OFFICE OF PROCUREMENT MANAGEMENT
523 EAST CAPITOL AVENUE
PIERRE, SOUTH DAKOTA 57501-3182

SD Medicaid NCCI/MUE Edits

PROPOSALS ARE DUE NO LATER THAN JULY 26, 2016, 5:00 pm CDT

RFP #687

BUYER: Division of Medical Services

POC: Mark Close
Mark.Close@state.sd.us

READ CAREFULLY

FIRM NAME: _____ AUTHORIZED SIGNATURE: _____

ADDRESS: _____ TYPE OR PRINT NAME: _____

CITY/STATE: _____ TELEPHONE NO: _____

ZIP (9 DIGIT): _____ FAX NO: _____

FEDERAL TAX ID#: _____ E-MAIL: _____

PRIMARY CONTACT INFORMATION

CONTACT NAME: _____ TELEPHONE NO: _____

FAX NO: _____ E-MAIL: _____

1.0 GENERAL INFORMATION

1.1 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

This is a request for proposals (RFP) from entities interested in providing to the State of South Dakota, Division of Medical Services, the necessary service, interfaces, and support to perform the national correct coding initiative (NCCI) and medically unlikely (MUE) claims edits authorized by the Centers for Medicare and Medicaid Services (CMS) and required by section 6507 of the Patient Protection and Affordable Care Act (P.L. 111-152).

The Department of Social Services (DSS) is dedicated to effectively managing the State Medicaid program and realizing the Department's vision of strong families being the core of South Dakota's future. Effective management of the Medicaid program requires timely, accurate and secure processing of Medicaid claims. Maintaining and adhering to the confidentiality and security of Medicaid claims data is of the utmost importance to DSS and the Bureau of Information and Telecommunications (BIT) who manage, maintain and monitor adherence to security standards required by the Federal Government, the State and State contracted entities.

The Centers for Medicare and Medicaid Services (CMS) developed the National Correct Coding Initiative (NCCI) to create, promote and release to all states, a set of national correct coding methodologies. The Division of Medical Services currently utilizes SaaS contract services to comply with the CMS NCCI edits methodologies and related requirements. The purpose of this request is to maintain the current SaaS model of NCCI and MUE edit processing, provide business process improvements and incorporate scalability for future identification of additional edits at the discretion of the State, or as mandated by CMS or Administrative Rule. It is intended that a nightly file will be transferred to the Offeror, edits performed, and information returned that same night. Edit detail should be available to DSS staff that is not tied to existing DSS systems or MMIS. Each Offeror will provide their individual solution to the availability of edit detail.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Division of Medical Services (DMS) 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 #687**. Refer to this number on all proposals, correspondence, and documentation relating to the RFP.

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

1.3 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	06/20/2016
Deadline for Submission of Written Inquiries	06/30/2016
Responses to Offeror Questions	07/07/2016
Proposal Submission	07/26/2016 5:00 pm CDT
Oral Presentations/discussions (if required)	To be announced, if needed
Anticipated Awared Decision/Contract Negotiation	08/09/2016

1.4 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, six (6) identical copies, and one (1) digital, Portable Document Format (PDF) copy loaded on a USB flashdrive of the proposal, cost proposal, and all attachments shall be submitted**.**

All proposals must be signed 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 #687 Proposal Due July 26, 2016
South Dakota Department of Social Services
Attention: Mark Close
700 Governors Drive
Pierre SD 57501-2291

No punctuation is used in the address. The above address as displayed should 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.

1.5 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 shall attach an explanation to their offer.

1.6 NON-DISCRIMINATION STATEMENT

The State of South Dakota requires that all contractors, Offerors, 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.

1.7 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.

1.8 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after 06/30/2016. Email inquiries must be sent to *Mark.Close@state.sd.us* with the following wording, exactly as written, in the subject line: **RFP #687 Questions**.

The Department of Social Services will respond to offerors inquiries by posting the offeror aggregated questions and Department responses on the DSS RFP website at http://dss.sd.gov/keyresources/rfp.aspx no later than 07/07/2016. 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.

1.9 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.

1.10 LENGTH OF CONTRACT

The Offeror contract resulting from this RFP will be issued for a period of one (1) year, August, 2016 through May 31, 2017 with the option of yearly contract renewal thereafter, until terminated by either party in compliance with contract terms.

1.11 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.

1.12 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 A. As part of the negotiation process, the contract terms listed in Attachment A may be altered or deleted. The Offer must indicate in their response any issues or concerns they have with specific contract terms in Attachment A. If the Offer's response does not indicate any issues or concerns with any contract terms, the State will assume those terms are acceptable to the Offeror.

3.0 SCOPE OF WORK

In State Fiscal Year 2015, South Dakota's Medicaid program insured 146,736 individuals and maintained an average monthly enrollment of 117,346 recipients. The State's Medicaid Management Information System (MMIS) processed more than 5.2 million claims. The State is currently evaluating the possibility of expanding the Medicaid population to cover adults up to 138% FPL. If Medicaid Expansion is approved, the Division of Medical Services is expecting this expanded population to increase current eligibility by approximately forty percent (40%).

Offeror proposals must provide a response and supporting documentation, when applicable, to address and support the Offeror's approach and capability of, meeting each of the following requirements:

3.1 By submission of response, Offeror understands and agrees to fully comply with and meet, the State's BIT Security Standards and CMS confidentiality requirements.

- **3.1.1** The Offeror must review and acknowledge that the Security Acknowledgement Form (Attachment B) must be signed at contract signature.
- **3.1.2** The Offeror shall also be required to answer, sign and submit the Security Vendor Questions (Attachment C). These questions may be used in the proposal evaluation.
- **3.1.3** All software and cloud services purchased by the state will be subjected to non-production security scans by the State Bureau of Information and Telecommunications, without exception.

3.2 The proposed service Offeror shall be capable of receiving daily claims files via sFTP and process those claims through the necessary NCCI and MUE edits. The claim files will be returned the same evening with edits notated.

- **3.2.1** The proposed solution must demonstrate ability to intake and process UB 04 and CMS 1500 claim types. Individual lines on a CMS 1500 form are considered an individual claim within the South Dakota MMIS.
- **3.2.2** The proposed solution must be scalable to incur additional volume of daily claims for processing upon determination of the State to expand the current Medicaid population.
- **3.2.3** Offeror service shall be capable of receiving historical claims data to validate each claim line or revenue line level for NCCI and MUE edits.
- **3.2.4** The service shall be capable of processing claim edits for both NCCI and MUE edits on a 'per claim line' basis, with the appropriate explanations.
- **3.2.5** The service resulting file shall be capable of transmission via sFTP back to DMS for internal receipt and reading of each claim line, to MMIS in desired format within the same evening.
- **3.2.6** Offeror service shall demonstrate ability to exclude historical claims in the activity file transmissions back to DMS.
- **3.2.7** Offeror service shall demonstrate and ability to receive adjusted and voided claims data to update historical claims information.
- **3.2.8** The Offeror shall demonstrate the ability to accept and store acknowledgement files from MMIS to be referenced upon demand by DMS users for auditing, tracking and reporting purposes.
- **3.2.9** Solution shall provide ability to store and maintain multiple years' worth of the State's edits data and related cost savings information.
- **3.2.10** The Offeror shall support the State's CMS reporting requirement by offering the State a quarterly savings report. A demonstration of this report should be included with the response.

3.3 The Offeror service shall demonstrate ability to expedite timeline to full production implementation by solution's ability to mirror current State contracted services, utilizing SaaS, sFTP and online access points, as identified by the State no later than December 1, 2016.

3.3.1 The response should provide ability for the State to review technical overview documentation and samples of the means, by which Offeror's solution shall successfully intake, apply and report upon NCCI and MUE edits, explanations, cost savings results, and related results of those processes.

3.3.2 Proposed services which require customizations, are of a proprietary nature, or that are not currently in a production environment must fully detail how the benefits realized by the State, outweigh the time to production implementation, with specific regards to:

- Implementation Timelines,
- Costs to Implement,
- Business Process Improvements, and
- Continued Maintenance Cost over solutions which are currently available in production environments.

3.4 The State is expecting a coordinated effort with BIT staff to incorporate general claim header level edits prior to creating the daily claims adjudication files for transmission to the Offeror via sFTP. Offeror understands upon implementation of these edits, testing and validation may be required.

3.4.1 Offeror solution shall be able to demonstrate checks to verify that header level edits have been applied successfully to adjudicated claims files.

3.4.2 The proposed solution shall describe current processes or previously utilized processes by which coordination of testing efforts can be implemented prior to service implementation.

3.5 The Offeror shall schedule and facilitate quarterly discussions with DMS staff on statistical review of edits and cost savings. This quarterly review shall be expected to be held on-site at least once a year. It is expected that other discussions will be scheduled and facilitated by the Offeror remotely.

3.6 Offeror solution shall be capable of providing DSS user's access to related NCCI and MUE edits data. Offeror platforms must be in full compliance with South Dakota BIT standards.

3.6.1 The Offeror should address the number of users able to access the information at one time. South Dakota prefers individual access for users.

3.6.2 The proposed service shall provide DSS users with the ability to view related results data.

4.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

4.1 The offeror is cautioned that it is the offeror'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 offeror's failure to submit such information may cause an adverse impact on the evaluation of the proposal.

4.2 **Offeror's Contacts**: Offerors 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. Offerors 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. Offerors and their agents who have questions regarding this matter should contact the buyer of record.

