to the BIT HELP Desk (773-4357) for review using the Security Exemption Request Form at the BIT Intranet (http://intranet.bit.sd.gov/forms). For application access, applications are prohibited from using individual IPv4/IPv6 addresses. Domain names must be created for application reference instead of IPv4/IPv6 address. Requests for an exemption from references to domain names must be submitted to the BIT HELP Desk (773-4357) for review using the Security Exemption Request Form at the BIT Intranet (http://intranet.bit.sd.gov/forms). If an exemption is granted, the requestor assumes all liability for the support and the maintenance of the application when the host address is required to change due to infrastructure changes on the DDN. IPv4/IPv6 Addresses and device names are considered classified, private information of the State. Naming standards and IPv4/IPv6 addresses for workstations, servers, networking equipment, security devices, and any other technical device are classified as protected, nonpublic information that may not be distributed without express, written approval of the BIT Commissioner to an entity not associated with the State. Other internal network addresses, identifiers, configurations, and related system design information for the technology infrastructure of the State must be restricted. Technical devices and users outside the DDN must be unable to access classified information without explicit management approval. Exemptions to information access must be submitted to the BIT HELP Desk (773-4357) using the Security Exemption Request Form at the BIT Intranet (http://intranet.bit.sd.gov/forms).

Security-Network Discovery-Probing-Exploiting

620.1.1. Overview
BIT establishes and maintains security controls to secure State devices and protect data; therefore, it is important to provide guidelines to strictly prohibit individuals from probing the DDN network, including network, service and port discovery, or trying to exploit these security controls that exist on the DDN.

620.1.2. Purpose
This policy is designed to provide clarification on Probing/Exploiting Security Controls.

620.1.3. Scope
This policy provides a baseline set of expectations for security policies as applied to the State information technology systems.

620.1.3.1. Scope Assumptions

Security controls are tested frequently throughout the State infrastructure. This includes testing all BIT managed devices; external devices that require connectivity, including contractors and other unmanaged connections; workstations used by K-12 and Higher Education.

620.1.3.2. Scope Constraints

While this policy applies to BIT managed devices and users at our K-12 and Higher Education client locations, it does not apply to the local devices and networks operated by those institutions.

620.1.4. Policy

620.1.4.1. Limiting Tool Functionality

Technical tools must be used as directed by the manufacturer or BIT. Utilizing technical tools to cause damage to devices or disrupting the desired data flow across the DDN is prohibited. Authorization to use software such as packet capture, network probing, and network and endpoint discovery tools for troubleshooting activities does not imply that consent has been provided to utilize these tools without limitations. Individuals, identified in name, by the Director of the Division of Telecommunications are permitted to use discretion to expand the functionality of technical tools.

620.1.4.2. Exploiting Security Controls of Information Systems

All individuals must not exploit vulnerabilities or deficiencies found in information systems or perform probing of State network devices to damage systems or data. It is not permitted to obtain information that the individual is not authorized to view, to take resources away from other individuals, or to gain access to other systems for which proper authorization has not been granted. Any exploitation of vulnerabilities in information systems and damage from scanning or probing found must be reported using the Detailed Incident form located on the BIT Intranet.

620.1.4.3. Cracking Application or Passwords

All individuals are strictly prohibited from "cracking" passwords of the technical assets that exist on the DDN. Exemptions must be approved, in advance, and in writing, by the BIT Chief Security Information Officer. The Security Exemption Request Form at the BIT Intranet (http://intranet.bit.sd.gov/forms) must be used to request an exemption. Individuals, identified in name, by the Director of the Division of Telecommunications are permitted to "crack" passwords.

620.1.4.4. Exemptions

Exemptions must be approved, in advance, and in writing, by the BIT Chief Information Security Officer. Activities that are prohibited include but are not limited to the use of scanning software and utilities, keylogging devices, vulnerability assessment tools, and denial-of-service utilities. Exemptions for probing and exploiting security controls must be submitted to the BIT HELP Desk (773-4357) by using the Security Exemption Request Form at the BIT Intranet (http://intranet.bit.sd.gov/forms).

