Retrospective Drug Utilization Review (RDUR)

PROPOSALS ARE DUE NO LATER THAN July 19, 2018, 5:00 PM CDT

RFP #1277
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)

The Department of Social Services, Division of Medical Services is seeking proposals from qualified vendors to provide Retrospective Drug Utilization Review (RDUR) services.

1.2 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Division of Medical Services is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, Department of Social Services. The reference number for the transaction is RFP #1277. Refer to this number on all proposals, correspondence, and documentation relating to the RFP.

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

1.3 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFP Publication</td>
<td>6/4/2018</td>
</tr>
<tr>
<td>Deadline for Submission of Written Inquiries</td>
<td>6/19/2018</td>
</tr>
<tr>
<td>Responses to Offeror Questions</td>
<td>6/26/2018</td>
</tr>
<tr>
<td>Proposal Submission</td>
<td>7/19/2018, 5:00 PM CDT</td>
</tr>
<tr>
<td>Anticipated Award Decision/Contract Negotiation</td>
<td>8/23/2018</td>
</tr>
</tbody>
</table>

1.4 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received in the Department of Social Services, 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, eight (8) identical copies, and one (1) digital, Portable Document Format (PDF) copy loaded on a USB flashdrive of the proposal, all attachments, and the cost proposal(s) must be submitted.

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

Request For Proposal #1277 Proposal Due July 19, 2018
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, vendors, and suppliers doing business with any State agency, department, or institution, provide a statement of non-discrimination. By signing and submitting their proposal, the offeror certifies they do not discriminate in their employment practices with regard to race, color, creed, religion, age, sex, ancestry, national origin or disability.

1.7 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 June 19, 2018, 5:00 PM CDT. Email inquiries must be sent to mark.close@state.sd.us with the following wording, exactly as written, in the subject line: RFP #1277 Questions.

The Department of Social Services (DSS) will respond to offerors’ inquiries by posting offeror aggregated questions and Department responses on the DSS website at http://dss.sd.gov/keyresources/rfp.aspx no later than June 26, 2018, 5:00 PM CDT. For expediency, DSS may combine similar questions. Offerors may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.9 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 initial contract resulting from this RFP will be issued for a period of six (6) months, December 1, 2018 to May 31, 2019, with the option of renewal for up to two (2), one (1) year contracts at the discretion of the State.
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 (including contract exhibits) may be altered or deleted. The Offeror should indicate in their response any issues they have with any specific contract terms. If the Offeror does not indicate any contract term issues, then the State will assume the terms are acceptable.

3.0 SCOPE OF WORK

An efficient and robust Medicaid program is essential to the Department of Social Services vision of strong families being South Dakota’s foundation and future. One key component of the Medicaid program is a prescription drug benefit for eligible Medicaid recipients.

Provide a detailed response of how compliance will be achieved to each of the following requirements.

The contractor will:

3.1 Provide a web based, vendor hosted RDUR software program which is compatible with the State’s current browser standard which can be found at http://bit.sd.gov/standards/ BIT Standards are inclusive of Explorer 11, Microsoft Edge and Chrome.
3.2 Accept weekly electronic data feeds which consists of three files, (provider, claims, and recipient) in the state specified format to the RDUR system. See Attachment B for file layouts;
3.3 Warrants that all State’s data will be encrypted in transmission (including via web interface) and storage at no less than SHA256 level encryption with SHA256 or SHA2 hashing.
3.4 Provide timely Ad Hoc reporting services utilizing the RDUR claims data;
3.5 Provide State approved education materials to State selected providers. Education materials may include written or electronic notices or newsletters, and/or targeted interventions to individual prescribers or prescriber specialties;
3.6 Comply with all Federal rules pertaining to the Medicaid RDUR activities;
3.7 Submit to the Centers for Medicaid and Medicare Services the Annual Drug Utilization Review Report; and,
3.8 Provide a quarterly report of Medicaid recipients age 18 or less who received a prescription for a psychotropic medication. Report will include, at a minimum, medication name, medication strength, medication quantity, days’ supply, date of service, recipient identification number, recipient name, recipient age, prescriber identification number, pharmacy identification number;
3.9 Describe disaster recovery plan;
3.10 Describe level and amounts of cyber liability coverage.
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 **MUST** 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 System and Organization Controls, Statement on Standards for Attestation Engagements (SOC 1 SSAE18) report, then annually thereafter for the term of the agreement. For SOC 1 SSAE 18 the 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 submit information that demonstrates their availability and familiarity with the locale in which the project(s) are to be implemented.