4.3 The offeror may be required to submit a copy of their most recent independently audited financial statements.

4.4 The selected offeror will be required to provide a copy of its most recent Statement on Standards for Attestation Engagements (SSAE) 16 report, then annually thereafter for the term of the agreement. For

SSAE 16 the offeror must identify which of the following can be provided on an annual basis: SOC 1, SOC 2, or SOC 3. If unable to provide a copy of the most recent report, offeror must explain why and whether in the future the selected offeror will be able to provide a report.

4.5 Provide the following information related to at least three previous and current service/contracts performed by the offeror'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.

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

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

4.8 The offeror must describe their proposed project management techniques.

4.9 If an offeror's proposal is not accepted by the State, the proposal will not be reviewed/evaluated.

4.10 Submit examples of prior projects to demonstrate past performance, including price and cost data from previous projects, to support quality of work, ability to meet schedules, cost control and contract administration.

4.11 Describe your ability and proven history in handling special project constraints.

5.0 PROPOSAL RESPONSE FORMAT

5.1 An electronic submission by email shall be submitted.

5.1.1 The proposal should be page numbered and should have an index and/or a table of contents referencing the appropriate page number.

5.2 All proposals must be organized and labeled for the following headings:

5.2.1 **RFP Form**. The State's Request for Proposal form completed and signed.

5.2.2 **Executive Summary.** The one or two page executive summary is to briefly describe the offeror's proposal. This summary should highlight the major features of the proposal. It must indicate any requirements that cannot be met by the offeror. The reader should be able to determine the essence of the proposal by reading the executive summary. Proprietary information requests should be identified in this section.

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

5.2.3.1 A complete narrative of the offeror's assessment of the work to be performed, the offeror's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the offeror's understanding of the desired overall performance expectations.

5.2.3.2 A specific point-by-point response, in the order listed, to each requirement in the RFP as detailed in Sections 3 and 4. The response should identify each requirement being addressed as enumerated in the RFP.

5.2.3.3 A clear description of any options or alternatives proposed.

5.2.4 **Cost Proposal.** Cost will be evaluated independently from the technical proposal. Offerors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.

See section 7.0 for more information related to the cost proposal.

6.0 PROPOSAL EVALUATION AND AWARD PROCESS

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

6.1.1 Specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements;

6.1.2 Cost proposals to include two parts:
6.1.2.1 Administrative costs
6.1.2.2 Maintenance costs

6.1.3 Resources available to perform the work, including any specialized services, within the specified time limits for the project;

6.1.4 Record of past performance, including price and cost data from previous projects, quality of work, ability to meet schedules, cost control, and contract administration;

6.1.5 Proposed project management techniques;

6.1.6 Ability and proven history in handling special project constraints;

6.1.7 Availability to the project locale;

6.1.8 Familiarity with the project locale.

6.2 Experience and reliability of the offeror's organization are considered subjectively in the evaluation process. Therefore, the offeror 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.

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

6.4 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.

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

6.5.1 If the agency and the highest ranked offeror 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.

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

7.0 COST PROPOSAL

When submitting cost proposals, if there are multiple options, prepare a cost proposal for each option and the services covered. Provide costs for all services provided, training, and one-time set-up costs.

The cost proposal should consider these cost options at both the current State Medicaid eligibility population and secondarily for costs due to expanded eligibility, as numbered below. It is the expectation of the State that associated per member costs would be decreased in relation to the increased volume of claims processing.

1. Costs based upon current Medicaid eligible population
2. Costs based upon the additional Medicaid population with expansion

The cost proposal shall cover an initial contract period of one year with the option of yearly contract renewals. The proposal shall cover all fixed costs, to include maintenance and operations.

Current Medicaid Eligibility Population Cost Proposal				
Category	**Year 1**	**Year 2**	**Year 3**	**Comments**
Implementation Costs				
Maintenance and Support Costs -				
Designate Software License Fees Separately				
Operational Costs -				
List out base and per transaction Tiered Pricing Costs				
Training Costs				
Other				

Expanded Medicaid Eligibility Population Cost Proposal				
Category	**Year 1**	**Year 2**	**Year 3**	**Comments**
Maintenance and Support Costs - *Designate Software License Fees Seperately*				
Operational Costs - *List out base and per transaction Tiered Pricing Costs*				
Other				

Attachment A

STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES
DIVISION OF MEDICAL SERVICES

Consultant Contract
For Consultant Services
Between

State of South Dakota
Department of Social Services
Division of Medical Services
700 Governors Drive
Pierre, SD 57501-2291

Referred to as Consultant | Referred to as State

The State hereby enters into a contract 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 *[contract start date]* and shall end on May 3, 2017, unless sooner terminated pursuant to the terms hereof.

   B. Agreement is the result of Request for Proposal #687.

3. PROVISIONS:
   A. The Purpose of this Consultant contract:
      1.

      2. This agreement involves Protected Health Information. Exhibit A, Business Associate Agreement, is attached and is fully incorporated herein as part of the agreement.

      3. The consultant 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)
         .

   D. The TOTAL CONTRACT AMOUNT will not exceed **$_____.**

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 45 days of the contract end date to receive payment for completed services. If a final bill cannot be submitted in 45 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: , Byrd Anti Lobbing 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, 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, Americans with Disabilities Act of 1990, 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.

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 over payment of this contract 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, State Data, End User Data, Personal Health Information, and all information contained therein provided to the State by the Consultant in connection with its performance of service under this Contract 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 Contract 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 none the less 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 contract, unless otherwise agreed in a writing signed by both parties.

10. TERMINATION:
This Agreement may be terminated by the State upon thirty (30) days written notice. This agreement may be terminated by the Vendor for cause with the cause explained by the Vendor in writing and upon one hundred and eighty (180) days written notice. The Vendor is obligated to give the State one hundred and eighty (180) days written notice in the event the Vendor intends not to renew the contract or intends to raise any fees or costs associated with the Vendor's products or services in a subsequent contract unless such fees or costs have previously been negotiated and included in this contract. In the event the Vendor breaches any of the terms or conditions hereof, this Agreement may be terminated by the State at any time with or without notice. Upon notice of termination of a contract or upon reaching the end of the term of this contract unless the contract is renewed, the State of South Dakota requires that State applications that store information to repositories not hosted on the State's infrastructure require the vendor before termination (whether initiated by the State or the Vendor) to extract the State's information such that the State is able to be load the information onto\into repositories listed in the State's Standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's Standard repositories the information (metadata (data structure descriptions) and data) will be extracted into a text file format and returned to the State. Upon the effective date of the termination of the agreement the State of South Dakota again requires that State applications that store information to repositories not hosted on the State's infrastructure require the vendor before termination (whether initiated by the State or the Vendor) to extract the State's information such that the state is able to load the information onto or into repositories listed in the State's Standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's Standard repositories the information (metadata (data structure descriptions) and data) will be extracted into a text file format and returned to the State. If termination for such a default is effected by the State, any payments due to Vendor at the time of termination may be adjusted to cover any additional costs to the State because of Vendor's default. Upon termination the State may take over the work and may award another party an agreement to complete the work under this Agreement. In the event of termination or at the end of the term of this contract unless the contract is renewed, the Vendor shall deliver to the State all reports, plans, specifications, technical data, and all other information completed prior to the date of termination. If after the State terminates for a default by Vendor it is determined that Vendor was not at fault, then the Vendor shall be paid for eligible services rendered and expenses incurred up to the date of termination. The terms of this provision were arrived at after negotiation between the parties. This provision is the joint product or work of the parties, and not a provision written or demanded by any one party to this agreement. The Vendor recognizes and agrees, however, that the State of South Dakota cannot enter into an agreement providing for hosting of any of its data on the Vendor's servers and networks without provisions protecting its ability to access and recover its data in a usable, non-proprietary format in the event of termination of this contract with sufficient time to convert that data and the business functions provided by the Vendor to another system and vendor.

11. FUNDING:
This Contract 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 Contract 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. AMENDMENTS:
This Contract may not be assigned without the express prior written consent of the State. This Contract 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 Contract 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 Contract are superseded by the terms of this Contract, and except as specifically provided herein, this Contract constitutes the entire agreement with respect to the subject matter hereof.

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

16. SEVERABILITY:
In the event that any provision of this Contract 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 contract, which shall remain in full force and effect.

17. NOTICE:
Any notice or other communication required under this Contract 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 contract 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 Contract, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Contract. 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. 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.

20. INSURANCE:
Before beginning work under this Contract, Consultant shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Contract. The Consultant, at all times during the term of this Contract, 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 Contract 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 Contract. 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.)

21. 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 Contract 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.

22. CONFLICT OF INTEREST:
Consultant agrees to establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal 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.

23. REPORTING PROVISION:
Consultant agrees to report to the State any event encountered in the course of performance of this Contract 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.

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 contract; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this contract; (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 contract 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 contract except as required by applicable law or as necessary to carry out the terms of the contract or to enforce that party's rights under this contract. 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 contract 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. 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-part 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 that 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.

26. CHANGE MANAGEMENT PROCESS
From time to time it may be necessary or desirable for either the State or the Consultant to propose changes to the Services provided. Such changes shall be effective only if they are in writing and contain the dated signatures of authorized representatives of both parties. Unless otherwise indicated, a change or amendment shall be effective on the date it is signed by both parties. Automatic upgrades to any software used by the Consultant to provide any services that simply improve the speed, efficiency, reliability, or availability of existing services and do not alter or add functionality, are not considered "changes to the Services" and such upgrades will be implemented by the Consultant on a schedule no less favorable than that provided by the Consultant to any other customer receiving comparable levels of services.