Security-Content Control-Internet Filtering

620.5.1. Overview
All content accessed from the DDN must be sufficiently protected and monitored to be consistent with BIT Information Technology Security policies. These policies are designed to prevent unauthorized use, modification, disclosure, destruction or denial of access to State assets. Therefore, Internet traffic is monitored for all users and workstations connected to the DDN Intranet. Domain administrative accounts are prohibited from browsing the Internet.

620.5.2. Purpose

Primary purpose is to protect and secure information and assets managed by the State. Secondary purpose is to inform and educate users of their responsibilities towards the use of information, products, and services obtained from the Internet.

620.5.3. Scope

This policy incorporates all users initiating communication between workstations connected to the DDN and the Internet, including web browsing, (IM) instant messaging, file transfer, file sharing and the Intranet.

620.5.3.1. Scope Assumptions

Content filtering is provided to all users to protect them from the unintentional or deliberate accessing of Internet content that is offensive and inappropriate. Employees, contractors, and devices connected to the DDN must adhere to this policy.

620.5.3.2. Scope Constraints

This policy does not apply to K-12 and Higher Education accounts with administrator privileges. While this policy applies to BIT managed devices and users at our K-12 and Higher Education client locations, it does not apply to the local devices operated by those institutions.

620.5.4. Policy

620.5.4.1. Exemptions

If requesting a filter exemption, then justification is required. Exemptions to this policy must be submitted to BIT via the Security Exemption Request Form at the BIT Intranet (http://intranet.bit.sd.gov/forms). BIT will review the impact to the technology infrastructure of the State for each requested exemption; the period for the review process should not exceed two weeks. Exemption Details:

- All Internet filtering exemptions must be approved by the BIT Commissioner.
- All requests for the data of an individual pertaining to Internet practices must come from the Department Secretary or Bureau Commissioner of the agency directly to the BIT Commissioner as requests for data are handled at the highest level possible.
- A report on an individual should be completed within two weeks. All requests for data must be approved by the BIT Commissioner.

620.5.4.2. Appropriate Use of Administrator Access

Accounts that are members of the SD Domain Administrators group have administrator access to Active Directory services and systems. Use of those accounts specific to Internet access is strictly prohibited. These include Administrators, Domain Administrators, and other accounts with a level of access beyond that of a normal user account. Use of these privileged accounts is restricted to administrative responsibilities and must be prohibited from non-administrative activities. Web browsing or any access to/from the Internet under an Administrator role is strictly prohibited. A malicious website can be used to compromise a workstation or server while online. A
compromised asset with elevated Administrative privileges can cause significant additional harm over that of a normal user account.

620.5.4.3. **DDN Content Filtering**
BIT does not manage filtering of any degree for K-12 schools. BIT does not manage content filtering of any degree for Higher Education facilities. K-12 and Higher Education are completely responsible for the content that is permitted or blocked for their institutions.

620.5.4.4. **DDN Intranet Content Filtering**
BIT policy shall block access to the following categories, based on standard Web filtering suggestions. These categories are deemed inappropriate:

- Adult/Sexually Explicit Material
- Gambling
- Hacking
- Illegal Drugs
- Personals and Dating
- Malicious Websites
- Phishing
- Tasteless and Offensive Content
- Violence, Intolerance, and Hate
- Weapons
- Web Based Email
- Peer to Peer (P2P) File Sharing

620.5.4.5. **Filter Exemption Requests**
If access to a blocked Internet site is necessary for reasons related to work expectations or data is needed to understand the Internet surfing habits of an individual, the Department Secretary, Bureau Commissioner, or Executive Leadership must submit a request directly to the BIT Commissioner through the BIT HELP Desk (773-4357). Requests related to Internet site administration for the individual to meet work expectations or individual investigations are handled at the highest management level possible. Requests for access to blocked sites and requests for information on surfing habits are documented in the work order system maintained by the BIT HELP Desk (773-4357). The content-filtering category database of the filtering solution is updated daily. Requests must include:

- The name(s) of the requestor.
- The phone number(s) of the requestor.
- The SD Domain UID(s) of the requestor;
- The site for which access is required or the scope of the data requested for an individual.
- The length of time required for access to the site or the time-period to be recorded in a report.
**TERMS**

**Abstraction Technologies**
The removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services. *See also Directory, IP Address, and Relative Pathing.*

**Access Attempts**
When a user tries but fails to connect to an application or database so that they can make use of the resource.