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

4.8 The offeror must describe their proposed project management techniques.

4.9 The offeror understands and agrees to fully comply with and meet the State of South Dakota's Bureau of Information and Telecommunications (BIT) Standards and requirements.

   4.9.1 Without exception, all software and cloud services purchased by the State of South Dakota will be subject to non-production security scans by BIT.

   4.9.2 The offeror must review and acknowledge that the Security Acknowledgement Form (Exhibit C) must be signed at contract signature.

   4.9.3 The offeror must acknowledge that the selected offeror must undergo fingerprint-based background checks in accordance with the attached contract provisions (Exhibit A). The background checks will be used to check the criminal history records of the State as well as the Federal Bureau of Investigation’s records.
4.9.4 The offeror is required to answer and sign the attached Security and Vendor Questions (Attachment C) which may be used in the proposal evaluation.

4.10 The offeror must provide a system diagram of their proposed solution.

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

5.0 PROPOSAL RESPONSE FORMAT

5.1 An original and eight (8) copies shall be submitted.

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

5.1.2 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 tabbed with labels 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 Resources available to perform the work, including any specialized services, within the specified time limits for the project;

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

6.1.4 Cost proposal;

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; and

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**

The offeror’s cost proposal shall reflect costs to deliver the services identified in this RFP for the initial six month period and the additional cost per year for the full years of service for optional renewal periods two and three.
The State hereby enters into a contract (the “Agreement” hereinafter) for consultant services with the Consultant. While performing services hereunder, Consultant is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

1. CONSULTANT’S South Dakota Vendor Number is .

2. PERIOD OF PERFORMANCE:
   A. This Agreement shall be effective as of June 1, 2018 and shall end on May 31, 2019, unless sooner terminated pursuant to the terms hereof.
   B. Agreement is the result of request for proposal process, RFP #1277.

3. PROVISIONS:
   A. The Purpose of this Consultant contract:
      1. 
   2. Does this Agreement involve Protected Health Information (PHI)? YES (X) NO ( )
      If PHI is involved, a Business Associate Agreement must be attached and is fully incorporated herein as part of the Agreement (refer to Exhibit B).
   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)
            If YES, expenses submitted will be reimbursed as identified in this Agreement.
D. Due to the subject matter of this Agreement, it requires the approval of the SD Bureau of Information and Telecommunications ("BIT hereinafter). The consultant specifically agrees to the terms and conditions of the BIT supplementary contract clauses attached here to as Exhibit A, the BIT Security Acknowledgement attached hereto as Exhibit C, and the IT Security Policy attached hereto as Exhibit D, which Exhibits are collectively incorporated herein by reference and made a part hereof.

E. The TOTAL CONTRACT AMOUNT will not exceed $ .

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

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

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

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

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

All payments to the Consultant by the State are subject to site review and audit as prescribed and carried out by the State. Any over payment of this Agreement shall be returned to the State within thirty days after written notification to the Consultant.
9. WORK PRODUCT:
Consultant hereby acknowledges and agrees that all reports, plans, specifications, technical data, drawings, software system programs and documentation, procedures, files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, State Proprietary Information, as defined in the Confidentiality of Information paragraph herein, state data, end user data, Protected Health Information as defined in 45 CFR 160.103, and all information contained therein provided to the State by the Consultant in connection with its performance of service under this Agreement shall belong to and is the property of the State and will not be used in any way by the Consultant without the written consent of the State.