27. CURING OF BREACH OF AGREEMENT
In the event of a breach of these representations and warranties the State may, at the State's discretion, provide the Consultant with the opportunity to rectify the breach. The Consultant shall immediately, after notice from the State, begin work on curing such breaches. If the notice is telephonic the State will provide, at the Consultant's request, a written notice to reaffirm the telephonic notice. If such problem remains unresolved after three days, at State's discretion, Consultant will send, at Consultant's sole expense, at least one qualified and knowledgeable representative to the State's site where the system is located. This representative will continue to address and work to remedy the deficiency, failure, malfunction, defect, or problem at the site. The rights and remedies provided in this paragraph are in addition to any other rights or remedies provided in this Agreement or by law.

28. 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 will notify the State within two (2) business days of any such threat(s) or exploit(s) and, if the State requests, provide the State with information on the threat(s) or exploit(s).

29. SECURITY INCIDENT AND BREACH NOTIFICATION
A. The Consultant, unless stipulated otherwise, shall notify the State Contact within five (5) business days if the Consultant reasonably believes there has been a security incident.

   If notification of a security incident or data breach to the State Contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within twelve (12) hours after law-enforcement provides permission for the release of information on the security incident or data breach.

B. Notification to the State should include at a minimum all data available including: (i) Name of and contact information for the Consultant's Point of Contact for the security incident or data breach: (ii) date and time of the security incident or data breach; (iii) date and time the security incident or data breach was discovered: (iv) description of the security incident or data breach including the data involved, being as specific as possible; (v) potential number of records known, and if unknown the range of records; (vi) address where the security incident or data breach occurred: and, (vii) the nature of the technologies involved. Notifications must be sent electronically and encrypted via NIST or other applicable federally approved encryption techniques. If there are none use AES-256 encryption with SHA-256 or SHA-2 hashing. Consultant shall use the term "data incident report" in the subject line of the email. If not all of the information is available for the notification within the specified time period Consultant shall provide the State with all of the available information.

30. HANDLING OF DATA BREACHES
The Consultant will implement, maintain and update security incident and data breach procedures that comply with all State standards and Federal requirements. A data breach is the disclosure of, unauthorized access to, or use of, or modification of, or destruction of State data or the interference with system operations in an information system containing State data. The Consultant will also (i) fully investigate the incident, (ii) cooperate fully with the State's investigation of, analysis of, and response to the incident, (iii.) make a best effort to implement necessary remedial measures as soon as it is possible and (iv) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement. The Consultant will use a credit monitoring service, forensics company, advisors, and public relations firm that are acceptable to the State; preserve all evidence including, but not limited to,

communications, documents, and logs; and the State will have the authority to set the scope of the investigation. In addition, the Consultant shall inform the State of actions being taken or will be taken to reduce the risk of further loss to the State.

Except as otherwise required by law, the Consultant shall only provide notice of the incident to the State. The State will determine whether notification to the affected parties will (i) jeopardize the State's interests and (ii) be more appropriate for the Consultant to make. The method and content of the notification of the affected parties must be coordinated with, and is subject to, approval by the State. If the Consultant is required by federal law or regulation to conduct a security incident or data breach investigation, the results of the investigation must be reported to the State. If the Consultant is required by federal law or regulation to notify the affected parties, the State must also be notified.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to the State under law or equity, the Consultant will reimburse the State in full for all costs incurred by the State in investigation and remediation of the data breach including, but not limited, to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract. The Consultant shall also reimburse the State in full for all costs the State incurs in its offering of two (2) years credit monitoring to each person whose data were compromised. 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 data breach.

31. BROWSER
The system, site, and/or application must be compatible with the State's current browser standard which can be found at http://bit.sd.gov/standards/ and Microsoft Edge. No QuickTime, PHP nor Adobe ColdFusion, Adobe Flash or Adobe Animate CC will be used in the system, site, and/or application.

32. SECURITY ACKNOWLEDGEMENT FORM
The Consultant will be required to sign the Security Acknowledgement form which is attached to this Agreement as _____. 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 insuring 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 BIT Information Technology Security Policy (BITSP) attached to this Agreement as _____. Failure to abide by the requirements of the BITSP 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.

33. BACKGROUND CHECKS
The State of South Dakota requires all employee(s) of the Consultant, Subcontractor's, 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 background checks must be performed by the State with support from the State's law enforcement resources. The State will supply the finger print cards and prescribe the procedure to be used to process the finger print cards. Project plans should allow two to four 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, Subcontractor's, Agents, Assigns and or Affiliated Entities from performing work under this Agreement that the State, in its sole discretion, believes 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 its determination.

34. 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.

35. MALICIOUS CODE
    A. The Consultant warrants that the service contains no code that does not support an application requirement.
    B. The Consultant warrants that the service contains no malicious code.
    C. The Consultant warrants that the Consultant will not insert into the service or any media on which the service is delivered any malicious or intentionally destructive code.

36. 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.

37. 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. have no code not required for the functioning of application;
    E. 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;
    F. 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;
    G. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation;
    H. 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);
    I. 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;
    J. access no data outside that which is defined in the "About" information for the Consultant's application.

    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.

38. AUTHORIZED SIGNATURES:
In witness hereto, the parties signify their agreement by affixing their signatures hereto.

Consultant Signature	Date
State - DSS Division Deputy Director Lori Lawson	Date
State - DSS Deputy Secretary Brenda Tidball-Zeltinger	Date
State – DSS Cabinet Secretary Lynne A. Valenti	Date
State – BIT Commissioner David Zolnowsky	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 Fiscal Contact Person _____
Phone _____
Consultant 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.

Exhibit A Business Associate Agreement

State of South Dakota, Department of Social Services

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.

(f) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164 (Subparts A, C, D and E). More specifically, the "Privacy Rule" shall mean the regulations codified at 45 CFR Part 160 and Part 164 (Subparts A and E), and the "Security Rule" shall mean the regulations codified at 45 CFR Part 160 and Part 164 (Subparts A and C).

(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.

Attachment B

south dakota bit bureau of information & telecommunications

Security Acknowledgement

Following is the Employee Agreement that all BIT employees and State contractors must sign; **Employee Agreement to Comply with BIT Information Technology Security Policy (the "Policy").** The State of South Dakota is dedicated to information security and has security specialists in each BIT Division.
However, users are responsible for compliance to all information security policies and procedures. *By signature below, the employee / 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 / contractor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;**
3. **Employee / contractor agrees to follow state and federal regulations in regards to confidentiality and handling of data;**
4. **Employee / contractor has read and agrees to abide by the Policy;**
5. **Employee / contractor consents to discuss with a supervisor / State contact regarding Policy violations;**
6. **Employee / contractor shall abide by the policies described as a condition of continued employment / service;**
7. **Employee / 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 and contracts;**
10. **Employee / contractor shall promptly report violations of security policies to a manager / 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/ ***Information Technology Security Policy – CONTRACTOR:*** http://bit.sd.gov/vendor/default.aspx

ACKNOWLEDGMENT: STATE OF SOUTH DAKOTA INFORMATION TECHNOLOGY SECURITY POLICY

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 form. **State of South Dakota Contract Number:**

Employee / Contractor signature	**Date**	**Manager / State Contact**	**Date**

Employee / Contractor name in block capital letters

Attachment C

Information Technology Security Policy

CONTRACTOR
v 1.0

Last Updated: 04/18/2016

General-Information Technology Security Policy-Introduction 5

1.1.4.1. General 11

1.1.4.2. Chief Information Security Officer 12

1.1.4.3. Policies 12

1.1.4.4. Security Infrastructure Team (SIT) 13

1.1.4.5. Security Operations Team (SOT) 13

1.1.4.6. BIT Executive Working Group on Cyber Security 13

Administrative-I/T Asset Protection-Background Checks 15

10.1.4.1. Background Checks 15

Administrative-I/T Asset Protection-Confidentiality 16

10.3.4.1. Confidentiality Agreement 17

10.3.4.2. Security Acknowledgement and Access 18

Mainframe-Mainframe Security-Overview 18

210.1.4.1. Security of Mainframe Resources 19

210.1.4.2. Mainframe Access Granted by Business Need 19

210.1.4.3. Requesting Mainframe System Access 19

210.1.4.4. Mainframe Resource Examples 19

Mainframe-Mainframe Security-Mainframe Accounts 19

210.3.4.1. Unique Account Requirement 20

210.3.4.2. Requests for Mainframe User IDs 20

210.3.4.3. Responsibility Mainframe User IDs and Passwords 20

210.3.4.4. Department Security Officers 20

Mainframe-Mainframe Security-Disposition of Mainframe Output and Documentation 21

210.20.4.1. Agency Defined Access to Output 21

210.20.4.2. Mainframe Documentation 22

Mainframe-Mainframe Security-Mainframe Access 22

210.25.4.1. Mainframe Access 22

Server-Server Security-Overview 22

220.1.4.1. Scope of Server Platforms 23

Server-Server Security-File Transfer Protocol 23

220.7.4.1. Use of File Transfer Protocol Server 24

Server-Server Security-Assurance HIPAA Regulations are Met 24

220.10.4.1. The Data User is Responsible for Adhering to HIPAA Regulations 25

Server-Server Security-Technical Asset Connections 25

220.11.4.1. Requirements for State Connected Devices 26

220.11.4.2. Exemptions 26

Network-Service-Domain Naming System 26

220.13.4.1. South Dakota Agency Website Naming 27

220.13.4.2. Registering a Domain 27

Data Center General-Data Center Security-Cloud Based Services and System Information 27