**Accreditation (also referred to as Vulnerability Assessment)**
Scanning of a system looking for security vulnerabilities.

**Accreditation Boundary**
All components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected. If a set of information resources is identified as an information system, the resources should:
- Generally, be under the same direct management control.
- Have the same function or mission objective and essentially the same operating characteristics and security needs.
- Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments.)

**ADABAS**
Software AG's database management system (DBMS). ADABAS organizes and accesses data according to relationships among data fields. The relationships among data fields are expressed by ADABAS files, which consist of data fields and logical records.

**Ad hoc Networking (WANET or MANET)**
A decentralized type of wireless network, considered ad hoc because it does not rely on a pre-existing infrastructure, such as routers or access points.

**Adverse Event**
An observable occurrence where there is unauthorized use of system privileges, unauthorized access to State data, execution of malware, physical intrusions, or electronic intrusions that may include network, applications, servers, workstations, and social engineering of staff.

**Agency**
An association, authority, board, commission, committee, council, department, division, task force or office within the Executive Branch of State government. Includes the staff of that individual department.

**Application**
A complete and self-contained program or group of programs designed to perform a function for the user.

**Application Scans**
Scans performed by BIT against business software applications to identify security vulnerabilities. This includes applications BIT writes and software that is procured from other software companies.

**Application Server**
A type of server designed to install, either on workstations or other servers, operate, host applications, and associated services for end users and I/T services. It facilitates the hosting and delivery of applications, which are used by multiple and simultaneously connected local or remote users.

**Authorized Developer**
An individual which has been granted permission and access to systems by an administrator of said system so that they can build and create software and applications.

**Authorized Persons**
The vendor’s and their employees, contractors, subcontractors, or other agents who need and have been granted access to the State's data or IT facilities to enable the Vendor to perform the services required.

**Back Door**
Access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes during development. Attackers can use back doors that they detect, or install themselves, to gain access to an application or database for malicious purposes.

**Blocked mail**
Incoming emails which are being stopped at the mail gateway because they are or appear to be phishing emails, spam, or they have malicious attachments.

**Bluetooth**
The wireless communication technology that conforms to the Bluetooth computing and telecommunications industry specification. This specification describes how mobile phone, landline phones, computers, and mobile devices can easily exchange information by using a short-range wireless connection.

**Browser**
A software application used to locate, retrieve, and display content from the World Wide Web, including Web pages, images, video, and other files.

**Brute Force Attack**
A hacker sets up an automated process against login pages to repeatedly test the user id or password. If they guess a correct combination, they have gained access to the system.

**Bureau of Information and Telecommunications**
The Bureau of Information and Telecommunications which strives to partner and collaborate with clients in support of
their missions through innovative information technology consulting, systems, and solutions.

Business Associate (BA)
A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity or another Business Associate. Business associate functions and activities include: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Business associate services are: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. BIT is considered a Business Associate of DSS, DOH, DHS, and BHR.

Business Associate Agreement (BAA)
An agreement with a third party or vendor to assure the State that the vendor is appropriately protecting confidential client information and data. If a governmental agency is the BA of another governmental agency who is the covered entity a MOU maybe substituted for a BAA. See also Regulated data and Health Information Portability and Accountability Act.

Chief Information Security Officer (CISO)
BIT senior executive charged with implementing the information technology security programs for the State.

Circuit
A theoretical structure simulating electrical and data paths.

Closed Source
Proprietary software where the state does not hold the copyright.

Cloud Service
Services made available to users on demand via the internet from a cloud computing provider’s server as opposed to being provided by the State’s on-premise servers. See also Infrastructure as a Service and Platform as a Service.

Code
The instructions commonly used in a program that cause a computer to perform a specific task.

Commercial off the Shelf Software
Closed source software that is purchased and used by the State with no changes made by the vendor.

Communication Protocols
The agreed upon format for data that allows the data to be sent between computers.

Connectivity
The ability of hardware devices or software packages to transmit data between other devices or packages.

Content Filtering
Using a program to screen and exclude from access or availability, Web pages or email that is deemed objectionable.

Contractor
Regarding a signatory to a contract or agreement, the terms Contractor, Consultant, and Vendor are equivalent. Subcontractors, Agents, Assigns and/or Affiliated Entities are not signatories to the contract or agreement. The ITSP may be attached to the contract or agreement and all policies in the ITSP apply to all.