230.9.4.1. Responsibility for Cloud Based Services and Systems 28

Data Center General-Data Center Security-Federal Tax Information 28

230.11.4.1. Federal Tax Information Returns and Return Information 29

230.11.4.2. What is Not Federal Tax Information 29

230.11.4.3. Safeguarding Federal Tax Information 30

Data Center General-Technical Asset Connections-Domain 30

230.52.4.1. Protection of External Devices 30

Data Center General-Operational-Change Control Process 31

230.53.4.1. Assessment, Alerts and Procedures 31

230.53.4.2. Weekly Maintenance Schedules 31

Data Center General-Procedural-Physical Access - Proximity Cards 32

230.58.4.1. Proximity Card for Non-BIT Employee Access 32

Data Center General-Accountability-Authorization 33

230.65.4.1. Administrative Capabilities on Servers 33

Data Center General-Data Center Security-Accounts Access Control and Authorization 34

230.67.4.1. Individual Access Authorization 35

230.67.4.2. User Privilege Capabilities 35

230.67.4.3. Least Privilege 35

230.67.4.4. Password Requirements 35

230.67.4.5. Agency Specific Policy DSS and DLR Resets 35

230.67.4.6. Individual Access Termination 36

Development-I/T Asset Management-Access Control and Accountability Application Security 36

400.3.4.1. Security Assessment 37

Network-Service-Access Control 39

610.1.4.1. System Access Expectations 40

610.1.4.2. Contractor Access 41

610.1.4.3. Modems 41
610.1.4.4. Remote Access 41
610.1.4.5. Inspection and Review 42
610.1.4.6. Department of Social Services 42
Network-Concept-Security Domain Zones 42
610.3.4.1. Intranet 43
610.3.4.2. DMZ 43
610.3.4.3. Extranet 43
Network-Concept-Network Integrity 43
610.9.4.1. Responsibilities 44
610.9.4.2. Management 44
610.9.4.3. Disabling Critical Components of Network Security Infrastructure 44
610.9.4.4. Technical Asset or Contractor Connections 44
610.9.4.5. Local Area Network 45
610.9.4.6. Wide Area Network 45
610.9.4.7. Physical Controls 45
Network-Communication-Internet 45
610.11.4.1. Multiple Connections 46
610.11.4.2. Interfaces 46
610.11.4.3. Security 46
610.11.4.4. Responsibilities 46
610.11.4.5. IPv4/IPv6 and Device Names 47
Security-Network Discovery-Probing-Exploiting 47
620.1.4.1. Exploiting Security Controls of Information Systems 48
620.1.4.2. Cracking Application or Passwords 48
620.1.4.3. Limiting Tool Functionality 48
620.1.4.4. Exemptions 48
Security-Content Control-Internet Filtering 49
620.5.4.1. DDN Intranet Content Filtering 49
620.5.4.2. Filter Exemption Requests 50
620.5.4.3. Exemptions 50
620.5.4.4. Appropriate Use of Administrator Access 50
620.5.4.5. DDN Content Filtering 51

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.

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 insure 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 & 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 breaches, suspected and/or attempted security breaches 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 insure 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;
- Agree 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;
- Insuring 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 owners area of responsibility;
- Authorizing individuals 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 Polices 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 clientele.

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 in regards to 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 insure 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 insure 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. Policies

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.

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

1.1.4.4. 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 CSO 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.

1.1.4.5. 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.

- 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.

1.1.4.6. 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

Prior to employment, all prospective State Technology employees and contractors desiring to work for the State shall be screened thoroughly including verification of qualifications.

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

10.1.2. Purpose

Insure that prospective BIT employees and 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. Credit checking and financial history is not subject to this policy.

10.1.3.1. Scope Assumptions

Prospective employees and contractors shall receive official State finger print cards. The fingerprinting can be done from most local law enforcement agencies. The completed cards shall be returned to the BIT CISO and processed by the Division of Criminal Investigation. The costs are borne by BIT if a prospective employee or the agency if a contractor.

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

The State requires all contractors who write code for or modify State owned software, alter hardware, configure software of State-owned technology resources, have access to source code and/or protected-personally identifiable or confidential information or have access to secure areas to have background checks.

These background checks must be fingerprint-based and performed by the State with support from our law enforcement resources. The State 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 - four

weeks. The steps involved include:

- The contractor / employee obtains the fingerprint cards from BIT Executive Assistant to the CISO;
- The Executive Assistant to the CISO will record in a tracking spreadsheet the Contractor Company, Names (if known @ this point), Contractor Address, Contract contact, BIT contact, dates provided, returned, completed & any other pertinent info;
- The manager / project leader / contact will send the fingerprint cards to prospective employee contractor - the *Fingerprint Form Letter* (http://intranet.bit.sd.gov/forms/) is a sample letter if interested in using it;
- The contractor / employee goes to local law enforcement / sheriff / police to get finger printed;
- The contractor / employee sends cards back to project leader / contact;
- The project leader / contact delivers the fingerprint card to the Executive Assistant to the CISO;
- The Executive Assistant to the CISO will update the tracking sheet with the dates received back;
- The Executive Assistant to the CISO will mail the fingerprint card to the DCI contact;
- Everyone waits for the results;
- All results are delivered to the CISO - DCI requests a single point of contact;
- The CISO will deliver the results to the manager requesting the background check if there are issues of concern;
- The manager will interpret the results:
    - Approve;
    - Disapprove hire.
- The manager informs the Executive Assistant to the CISO of the final disposition;

- Fingerprint cards are destroyed;
- Disposition of application is filed.

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-Overview

210.1.1. Overview

This policy covers the mandatory use of the security systems installed on the mainframe to control access to individual mainframe resources by authorized users as defined by data owners.

210.1.2. Purpose

The purpose is to protect mainframe resources from unauthorized access while assuring authorized access is allowed.

210.1.3. Scope

Mainframe security covers all users of the mainframe administered by the BIT.

210.1.3.1. Scope Assumptions

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

210.1.3.2. Scope Constraints

This policy applies to mainframe users only.

210.1.4. Policy

210.1.4.1. Security of Mainframe Resources

BIT is the custodian of the data and other resources stored in and accessed via the mainframe. BIT provides the necessary control facilities to administer mainframe resource protection and access authorization when specified in writing by the authorized resource owner. The owner of data or resource is the agency on record as being responsible for the accuracy and collection of the data or creation and maintenance of the resource. The owner specifies the security settings and authorizations defining how the data and resources are protected and accessed. The responsibility of the owner is to request access rights for authenticated users or groups to specific files or groups of files or other resources. An authenticated user is an authorized individual signed on to the mainframe with a valid mainframe User ID. BIT is responsible for coordinating security, maintaining security standards and

procedures, training of security administrators, auditing of security authorizations, and monitoring of security violations.

210.1.4.2. Mainframe Access Granted by Business Need

Access to mainframe systems and data is granted only when a specific business need is proven, as defined by BIT Client Departments and BIT Security Administration. All mainframe access for department personnel must be requested by department personnel authorized to make such requests.

210.1.4.3. Requesting Mainframe System Access

All mainframe users and those who wish to become mainframe users as well as all mainframe resources must be defined and authorized under at least one mainframe security system or access will not be granted. BIT has installed two mainframe security systems to define and control access to mainframe resources. Contact your supervisor or BIT Point of Contact for instructions in how to request authorization to access or create mainframe resources.

210.1.4.4. Mainframe Resource Examples

Data files, CICS Transactions, journals, programs, transient data destinations, temporary storage queues, system programmer commands, spool output, and started transactions are among the resources that may be protected upon request through RACF. There are other mainframe resources not included in this list that can be protected by RACF as well. Please contact your supervisor or BIT Point of Contact for a complete list of resources that can be protected or for instructions regarding how to request protection for any mainframe resources.

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 Mainframe User IDs 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.

210.3.4.4. Department Security Officers

Each state agency must have a Department Security Officer that is responsible for the mainframe computer resources owned by that agency. These officers are designated by agencies and identified in the Security Contact Database maintained by the BIT Help Desk.

All User ID related requests from an agency must be routed through the Department Security Officer who will subsequently email the request to the BIT Help Desk. In the event that a Department Security Officer is not available to submit a request, any requests must be submitted by an authorized supervisor, manager, director, or higher level management.

Mainframe-Mainframe Security-Disposition of Mainframe Output and Documentation

210.20.1. Overview

This policy covers mainframe documentation output including, but not limited to, operational documentation, development documentation, job requests, and any other user source documents. It also covers the disposition and distribution of all printed output.

210.20.2. Purpose

The purpose of this policy is to protect mainframe resources from unauthorized or inappropriate access by assigning data access protection mechanisms to all written reports and/or documentation.

210.20.3. Scope

This policy applies to anyone who requests or handles mainframe documentation or printed output.

210.20.3.1. Scope Assumptions

This policy applies to printed mainframe documentation or printed output including electronically printed output.

210.20.3.2. Scope Constraints

This policy does not apply to electronic mainframe reports or printed documentation related to applications that reside on Windows, UNIX, or AS/400 platforms.

210.20.4. Policy

210.20.4.1. Agency Defined Access to Output

Mainframe output is distributed in accordance with agency instructions. Agencies with confidential output must consider requesting that all output, including abnormally terminated jobs, job streams or unacceptable output, be delivered directly to the requestor. Such requests must be made through the BIT Help Desk by authorized agency representatives.

210.20.4.2. Mainframe Documentation

Unless properly checked out by authorized agency representatives, user source documents including, but not limited to, source code, batch job instructions, and scheduling information may not be removed from BIT. Authorized agency representatives who wish to check out documents of this nature must present a valid

photo ID and sign for the documents before removing them from BIT. During normal business hours, resources can be checked out in Production Control. After normal business hours, check-out of resources may be conducted at the computer operations door.

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 to 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-Overview

220.1.1. Overview

This policy defines BIT's role regarding enterprise servers.

220.1.2. Purpose

The purpose is to delineate enterprise servers managed and supported by BIT.

220.1.3. Scope

This policy covers enterprise servers BIT managed enterprise servers at the State.

220.1.3.1. Scope Assumptions

This applies to the State's distributed system.

220.1.3.2. Scope Constraints

This only applies to the State's enterprise distributed system. Mainframe, AS/400, desktop, and mobile devices are not covered.

220.1.4. Policy

220.1.4.1. Scope of Server Platforms

BIT will install, administer and maintain enterprise servers within the technology infrastructure of the State. This includes, but is not limited to: enterprise application servers, print servers, attached storage devices and file transfer servers.

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, a 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

Ensure HIPAA regulations covered by title 45 of the Code of Federal Regulations (CFR) Part 160 and Part 164 are met.

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

Server-Server Security-Technical Asset Connections

220.11.1. Overview

All devices connected to any technology infrastructure that is external to the State must be protected. The connections must be designed and implemented to ensure compliance with the access control policies for each connected system.

220.11.2. Purpose

To define requirements for devices authorized to access State computing or network resources that are able to connect to any external technology infrastructure.

220.11.3. Scope

This policy provides a baseline set of expectations for security policies as applied to the State network.

220.11.3.1. Scope Assumptions

This policy applies to devices connected to the State network that can access the Internet.

220.11.3.2. Scope Constraints

This policy does not apply to devices that are not able to connect to the Internet.

220.11.4. Policy

220.11.4.1. Requirements for State Connected Devices

SD Domain technology devices with access to the Internet must utilize the standard operating system and applications defined by BIT and use with standard group policy, IP address configuration, automatic system updates, and anti-virus definitions.

220.11.4.2. Exemptions

Requests for exceptions to the SD Domain policy must be submitted in writing to BIT. Such requests will be reviewed on a case by case basis and will be allowed or denied based on what is determined to be in the best interests of the State's enterprise resources.

Network-Service-Domain Naming System

220.13.1. Overview

Domain names, or internet web addresses (sometimes called URLs) must be consistently named and processed to allow for agency publication of content on the internet. Standards have been defined for the naming of these sites and processes have been defined in order to provide consistency in the management of these sites over time.

220.13.2. Purpose

This policy is intended to govern how internet domain names are named, approved, registered, renewed, transferred, or terminated.

220.13.3. Scope

All internet domain names administered and registered by BIT on behalf of the State's agencies are included within this policy.

220.13.3.1. Scope Assumptions

If an agency has a need for resources to be provided on the internet they must adhere to the registration requirements within this policy. This includes, but is not limited to, the following registrations name types:

- Sd.gov;
- State.sd.us;
- Other specialty names, such as 'www.travelsouthdakota.com.'

220.13.3.2. Scope Constraints

Agencies who have a need for a non-'sd.gov' registered domain and are being provided the name from a contractor or outside entity who registers and administers the name ongoing.

220.13.4. Policy

220.13.4.1. South Dakota Agency Website Naming

To conserve time, money, and administrative expenses, content viewable by the public must reside under the sd.gov domain name. If an agency requires a non sd.gov domain name the agency must contact the BIT Help Desk to request that BIT approve the domain name. If approved, BIT will then register and maintain ownership of the domain name on behalf of the client agency. Regardless of who supports a website the client agency that requested the domain name is responsible for the content located on the website.

220.13.4.2. Registering a Domain

To request a domain name be registered on behalf of an agency, a request to the BIT Help Desk must be submitted. If approved, BIT will verify if the desired domain name is available for registration. If the desired domain name is available, BIT will register the domain on behalf of the state. BIT will contact the requester for approved domain names to gather any information needed to complete a domain name registration.

The State assumes ownership of all domain names, and BIT manages the registration and renewal of all domains for the State. BIT will maintain a domain name longer than a client agency uses it in many cases to assure the state does not become associated with inappropriate content. BIT will

terminate registration of legacy domain names after a period of time, normally 1-2 years after the name is found to be no longer advertised and no longer found within search engines.

A written request to the BIT Help Desk by an authorized agency representative is required to transfer a domain name owned by a third party entity to the State. If the request is approved, BIT will coordinate the transfer on behalf of the state.

BIT will automatically renew all active BIT managed domains.

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

230.9.1. Overview

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.

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. 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.

Return information, in general, is any information collected or generated by the IRS with regard to any person's liability or possible liability under the Internal Revenue Code (IRC). Return information 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

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.

Data Center General-Technical Asset Connections-Domain

230.52.1. Overview

All devices which are authorized to access State computing or network resources that are able to be connected to any technology infrastructure that is external to the State must be protected. The connections when used must be designed and implemented to ensure compliance with the access control policies for each connected system. Non-compliance may result in a disconnection from the DDN of a technical device or a network site. The individual or organization responsible for the non-compliant technical device or network may also receive a service charge.

230.52.2. Purpose

Define the protection requirements for all devices authorized to access state computing or network resources that are able to be connected to any technology infrastructure that is external to the state.

230.52.3. Scope

This policy provides a baseline set of expectations for security policies for all devices authorized to access State computing or network resources which can be connected to any technology infrastructure that is external to the State.

230.52.3.1. Scope Assumptions

The policy applies to devices that can be sequentially connected to state computing or network resources and that of any technology infrastructure external to the State.

230.52.3.2. Scope Constraints

This policy does not apply to devices that can connect to State computing or network resources but cannot connect to technology infrastructures external to the State.

230.52.4. Policy

230.52.4.1. Protection of External Devices

All technology systems such as, but not limited to, workstations or servers connected to the technology infrastructure of the State must be connected to and configured as members of the SD Domain architecture of the State.

Data Center General-Operational-Change Control Process

230.53.1. Overview

This policy describes the change control process that will be used by BIT. It also contains information about the BIT patch implementation process and schedule BIT will follow when conducting scheduled maintenance on computing or network assets.

230.53.2. Purpose

The State's technology infrastructure requires routine and periodic modifications.

230.53.3. Scope

This policy applies to the technology infrastructure of the State maintained by BIT.

230.53.3.1. Scope Assumptions

Routine and periodic modifications include, but are not limited to functionality updates, modifications and reallocation, cleaning, and testing of hardware and software. Maintenance may include any of the afore mentioned tasks. The list is not inclusive.

230.53.3.2. Scope Constraints

This policy does not apply to unsupported hardware or software nor do they apply to non-standard hardware or software.

230.53.4. Policy

230.53.4.1. Assessment, Alerts and Procedures

A change control process will be used to reduce the risk that changes made to an asset will result in a compromise to the confidentiality, the integrity or the availability of technical assets or services. BIT will follow a change management process that ensures changes are communicated, evaluated and tested as appropriate.

This change management process will include the requirement that management approve all non-routine changes prior to implementation.

230.53.4.2. Weekly Maintenance Schedules

BIT has two regular maintenance periods:

- 4:00am to 7:00am, Central Time, every Tuesday is reserved by BIT for maintenance related to platforms other than the mainframe;
- 5:00am to 12:00 noon, Central Time, every second Sunday of each month will be reserved by BIT for maintenance related to the State mainframe. If a holiday is associated with the second weekend of the

month, either on the Friday or the Monday, the downtime of the mainframe is moved to the third Sunday of the month.

Data Center General-Procedural-Physical Access - Proximity Cards

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-Accountability-Authorization

230.65.1. Overview

Administrative access to BIT computing, storage, and networking equipment must be assigned using the principal of least privilege.

230.65.2. Purpose

Access based on separation of duties is a critical component of BIT security posture and must be maintained.

230.65.3. Scope

This policy covers all BIT System Administrators and BIT Network Administrators as well as anyone who wishes to be granted administrative access to BIT hardware and/or software.

230.65.3.1. Scope Assumptions

Privileges will be assigned to individuals only by their immediate supervisor or higher level manager. Security administrators will conduct periodic reviews to verify that only access rights corresponding to an individual's job duties have been assigned.

230.65.3.2. Scope Constraints

This policy does not apply to computing or networking equipment that is not owned or operated by BIT.

230.65.4. Policy

230.65.4.1. Administrative Capabilities on Servers

Only individuals designated as a System or Network Administrator will have administrative capabilities on computing equipment within their specific area of responsibility.

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.

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

230.67.1. Overview

All work stations capable of connecting to the state domain and/or managed by BIT as well as their associated peripheral devices will have security policies established and implemented to restrict unauthorized activities. Authorization for individuals, programs, and related technologies will be enforced for resources accessible through the workstations as well as for information and software installed on or running on the workstations.

Access to resources must be based on individual needs. Individual accounts are created for those with a justifiable access requirement to the DDN Intranet. Access must be terminated when the manager of an employee or contractor determines said access is no longer required or justified.

Only authorized personnel will be allowed to change the passwords and they will need to have credentials to prove who they are.

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

230.67.2. Purpose

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

230.67.3. Scope

This policy incorporates all intranet users of the DDN and is managed by BIT.

230.67.3.1. Scope Assumptions

All devices authorized to the DDN or managed by BIT must be protected. Employees and contractors requesting or requiring individual accounts must be aware of the security policies and expectations applied to them and commit to follow them. Privileges will be assigned to individuals only by their immediate supervisor or higher level manager. Security administrators will conduct periodic reviews to verify that only access rights corresponding to an individual's job duties have been assigned. Managers of employees and contractors must notify BIT via defined processes when those

managers determine access is no long required or justified to accounts and/or DDN computing data or network resources.