Covered Entity
A HIPAA covered entity is any organization or corporation that directly handles Personal Health Information (PHI) or Personal Health Records (PHR). The most common examples of covered entities include hospitals, doctors’ offices, and health insurance providers. DSS, DOH, and BHR are covered entities. See also Business Associate, Regulated data and Health Information Portability and Accountability Act.

Cracking passwords
The process of recovering passwords from data that have been stored in or transmitted by a computer system.

Credentials
Credentials are a UID plus additional information and data such as a password, account number, or access code. Examples are:
- RACF
- NATURAL

Data and Information Types
Data is measured, collected, reported, and analyzed. Data as a general concept refers to the fact that some existing information or knowledge is represented or coded in some form suitable for better usage or processing. Pieces of data are individual pieces of information.

Data and Information Types: Confidential
Any data or information, other than trade secrets, that is materially sensitive in nature, whether manual or electronic, which is valuable and not generally known to the public. Identified here, are few examples, this list is not inclusive. Personally Identifiable Information which is not in the public domain, and if improperly disclosed could be used to steal the identity of an individual, violate the right of an individual to privacy or otherwise harm the individual or business to include, but is not limited to social security numbers, tax payer identification numbers, and any other department determined data that is not in the public domain or intended for release to the public domain and if improperly disclosed might:
- Cause a significant or severe degradation in mission capability.
- Cause loss of organizational integrity or public confidence.
- Result in significant or major damage to organizational assets.
Data and Information Types: Federal Tax Information (FTI)
Consists of returns or return information and may contain personally identifiable information (PII). FTI is any return or return information and data received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information and data. FTI does not include information and data provided directly by the taxpayer or third parties. If the taxpayer or third party subsequently provides returns, return information and data or other PII independently, the information and data is not FTI as long as the IRS source information and data is replaced with the newly provided information and data.

Data and Information Types: Personally Identifiable Information (PII)
Any information about an individual that is maintained or collected by an agency, including:
- Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Data and Information Types: Protected
Very specific types of data regulated by law, which includes but is not limited to PCI, FERPA, HIPAA, GLBA, ITAR and EAR.
- FERPA: Education records are protected by FERPA (Family Educational Rights and Privacy Act). For example, tax records of parents and students, class lists, grade rosters, records of advising sessions, grades, and financial aid applications.
- HIPAA: Certain health information and data is protected by HIPAA (Health Information Portability and Accountability Act) if it is individually identifiable and held or transmitted by a covered entity. For example, health records, patient treatment information and data, health insurance billing information and data.
- GLBA: Financial records are protected by GLBA (Gramm-Leach-Bliley Financial Services Modernization Act).
- ITAR and EAR: Export Controlled Research is protected by ITAR (International Traffic in Arms Regulations) and EAR (Export Administration Regulations). For example, dual-use technology used for scientific advancement as well as military applications, see SDCL 1-27-1.5.

Data and Information Types: Return Information
Any information and data collected, or generated, by the IRS with regard to any person’s liability, or possible liability, under the Internal Revenue Code (IRC). Return information and data includes, but is not limited to:
- Information and data, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense;
- Information and data extracted from a return, including names of dependents or the location of business, the taxpayer's name, address, and identification number. Information and data collected by the IRS about any person’s tax affairs, even if identifiers, such as name, address, and identification number are deleted. FTI may include PII. FTI may include the following PII elements:
  - The name of a person with respect to whom a return is filed
  - His or her mailing address
  - His or her taxpayer identification number
  - Email addresses
  - Telephone numbers
  - Social Security Numbers
  - Bank account numbers
  - Date and place of birth
  - Mother's maiden name
  - Biometric data (e.g., height, weight, eye color, fingerprints)
  - Any combination of the preceding.

Returns are forms submitted on paper or electronically with return information to the IRS by, or on behalf of, or with respect to any person or entity. Examples can include Forms 1040, 941, 1120 and other informational forms, such as 1099 or W-2.

Data and Information Types: Sensitive
Any information and data not available to the public via the Freedom of Information Act or the State Open Records Laws SDCL 1-27.