230.67.3.2. Scope Constraints

This policy does not apply to devices which are not authorized to the DDN and are not managed by BIT and non-work station computing devices such as mainframes, AS/400s, or mobile devices. The lockout threshold, lockout duration, and reset requirements to not apply to non-DSS or DLR workstations.

230.67.4. Policy

230.67.4.1. Individual Access Authorization

Authorization for individual accounts and access via such individual accounts to the DDN Intranet and its computing, data, and network resources must be based on a documented request from an authorized requestor that identifies resources required for the duties of the job for which the person has been hired, and must be sent to the BIT Help Desk.

The *Employee Request Form (New/Move)* at the BIT Intranet (http://intranet.bit.sd.gov/forms) is used to request access to the technology infrastructure of the State.

All BIT employees and contractors are required to sign the *Security Acknowledgement form* found at BIT intranet http://intranet.bit.sd.gov/forms/, which acknowledges responsibilities pertaining to integrity of data, policies, procedures, and the proper use of resources. All BIT employees and contractors must have a copy signed, and filed.

230.67.4.2. User Privilege Capabilities

All users with access to the DDN will be granted user level access rights for their BIT managed workstation. Individuals who wish to have Administrative privileges on their BIT managed workstation must

contact their agency BIT Point of Contact or the BIT Help Desk. Written business justification must be provided with the request by an agency manager for the request to be considered.

230.67.4.3. Least Privilege

Administrative 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.

230.67.4.4. Password Requirements

- Must be changed every ninety days;
- Must be at least eight characters;
- Must 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 six most recent passwords;
- Must not have been changed within the last seven days;
- Does not contain your account or full name that exceeds two consecutive characters.

230.67.4.5. Agency Specific Policy DSS and DLR Resets

A security setting determines the number of minutes that must elapse after the threshold of failed logon attempts has been reached before the counter is reset to zero. The failed logon attempt counter shall be reset after fifteen minutes.

230.67.4.6. Individual Access Termination

Access privileges must be terminated immediately when authorization ceases for a user as identified by the manager of the individual.

When an employee or contractor transfers, resigns or employment is terminated, the manager is responsible for completing the *Departing Employee Request form* to be found at BIT intranet http://intranet.bit.sd.gov/forms/, and submitting the document to the BIT Help Desk prior to the last day of employment for the individual.

For situations involving immediate termination, the BIT Help Desk must be notified immediately 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.

Development-I/T Asset Management-Access Control and Accountability Application Security

400.3.1. Overview

To prevent unauthorized use, modification, disclosure, destruction or denial of access to assets of the State, applications developed by BIT and any Third party must be sufficiently protected and monitored to ensure consistency with BIT Information Technology Security policies.

400.3.2. Purpose

To ensure compliance with BIT defined security standards, no hosted application or website may be moved into production without receiving a security assessment. Security assessments will be performed as part of the provisioning process.

400.3.3. Scope

This policy includes any software applications developed by BIT or by a Third party contractor.

400.3.3.1. Scope Assumptions

This policy assumes that the application or website is capable of being security scanned, as long as the application hosts any type of state government data. The security assessment will include active penetration testing and analysis of an application from a security perspective based upon, but not limited to, the latest Top 10 categories of the OWASP and NIST (National Institute of Standards and Technology) standards.

400.3.3.2. Scope Constraints

Constraints on this policy include mainframe applications and desktop applications. Desktop applications themselves are scanned only for connections to an unauthorized location or if it opens up dangerous ports.

400.3.4. Policy

400.3.4.1. Security Assessment

Configurations and installation parameters on all State applications must comply with BIT security management policies and standards.

No BIT developed software or 3rd party applications or websites (regardless whether hosted internally or externally) may not be moved into production without a security assessment. The following security assessment standards regarding security assessment processes, responsibilities and procedures ensure compliance with this requirement:

- It is the responsibility of the application owner, website owner or the party requesting that the application or website be moved into production, to verify that a security assessment is performed;
    - The security assessment process is initiated by sending a request to provision a production environment, to the BIT Help Desk.
- Prior to any hosted application or website being moved into production, written verification from the BIT Security team (BIT.ENTNETWORKSEC@state.sd.us) must exist, verifying that the application or

website has passed a security assessment:

- The security assessment will be performed as part of the provisioning process;
- All information regarding security assessments and official records of such will be recorded in the Pegasus system;
- All reports are emailed back to the application owner. It is the owner's responsibility that any part of the application that has failed, be remediated and that the appropriate documentation is sent back to the security team with the remediation documented.
- The application or website will not be moved into production until the entire security assessment has been passed.

- If an application has significant changes, a scan will need to be re-initiated:
  - Significant changes include:
    - .Net Version upgrades;
    - Database upgrades;
    - Changes outside of the application.
    - IIS upgrade;
    - Server moves.

Upon receipt of the request to provision a production environment, the following tasks are delegated to appropriate members of the BIT SIT by the BIT Help Desk. Each Security Assessment task is required to be closed individually, with comment(s) in the close information and to include any documentation referenced:

Security Assessment Task Responsibility List -	
Development	Security Testing
	Load & Performance Testing
	Desktop Compatibility Confirmation
	Documentation & Deployment Diagrams
	DP01 & APM Updates
TAWeb	Creates Production Environment
	Server Compatibility Confirmation
	PCI Testing
Network	Security Testing

Subsequent updates to the application or website obtain written verification, through the same security assessment requirements validation processes, as defined above, by the BIT SIT. This written verification will validate that any subsequent application or website updates have passed a security assessment prior to any updates being moved into the production environment.

The process is also initiated by sending a request to provision a production environment to the BIT Help Desk.

Failure to provide such verification may result in the application or website not being placed in production until the security assessment passes and received certification of completion. The application or website will remain unavailable until which time the security assessment certification and testing has been

completed and verified in writing, as required. A detailed report that includes remediation requirements is sent to the appropriate parties responsible for the application. This process will repeat itself as many times as needed until the application is deemed secured.

BIT Assessment Team

BIT will form an annual assessment team comprised of BIT individuals who have been identified as having the knowledge and skills to properly assess the requirements for effective 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 the BIT level annual security discussions and will verify:

- The extent to which security controls are implemented correctly,
- Operating as intended,
- Meets the life cycle and level of risk security requirements of the system(s).

BIT Security Policy

The BIT security policy requires that an assessment of applications supporting the needs of the Medicaid Management Information System (MMIS) and the Medicaid eligibility determination system be conducted no less than every three years. Assessments are also required when significant enhancements are made to applications currently in production and prior to new applications being moved into production. The assessments shall be independent of the application manager and verify the following:

- Responsibility for the security of the application has been assigned;
- A viable security plan for the application is in place;
- That a manager has authorized the processing of the application.

Assessment Report

A report specifying each area reviewed or audited during the assessment process will be completed and filed. The *Audit Findings Template Follow Up - Status form* is located at http://intranet.bit.sd.gov/forms/. This form is required to be attached to the report for reviewing and auditing purposes and shall contain the following:

- All deficiencies discovered during the assessment shall be entered on the form;
- Each identified deficiency will be analyzed, assigned to an area within BIT including a solution noted and a due date for the solution(s) to become effective;
- If a deficiency is identified outside of a review or audit, the same procedures and processes shall be followed to log and track the deficiency and resolution status;
- The Audit Findings Template Follow Up - Status form shall be reviewed on a quarterly basis to ensure all deficiencies have been resolved in a timely manner.

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;
- Any and 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. This process ensures 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 meet the following requirements:

- 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. 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. 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;
- 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.

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 in order 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 private, 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 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.

610.9.4.3. 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 should 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 be in compliance 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

Preserving control of all Internet or other connections to the DDN and its devices is paramount to maintaining a secure perimeter. Therefore, 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 of all 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) by the use of 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. 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.

620.1.4.2. 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.

620.1.4.3. 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.

620.1.4.4. 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. 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.

620.5.4.2. 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). Additionally, 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.

620.5.4.3. 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.

620.5.4.4. 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.

620.5.4.5. 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.

INFORMATION TECHNOLOGY SECURITY POLICY: ABBREVIATIONS, DEFINITIONS, and TERM USAGE.

- **Accreditation**: 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 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.

- **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.

- **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.

- **Bureau of Information and Telecommunications (BIT)**: 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 Agreement**: An agreement with a Third party or vendor to assure the State that the vendor is appropriately protecting confidential client information and data.

- **Chief Information Security Officer (CISO)**: BIT senior executive charged with implementing the information technology security programs for the State.

- **Contractor**: Signatory to a contract/agreement the terms Contractor, Consultant and Vendor are equivalent. Subcontractors, Agents, Assigns and/or Affiliated Entities are not signatories to the contract/agreement the Information Technology Security Policy may be attached to but all policies in the Information Technology Security Policy apply to them also.

- **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 and 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. Examples:

  - **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;
- 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;
    - Damage the integrity of the State;
    - Result in significant or major financial loss;
    - Result in significant, severe or catastrophic harm to individuals.

- **Federal Taxpayer Identification (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.

- **Personally Identifiable Information: (PII):** Any information about an individual 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

- **Regulated**: Very specific types of data regulated by law. In the context of the Regulated Data Chart these data types are FERPA, HIPAA, GLBA, ITAR and EAR:

    - *FERPA*: Education records are protected by FERPA (Family Educational Rights and Privacy Act). Examples: Tax records of parents and students; Class lists, grade rosters, records of advising sessions, grades, financial aid applications. See Policy 4.5, Access to Student Information and data;
    - *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. Examples: Health records, patient treatment information and data, health insurance billing information and data. The HIPAA covered entities at Cornell are Weill Cornell Medical College, Gannett Health Services, HR Benefits (both for the Ithaca campus and WCMC), and

Counsel's Office;

- *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). Example: dual-use technology used for scientific advancement as well as military applications.