Data and Information Types: Trade Secret
Any scientific or technical information and data, design, process, procedure, formula, pattern, compilation, program, device, method, technique, process, strategic planning information or improvement whether manual or electronic that is:
- Valuable and not generally known to the public, including, but not limited to, workstation software programs;
- Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use;
- The subject of efforts that are reasonable under the circumstances to maintain its secrecy, see SDCL 1-27-30.

Database
An organized collection of data that supports the processing of the data to provide information.
Data Breach
The unauthorized access by a non-authorized person(s) that result in the use, disclosure, corruption, or theft of State's data.

Data Mining
The analysis of a data base to extract patterns that can be used to learn more about the user; usually used for marketing purposes.

Dataset
A collection of related sets of information and data that is composed of separate elements but can be manipulated as a unit by a workstation.

DDN Intranet
The private, internal network of State government. Executive, judicial branch and constitutional offices connect to the internal aspect of the DDN. The DMZ, K12, REED are examples of external aspects of the DDN.

De-Militarized Zone (DMZ)
A perimeter network that contains external-network facing services. Applications needing access from the public Internet are located in the DMZ.

Digital Dakota Network (DDN)
The name of the Statewide workstation network including, but not limited to, data, video, and VoIP services that connects many entities together, including the local and wide area networks of the Executive & Judicial branches, K12 schools and Board of Regents.

Directory
The service that identifies all resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, computers, and peripheral devices such as printers. The directory service allows a user on a network to access any resource without knowing where or how it is physically connected.

Distributed Denial of Service (DDOS)
A botnet is a series of computers compromised. A DDOS attack utilizes one or more botnets to target a single computer or website. The massive amount of botnet traffic overloads the recipient with more data than it can handle, resulting in service delays or outages. The counts indicate the number of attacks targeting the Board of Regents, K12 public schools and State government.

Domain Name
A name owned by a person or organization and consisting of an alphabetical or alphanumemiric sequence followed by a suffix. It is used as an Internet address to identify the location of specific Web pages.

Dynamic Naming System (DNS)
An automated means of translating Internet URLs into the equivalent IP address (translating web addresses from near-English into the URL’s digital address).

Easter Egg
A secret message buried in an application.

Employee
Anyone employed directly by the State of South Dakota or employed by any third-party company (contractor or subcontractor) that has a contract to provide work for a State government agency. Contractors and Employees are treated identically throughout the Information Technology Security Policy.

End User Data
Data that is not state data but is non-public or personal data provided by an entity other than the state and is used by someone other than the state.

External Network
Any network that resides outside of the established security perimeter.

Extranet
A controlled private network that allows access to an authorized set of customers.

Fail Over
The process that takes place when a computing resource fails, and the functions are automatically moved to another computing resource.

Federal Parent Locator System (FPLS)
The FPLS is an assembly of systems operated by Office of Child Support Enforcement (OCSE), to assist states in locating noncustodial parents, putative fathers, and custodial parties for the establishment of paternity and child support obligations, as well as the enforcement and modification of orders for child support, custody, and visitation. It also identifies support orders or support cases involving the same parties in different states. The FPLS helps federal and state agencies identify over-payments and fraud and assists with assessing benefits.

Federal Tax Information (FTI)
Tax returns or tax return information received from the IRS or secondary source. Information, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person for any tax, penalty, interest, fine, forfeiture, or other imposition or offense and (2) Information extracted from a return, including names of dependents or the (2) location of business (3) The taxpayer’s name, address, and identification number (4) Information collected by the IRS about any person’s tax affairs, even if identifiers, such as name, address, and identification number are deleted.

File Transfer Protocol (FTP)
A standard network protocol used to transfer data files between one workstation network and another.
Firewall
A set of related programs, located on a state network gateway server that protects the resources of the state’s network from unauthorized users from other networks.

Hackers
Individuals or a group of individuals with the intent of doing harm to state data, infrastructure, or services.

Hot Spot
A physical location where people may obtain Internet access.

Hypervisor
A program that is running one or more virtual machines on a single physical server. See also virtualization.

Identity Theft
When a hacker gains access to enough personal information about someone that they can impersonate one to acquire financing in that person’s name or can gain access to data networks as that person.

Inbound Traffic
Network traffic that originates outside of the enterprise network with a destination inside the network.