- **Return Information:** In general, is 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.

- **Sensitive:** Any information and data not available to the public via the Freedom of Information Act (http://www.foia.gov/index.html) or the State Open Records Laws SDCL 1-27 (http://legis.sd.gov/Statutes/Codified_Laws/DisplayStatute.aspx?Type=Statute&Statute=1-27).

- **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;
- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

- **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.

- **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.

- **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-Miliarized Zone (DMZ)**: A perimeter network that contains external-network facing services. Applications needing access from the public Internet are located in the DMZ.

- **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).

- **Employee**: You are classified as an employee of the State of South Dakota or you are a third party individual or company providing work for a State government agency. Contractors and Employees are treated identically throughout the Information Technology Security Policy.

- **Federal Parent Locator System (FPLS)**: The FPLS is an assembly of systems operated by 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. Definition from: (http://www.acf.hhs.gov/programs/css/resource/federal-parent-locator-service-information-for-families).

- **File Transfer Protocol (FTP)**: A standard network protocol used to transfer data files between one workstation network and another.

- **Hackers**: Individuals or a group of individuals with the intent of doing harm to state data, infrastructure or services.

- **Internet of Things**: The network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data such as, but not limited to, monitoring implants, automobiles with built-in sensors, DNA analysis devices. Look at "Things" as an "inextricable mixture of hardware, software, data and service" that collect useful data with the help of various existing technologies and then autonomously flow the data between other devices.

- **IRS**: Internal Revenue Service.

- **Malware**: short for malicious software, is any software used to disrupt workstation operations, gather various types of data and information, gain access to DDN Intranet or display unwanted popups or ads.
- **MMIS:** Medicaid Management Information System.
- **Mobile Device:** A portable, wireless computing device that is small enough to be used while held in the hand.
- **Mobile Wi-Fi (MIFI)**: A wireless router that acts as a mobile wireless network hotspot.
- **NATURAL:** A programming language created by Software AG used to interface with ADABAS (Adaptable Data Base System).
- **NIST:** National Institute of Standards and Technology.
- **OWASP:** Open Web Application Security Project.
- **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.
- **Reaccreditation**: The periodic rescanning of a system looking for security vulnerabilities.
- **Remote Access Device (RAD)**: RADs include smartphones like iPhones, Windows and Android phones; mobile computing devices like iPods, 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.
- **Security Incident**: Any cyber security event or threat of an event affecting the normal operation of a workstation, software application or the technology infrastructure of the State.
- **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.
- **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.

- **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.

- **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.

- **Workstations**: Any State owned desktop, laptop, or tablet computer.

Attachment D

Security and Vendor Questions

A = Data Center
B = Development
C = PMO Office
D = Telecommunications

	BIT Owner	Question	Response	Add text as required
1.	C	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?	Yes☐ No☐ NA ☐	
2.	D	Is there a workstation install requirement?	Yes☐ No☐ NA ☐	
3.	A/D	Is this a browser based User Interface?	Yes☐ No☐ NA ☐	
4.	B/C	What is the development technologies used for this system? ASP _____ VB.Net _____ C#.Net _____ .NET Framework _____ Java/JSP _____ MS SQL _____		
5.	A	Will the system support authentication?	Yes☐ No☐ NA ☐	
6.	A	Will the system infrastructure require an email interface?	Yes☐ No☐ NA ☐	
7.	A	Will the system require a database?	Yes☐ No☐ NA ☐	
8.	A	Will the system infrastructure require database replication?	Yes☐ No☐ NA ☐	

9.	A	Will the system require transaction logging for database recovery?	Yes☐ No☐ NA ☐	
10.	A	Will the system infrastructure have a special backup requirement?	Yes☐ No☐ NA ☐	
11.	B/C	Will the system provide an archival solution? If not is the State expected to develop a customized archival solution?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
12.	A	Will the system infrastructure have any processes that require scheduling?	Yes☐ No☐ NA ☐	
13.	A/B	Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?	Yes☐ No☐ NA ☐	
14.	A/B	Will the system infrastructure require a Business Intelligence solution?	Yes☐ No☐ NA ☐	
15.	B/C	Will the system have any workflow requirements?	Yes☐ No☐ NA ☐	
16.	C	Explain the software licensing model.		
17.	A	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?	Yes☐ No☐ NA ☐	
18.	A	Can the system be implemented via Citrix?	Yes☐ No☐ NA ☐	
19.	B/D	Will the system implement its own level of security?	Yes☐ No☐ NA ☐	
20.	A	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?	Yes☐ No☐ NA ☐	
21.	A	Will the system print to a Citrix compatible networked printer?	Yes☐ No☐ NA ☐	
22.	D	Will the network communications meet IEEE standard TCP/IP and use either standard ports or State defined ports as the State determines?	Yes☐ No☐ NA ☐	
23.	A/D	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)?	Yes☐ No☐ NA ☐	
24.	D	Will the system provide Internet security functionality on a public portal to include firewalls?	Yes☐ No☐ NA ☐	

25.	D	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?	Yes☐ No☐ NA ☐	
26.	D	Does your application use Java, is it locked into a certain version or will it use the latest version if so what is your process for updating the application?	Yes☐ No☐ NA ☐	
27.	D	If your application does not run under the latest Microsoft operating system what is your process for updating the application?		
28.	A	Will the server based software support: a. Windows server 2012 R2 b. IIS7.0 or higher c. MS SQL Server 2008R2 or higher d. Exchange 2010 or higher e. Citrix presentation server 4.5 or higher f. VMWare ESXi 5.5 or higher g. MS Windows Updates h. Symantec End Point Protection	 Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
29.	B	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.		
30.	D	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?	Yes☐ No☐ NA ☐	
31.	A	It is State policy that all systems must be compatible with BITs dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
32.	A	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?	Yes☐ No☐ NA ☐	

33.	D	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 Secure Gateway. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
34.	D	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?	Yes☐ No☐ NA ☐	
35.	A	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?	Yes☐ No☐ NA ☐	
36.	A	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?	Yes☐ No☐ NA ☐	
37.	D	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?	Yes☐ No☐ NA ☐	
38.	D	It is State policy that systems must support NAT and PAT running inside the State Network. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
39.	D	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?	Yes☐ No☐ NA ☐	
40.	D	Will your system use Adobe Air, Adobe Flash, Apache Flex, JavaFX , Microsoft Silverlight? If yes what are your plans for moving off them?	Yes☐ No☐ NA ☐	
41.	D	Does your web application use PHP or Adobe ColdFusion?	Yes☐ No☐ NA ☐	
42.	A/B	How does data enter the system (transactional or batch or both)?		
43.	C	Is the system data exportable by the user for use in tools like Excel or Access?	Yes☐ No☐ NA ☐	

44.	C	Will user customizable data elements be exportable also?	Yes☐ No☐ NA ☐	
45.	C	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?	Yes☐ No☐ NA ☐	
46.	C	Will this system provide the capability to track data entry/access by the person, date and time?	Yes☐ No☐ NA ☐	
47.	A/B/ C/D	Will the system provide data encryption for sensitive information both in storage and transmission?	Yes☐ No☐ NA ☐	
48.	D	It is State policy that systems at the discretion of the State may have a Security Audit performed on it by BIT or a 3rd Party for security vulnerabilities. Would this affect the implementation of the system?	Yes☐ No☐ NA ☐	
49.	C/D	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?	Yes☐ No☐ NA ☐	
50.	A	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?	Yes☐ No☐ NA ☐	
51.	A/C	Will the vendor provide assistance with installation?	Yes☐ No☐ NA ☐	
52.	A/C	Is there an installation guide available and will you provide a copy to the State?	Yes☐ No☐ NA ☐	
53.	A/C	Is telephone assistance available for both installation and use?	Yes☐ No☐ NA ☐	
54.	A/B /C	Is on-site assistance available? If so, is there a charge?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
55.	A/B /C	Will the implementation plan include user acceptance testing?	Yes☐ No☐ NA ☐	

56.	B	Will technical documentation for application maintenance purposes be provided to the State?	Yes☐ No☐ NA ☐	
57.	B/C	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?	Yes☐ No☐ NA ☐	
58.	C	Can the user manual be printed?	Yes☐ No☐ NA ☐	
59.	C	Is the user manual electronically available?	Yes☐ No☐ NA ☐	
60.	C	Is there on-line help assistance available?	Yes☐ No☐ NA ☐	
61.	C	Describe your Support options.		
62.	A/C	Is there a method established to communicate availability of system updates?	Yes☐ No☐ NA ☐	
63.	A/D	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?	Yes☐ No☐ NA ☐	
64.	B/C	Will you provide customization of the system if required by the State of South Dakota?	Yes☐ No☐ NA ☐	
65.	B	Will the state be required to develop customized interfaces to other applications?	Yes☐ No☐ NA ☐	
66.	B	Will the State be required to develop reports or data extractions from the database?	Yes☐ No☐ NA ☐	
67.	A/B /C	Will the State of South Dakota have access to the underlying data and data model for ad hoc reporting purposes?	Yes☐ No☐ NA ☐	
68.	C	Will the source code for the system be put in escrow for the State of South Dakota?	Yes☐ No☐ NA ☐	
69.	C	If the source code is placed in escrow, will the vendor pay the associated escrow fees?	Yes☐ No☐ NA ☐	
70.	B/C	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?	Yes☐ No☐ NA ☐	
71.	C	Explain the basis on which pricing could change for the state based on your licensing model.		

72.	C	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?		
73.	B/C	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?	Yes☐ No☐ NA ☐	
74.	B/C	Has your company ever conducted a project where you were tasked with performing load testing?	Yes☐ No☐ NA ☐	
75.	B/C	Has your company ever developed a system that ran on Citrix Metaframe?	Yes☐ No☐ NA ☐	
76.	B/C	Have you ever created a User Acceptance Test plan and test cases?	Yes☐ No☐ NA ☐	
77.	C	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 Secure Gateway or Skype for Business. Would this affect implementation of the system?	Yes☐ No☐ NA ☐	
78.	C	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.		
79.	C	Are there expected periods of time where the application will be unavailable for use?	Yes☐ No☐ NA ☐	
80.	C	Is there a strategy for mitigating unplanned disruptions?	Yes☐ No☐ NA ☐	
81.	C	Will the State of South Dakota own the data created in your hosting environment?	Yes☐ No☐ NA ☐	
82.	C	Will the State acquire the data at contract conclusion?	Yes☐ No☐ NA ☐	
83.	C	Will organizations other than the State of South Dakota have access to our data?	Yes☐ No☐ NA ☐	

84.	C	Will the State's data be used for any other purposes other than South Dakota's usage?	Yes☐ No☐ NA ☐	
85.	C	Will the State's data be protected?	Yes☐ No☐ NA ☐	
86.	C	List any hardware or software you propose to use that is not state standard, the standards can be found at http://bit.sd.gov/standards/.		
87.	A	Please explain the pedigree of the software, include in your answer who are the people, organization and processes that created the software		
88.	A	Explain the change management procedure used to identify the type and extent of changes allowed in the software throughout its lifecycle. Include information on the oversight controls for the change management procedure.		
89.	D	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.	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
90.	B	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)?		
91.	B	Explain the use cases used for software assurance during development.		
92.	D	Describe the training your company offers related to defining security requirements, secure architecture and design, secure coding practices, and security testing.		
93.	D	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?	Yes☐ No☐ NA ☐	
94.	B	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?	Yes☐ No☐ NA ☐	
95.	B	Are there some requirements for security that are "structured" as part of general releasability of a product and others that are "as needed" or	Yes☐ No☐ NA ☐	

		"custom" for a particular release?		
96.	D	What process is utilized by your company to prioritize security related enhancement requests?		
97.	D	What threat assumptions were made, if any, when designing protections for the software and information assets processed?		
98.	D	In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?	Yes☐ No☐ NA ☐	
99.	A	Explain how and where the software validates (e.g., filter with white listing) inputs from untrusted sources before being used.		
100.	D	Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user) and is it designed to isolate and minimize the extent of damage possible by a successful attack?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
101.	D	Where applicable, does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?	Yes☐ No☐ NA ☐	
102.	D	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?		
103.	D	What security criteria, if any, are considered when selecting third-party suppliers?		
104.	B	What coding and/or API standards are used during development of the software?		
105.	B	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing, integrated testing)?		
106.	D	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?		
107.	B	Are misuse test cases included to exercise potential abuse scenarios of the software?	Yes☐ No☐ NA ☐	
108.	B	Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?	Yes☐ No☐ NA ☐	

109.	D	What release criteria does your company have for its products with regard to security?		
110.	B	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?		
111.	B	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?		
112.	D	How has the software been measured/assessed for its resistance to identified, relevant attack patterns? Are Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs) used? How have the findings been mitigated?		
113.	D	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If the CC, what evaluation assurance level (EAL) was achieved? If the product claims conformance to a protection profile, which one(s)? Are the security target and evaluation report available?	Yes☐ No☐ NA ☐	
114.	A/D	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?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
115.	A/B	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
116.	A/D	Has the product undergone any penetration testing? When? By whom? Are the test reports available under a nondisclosure agreement? How have the findings been mitigated?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	

117.	B	Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)? If yes please explain.	Yes☐ No☐ NA ☐	
118.	A/B	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?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
119.	A	How will patches and/or Service Packs be distributed to the Acquirer?		
120.	B	What services does the help desk, support center, or (if applicable) online support system offer?		
121.	A/B	How extensively are patches and Service Packs tested before they are released?		
122.	A	Can patches and Service Packs be uninstalled? Are the procedures for uninstalling a patch or Service Pack automated or manual?	Yes☐ No☐ NA ☐	
123.	A/B	How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?		
124.	A	How do you set the relative severity of defects and how do you prioritize their remediation?		
125.	A	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches?		
126.	A	Are third-party developers contractually required to follow your configuration management policies?	Yes☐ No☐ NA ☐	
127.	B	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?		
128.	B	How is the software provenance verified (e.g. any checksums or signatures)?		
129.	A	Does your company publish a security section on its Web site? If so, do security researchers have the ability to report security issues?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
130.	A	Does your company have an executive-level officer responsible for the	Yes☐ No☐ NA ☐	

		security of your company's software products and/or processes?		
131.	A	Has your company ever filed for Recompany under U.S. Code Chapter 11? If so, please provide dates for each incident and describe the outcome.	Yes☐ No☐ NA ☐	
132.	A	Are security requirements developed independently of the rest of the requirements engineering activities, or are they integrated into the mainstream requirements activities?		
133.	A/B /D	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?		
134.	B	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.	Yes☐ No☐ NA ☐	
135.	B	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?	Yes☐ No☐ NA ☐	
136.	A	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.	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
137.	B	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?		
138.	B	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?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
139.	B	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?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
140.	A	Does the software have any security critical dependencies or need additional controls from other software (e.g., operating system, directory	Yes☐ No☐ NA ☐	

		service, application), firmware, or hardware? If yes, please describe.		
141.	A	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?		
142.	A	Does your company's defect classification scheme include security categories?	Yes☐ No☐ NA ☐	
143.	B	What percentage of code coverage does your testing provide?		
144.	B	When does security testing occur during the SDLC (e.g., unit level, subsystem, system, certification and accreditation)?		
145.	A	Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration following installation?	Yes☐ No☐ NA ☐	
146.	B	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?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
147.	B	How is the assurance of software produced by third-party developers assessed?		
148.	D	How are trouble tickets submitted? How are support issues, specifically those that are security related, escalated?		
149.	A	Are help desk or support center personnel internal company resources or are these services outsourced to third parties?		
150.	A	If help desk or support center services are outsourced to third parties, are they located in foreign countries?		
151.	B	Does your company have a vulnerability management and reporting policy? Is it available for review?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
152.	A	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.	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
153.	B	Does your company have formally defined security policies associated	Yes☐ No☒ NA ☐	

		with clearly defined roles and responsibilities for personnel working within the software development life cycle, explain.		
154.	A	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.	Yes☐ No☐ NA ☐	
155.	A	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).		
156.	A	Is the controlling share (51+%) of your company owned by one or more non-U.S. entities?	Yes☐ No☐ NA ☐	
157.	A	What are your customer confidentiality policies? How are they enforced?		
158.	D	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?		
159.	A	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?		
160.	A	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?	Yes☐ No☐ NA ☐	
161.	A	What are your policies and procedures for hardening servers?		
162.	A	What are your data backup policies and procedures? How frequently are your backup procedures verified?		
163.	A	What are the procedures for evaluating any vendor security alerts and installing patches and Service Packs?		
164.	A	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?	Yes☐ No☐ NA ☐	

165.	A	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?		
166.	A	What are the procedures and policies used to control access to the servers? Are audit logs maintained?		
167.	A	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?		
168.	A	Do you have a formal disaster recovery plan? What actions will be taken to recover from a disaster? Are warm or hot backups available?	Yes☐ No☐ NA ☐	
169.	A	Is two-factor authentication used for administrative control of all security devices and critical information systems?	Yes☐ No☐ NA ☐	
170.	A/D	How are virus prevention, detection, correction, and updates handled for the products?		
171.	D	What type of firewalls (or application gateways) do you use? How are they monitored/managed?		
172.	D	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?		
173.	A/D	Explain or provide a diagram of the architecture for the application including security mitigation.		
174.	A	Do you perform regular reviews of system and network logs for security issues?	Yes☐ No☐ NA ☐	
175.	A	Do you have an automated security event management system?	Yes☐ No☐ NA ☐	
176.	A	What are your procedures for intrusion detection, incident response, and incident investigation/escalation?		
177.	A	Will you provide on-site support 24x7 to resolve security incidents?	Yes☐ No☐ NA ☐	
178.	A	Are security logs and audit trails protected from tampering or modification?	Yes☐ No☐ NA ☐	
179.	A	How do you control physical and electronic access to the log files? Are log files consolidated to single servers?		

180.	A	Do you provide security performance measures to the customer at regular intervals?	Yes☐ No☐ NA ☐	
181.	A	Describe your security testing processes.		
182.	A	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?	Yes☐ No☐ NA ☐	
183.	A	The state does not allow applications to be placed on the state's system, or the state's system to connect to another system, or the consultant to store or process state data without first doing security scans. The state would want to scan a test system not a production system, are either of these an issue, if so please explain.	Yes☐ No☐ NA ☐	
184.	A	How frequently is the security tests performed? Are the tests performed by internal resources or by a third party?		
185.	A	Do you have a SOC 2 audit report? Is the audit done annually? Does the audit cover all 5 of the trust principles? Does the audit include subservice providers? Has the auditor always been able to attest to an acceptable audit result? Will you provide a copy of your latest SOC 2 audit upon request, a redacted version is acceptable.	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	
186.	A	Are you or if the data is being hosted by a subservice provider are they FedRAMP certified?	Yes☐ No☐ NA ☐	
187.	B	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?	Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐ Yes☐ No☐ NA ☐	