Individually Identifiable Health Information (Also known as Personal or Personally Identifiable Health Information)
Is information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Information system
A computer, storage, networking and other physical devices, infrastructure, and processes to create, process, store, secure and exchange all forms of electronic data.

Infrastructure
The technology (hardware and software) that comprise the computer network, phone network, and connections to the Internet including the computer and storage environments.

Infrastructure-as-a-Service
The capability provided to the state to provision, process, and store networks and other fundamental deployments and run arbitrary software, which can include operating systems and applications. The state does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components, for example, host firewalls.

Internet of Things (IoT)
The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to connect and exchange data.

IP Address
The address of a connected device on the State's IP network. Every desktop and laptop computer, server, scanner, printer, modem, router, smartphone, and tablet is assigned an IP address.

Load Balancing
Dividing the amount of work that a computer has to do between two or more computers so that more work gets done in the same amount of time and, in general, all users get served faster.

MAC Address
A 12-digit hexadecimal address that is preprogrammed into a computer's network adapter that uniquely identifies that computer on the network.

Malicious Phishing
Email messages disguised to entice the user to enter personal information, network, or banking account information. This information will be sent to the attacker who will use it to steal the user’s identity, money, or to access the state network using the user’s network log-in information to steal data. State Facilitated Phishing is internal phishing of employees to test and evaluate our education and training efforts.

Malicious Software
A program that gives a hacker control of your computer.

Malware
A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim.

Metadata
Data that describes other data. For example, the date modified field in a listing of files is metadata.

Mobile Applications
Applications running on a mobile device like a smart phone or tablet.

Mobile Device
A portable, wireless computing device that is small enough to be used while held in the hand.

Mobile Wi-Fi
A wireless router that acts as a mobile wireless network outbound spot.
NATURAL
A programming language created by Software AG used to interface with ADABAS (Adaptable Data Base System).

Network
A group of computer systems and hardware devices linked together to facilitate the communication between the devices, the sharing of resources, and that make the exchange of information easier.

Non-Public Data
Data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, ordinance, or administrative rule from access by the general public as public information.

On Premise
The IT infrastructure, applications or data that is located at State facilities. Cloud services, SaaS, PaaS, and IaaS would not be considered to be on premise.

Open Source
Software where the copyright holder allows anyone to study, change and distribute the software to anyone for any purpose without paying a licensing fee.

Operating System
A program that controls the operation of a computer and directs the processing of other programs.

Outbound Traffic
This is traffic that originates inside an enterprise network and has a destination outside of the network.

Payment Card Industry (PCI)
Credit card security specifications created by the credit card industry.

Peripherals
Devices that are utilized to enter data and information into a workstation or retrieve data and information from a workstation.

Personally Identifiable Information (PII)
Data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers, for example, Social Security, driver’s license, and passport numbers. PII also includes financial account information, including account number, credit or debit card numbers, or protected health information (PHI) relating to a person.

Platform
The type of computer system the network is running on. The state has three; the Windows based platform, the mainframe system, and the AS 400 system.

Platform-as-a-Service (PaaS)
The capability provided to the state to deploy onto the cloud infrastructure state-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The state does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Portable Device
Any computing device that can easily be carried that is designed to be held and used in the hands. Portable devices include laptops, tablets, and smartphones. A portable device may also be called a handheld device or mobile device. See also Remote Access Device (RAD).

Portable storage device
A computer media storage device that is capable of being physically transported, including but not limited to USB/flash drives/thumb drives, external hard drives, tapes, CDs, DVDs, and cameras.

Power over Ethernet (POE) switches
A network switch that has Power over Ethernet injection built in.

Presentation Layers
The layer that translates between multiple data formats used by computers that are trying to communicate. The internal communication functions of a computer system are conceptualized by being partitioned into layers, each layer having different functions.

Processor
The actual circuit that processes the instructions that drive a computer.

Production Environment
The setting where applications are run using actual client data as opposed to test environment which is the setting where applications are run using test data.

Program
A sequence of instructions that can be interpreted and executed by a computer.

Protected Data
Data protected by any law, regulation, or industry standard.

Protected Health Information (PHI)
Individually identifiable health information that is:
- Transmitted by electronic media.
- Maintained in electronic media.
- Transmitted or maintained in any other form or medium.

PHI excludes individually identifiable health information in:
• Education records covered by the Family Educational Rights and Privacy Act
• Employment records held by a covered entity in its role as employer.

PHI includes but is not limited to the patient’s name, address, patient’s doctor, patient’s clinic, diagnosis, and prescribed medication.

Reaccreditation
The periodic rescanning of a system looking for security vulnerabilities.

Relative Pathing
A location that is relative to the current directory or folder. By making pathing relative rather than hard coded in an application is less likely to “break” the application because it is looking for a location that has been changed.

Remote Access Device (RAD)
RADs include smartphones like iPhones, Windows, and Android phones; mobile computing devices like iPads, iPads, and notebooks; as well as other non-state workstations such as public access terminals located in libraries, schools and airports or any other internet capable computing device that is mobile or outside the management of BIT. This list is not inclusive.

Resource Access Control Facility (RACF)
An IBM software product. It is a security system that provides access control and auditing functionality for the z/OS and z/VM operating systems.

Rouge Access Point
A wireless access point (WAP) that has been installed on a secure network without authorization.

Router
A networking device that forwards data packets between computer networks.

Sanitization
A process by which data is irreversibly removed from media or the media is permanently destroyed.

Script
A list of commands used by a program to automate processes on a computer.

Security Activity
Activity meant to enhance and maintain a high level of security. This includes scanning network and email communications with sources and destinations that are outside of the state network. It also includes installing upgraded security software and hardware including: anti-virus software, firewalls, content-filtering software, and intrusion detection software.

Security Incident
A violation of any BIT security policies, privacy policies, or contract agreements involving sensitive information, or the imminent threat of a violation.

Security Infrastructure Team (SIT)
The BIT SIT shall, in coordination with the CISO, recommend technology solutions, written policies and procedures necessary for assuring the security and integrity of State information technology.

Security Operations Team (SOT)
The BIT SOT meets daily to review any cyber security findings or issues with the State Infrastructure within the previous day.

Server
A computer that contains a program that awaits and fulfills requests from other programs in the same or other computers. A given application in a computer may function as a source of requests for services from other programs and also as a server of requests from to other programs.

Service Level Agreement
A written agreement between both the State and the Vendor that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed, and (6) any remedies for performance failures.

SIM card
A smart card that stores a subscriber’s personal identifier, billing information, and data.

Software-as-a-Service (SaaS)
Refers to the capability provided to the State to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The State does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Software Development Life Cycle (SDLC)
A software development methodology used by BIT.

State
Refers to the government of the State of South Dakota when capitalized.

State Contact
The person or persons designated in writing by the State to receive general project communications, adverse event notifications, security incident notifications, or breach notifications.

State Data
Means all data created or in any way originating with the State, and all data that is the output of computer processing
of or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State's hardware, the Vendor's hardware or exists in any system owned, maintained, or otherwise controlled by the State or by the Vendor.

State Proprietary Information
The state data plus any other record, information, or document, in any format, that originated with the state.

Statement of Work
A written statement in a solicitation document or contract that describes the State’s service requirements.

Structure Query Language
A computer language that is used to manage data, where the data is presented as a set of related tables, and to make queries of a database.

Social engineering
Manipulating individuals to provide confidential information or access to a secured site. Purposely “conning” individuals for the purpose of obtaining information to allow for nefarious cyber activities. The tendency of our culture in SD is to be helpful and thus makes us very vulnerable to being socially engineered.

Software patches
Changes made to applications to fix security vulnerabilities or impaired functionality.

Spoofing
Refers to various practices that conceal the identity of a user account, an email account, or a computer’s Internet Protocol (IP) address that is taking some action. For example, email spoofing involves forging the header of an email message so that the message appears to come from someone other than the true sender.

System
A set of interrelating or interdependent component parts forming framework, either software or hardware, connected together to facilitate the flow of data or information.

Test Environment
The setting where applications are run using test data as opposed to production environment which is the setting were applications are run using actual client data.

Time Bomb
A program that will stop functioning once a set time is reached.

Trojan Horse
A malicious program that gives a hacker access to a computer system were the program is disguised as something safe but hides a malicious program.

User Identification (UID)
A user, identifier, or account utilized for access control to specify which technical assets and resources an individual or entity can access. Examples are:
  • USERID
  • A User ID
  • SD Domain Account

Virtual Private Network (VPN)
A method to encrypt data that is sent or received over the public Internet.

Virtualization
The creation of a virtual version of something, such as an operating system, a server, a storage device, or network resources. By allowing multiple virtual versions of something on the same physical server more efficient use is made of network resources.

Web Probing
An intelligence gathering effort to gather background information and to identify configuration files and directories of servers providing web content.

Web Server
A computer that acts as a server that serves up Web pages and applications.

Web Server attacks
Attacks against the servers that connect the state network to the Internet as well as servers that host (store and run) websites. These attacks can be to access data that is not meant to be accessible through the websites via direct probes and software injections from malicious hosts. They can also be meant to prevent users from accessing the websites or the servers. Incidents is the number of successful compromises and Hack Scans are the number of infiltration attempts.

Wi-Fi
The 802.11b standard for wireless networking. A standard for delivering digital information over high-frequency, wireless local area networks.

Wireless Access Point (WAP)
A networking hardware device that allows a Wi-Fi device to connect to a wired network.

Wiring closet
A small room commonly found in institutional buildings where electrical connections are made.

Workstations
Any State-owned desktop, laptop, or tablet computer.

Worm
A malicious program that reproduces itself, so it can spread from one computer to others.
<table>
<thead>
<tr>
<th>ACRONYMS</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>ADABAS</td>
<td>Adaptable Data Base System</td>
</tr>
<tr>
<td>BA</td>
<td>Business Associate</td>
</tr>
<tr>
<td>BAA</td>
<td>Business Associate Agreement</td>
</tr>
<tr>
<td>BHR</td>
<td>South Dakota Bureau of Human Resources</td>
</tr>
<tr>
<td>BIT</td>
<td>Bureau of Information &amp; Telecommunications</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial off the Shelf Software</td>
</tr>
<tr>
<td>DBMS</td>
<td>Database Management System</td>
</tr>
<tr>
<td>DDN</td>
<td>Digital Dakota Network</td>
</tr>
<tr>
<td>DDOS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DMZ</td>
<td>De-Militarized Zone</td>
</tr>
<tr>
<td>DNS</td>
<td>Dynamic Naming System</td>
</tr>
<tr>
<td>DOH</td>
<td>South Dakota Department of Health</td>
</tr>
<tr>
<td>DSN</td>
<td>Data Source Name</td>
</tr>
<tr>
<td>DSS</td>
<td>South Dakota Department of Social Services</td>
</tr>
<tr>
<td>EAR</td>
<td>Export Administration Regulations</td>
</tr>
<tr>
<td>FERPA</td>
<td>Family Educational Rights and Privacy Act</td>
</tr>
<tr>
<td>FPLS</td>
<td>Federal Parent Locator System</td>
</tr>
<tr>
<td>FTI</td>
<td>Federal Tax Information</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GLBA</td>
<td>Gramm-Leach Bliley/ Financial Services Modernization Act</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Information Portability and Accountability Act</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol version 6</td>
</tr>
<tr>
<td>IRS</td>
<td>Internal Revenue Service</td>
</tr>
<tr>
<td>ITAR</td>
<td>International Traffic in Arms Regulations</td>
</tr>
<tr>
<td>MANET</td>
<td>Mobile Ad Hoc Network</td>
</tr>
<tr>
<td>MIFI</td>
<td>Mobile Wi-Fi</td>
</tr>
<tr>
<td>MMIS</td>
<td>Medicaid Management Information System</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform-as-a-Service</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>RAD</td>
<td>Remote Access Device</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software-as-a-Service</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Center</td>
</tr>
<tr>
<td>SOT</td>
<td>Security Operations Team</td>
</tr>
<tr>
<td>SOW</td>
<td>Statement of Work</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SQL</td>
<td>Structure Query Language</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access-Control System Plus</td>
</tr>
<tr>
<td>UAT</td>
<td>User Assurance Testing</td>
</tr>
<tr>
<td>UID</td>
<td>User Identification</td>
</tr>
<tr>
<td>VOIP</td>
<td>Voice Over Internet Protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WANET</td>
<td>Wireless Ad Hoc Network</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Access Point</td>
</tr>
</tbody>
</table>