Paper, reports, forms, software programs, source code(s) and other materials which are a part of the work under this Agreement will not be copyrighted without written approval of the State. In the unlikely event that any copyright does not fully belong to the State, the State nonetheless reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, and otherwise use, and to authorize others to use, any such work for government purposes.

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

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

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

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

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

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

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

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

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

18. SUBCONTRACTORS:
The Consultant may not use subcontractors to perform the services described herein without express prior written consent from the State. The State reserves the right to reject any person from the Agreement presenting insufficient skills or inappropriate behavior.

The Consultant will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with this Agreement. The Consultant will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance. The State, at its option, may require the vetting of any subcontractors. The Consultant is required to assist in this process as needed.

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

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

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

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

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

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

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

(Medical Health Professional shall maintain current general professional liability insurance with a limit of not less than one million dollars for each occurrence and three million dollars in the aggregate. Such insurance shall include South Dakota state employees as additional insureds in the event a claim, lawsuit, or other proceeding is filed against a state employee as a result of the services provided pursuant to this Agreement. If insurance provided by Medical Health Professional is provided on a claim made basis, then Medical Health Professional shall provide “tail” coverage for a period of five years after the termination of coverage.)
22. CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:
Consultant certifies, by signing this Agreement, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by the federal government or any state or local government department or agency. Consultant further agrees that it will immediately notify the State if during the term of this Agreement either it or its principals become subject to debarment, suspension or ineligibility from participating in transactions by the federal government, or by any state or local government department or agency.

23. CONFLICT OF INTEREST:
Consultant agrees to establish safeguards to prohibit employees or other persons from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Consultant expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.

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

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

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

<table>
<thead>
<tr>
<th>Consultant Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consultant Printed Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State - DSS Division Director</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State - DSS Chief Financial Officer Laurie Mikkonen</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State - DSS Cabinet Secretary Lynne A. Valenti</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State - BIT Interim Commissioner Patrick Snow</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

State Agency Coding:

<table>
<thead>
<tr>
<th>CFDA #</th>
<th>Company</th>
<th>Account</th>
<th>Center Req</th>
<th>Center User</th>
<th>Dollar Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS Program Contact Person</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DSS Fiscal Contact Person</th>
<th>Contract Accountant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>605 773-3586</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consultant Program Contact Person</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consultant Fiscal Contact Person</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
INFORMATION TECHNOLOGY SUPPLEMENT CLAUSES
Exhibit A

1. APPLICATION OF CONTRACT TERMS
All of the following terms and provisions are applicable to each and every entity that hosts State data. If the Consultant is proposing to subcontract any hosting of State data to another entity, the relationship between Consultant and any such subcontracting entity must be that of Principal and Agent. No such Agent may act as an independent contractor for Consultant. Consultant must include in its contract with any such Agent explicit terms providing for this Principal and Agent relationship, and Consultant must further supervise such Agent so as to insure that such Agent complies with all of the following terms. If the Consultant shares any Personal Health Information with any other entity, other than the individual who owns the information, the Consultant will ensure that that entity also adheres to the security requirements of this agreement. This includes any Personal Health Information that is shared as part of providing health care services, except in emergency situations.

2. DATA LOCATION
The Consultant shall provide its services to the State as well as storage of State data solely from data centers in the continental United States. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States. The Consultant shall not allow its personnel or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at its data centers. The Consultant shall permit its personnel and contractors to access State data remotely only as required to provide technical support.

3. CESSATION OF BUSINESS
The Consultant will notify the State of impending cessation of its business or that of a tiered provider and the Consultant’s contingency plan. This plan should include the immediate transfer of any previously escrowed assets and data and State access to the Consultant’s facilities to remove or destroy any State-owned assets and data. The Consultant shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Consultant will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Consultant will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State. The Consultant will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the State, all such work to be coordinated and performed in advance of the formal, final transition date.

4. SERVICE LEVEL AGREEMENTS
The Consultant warrants that all services will be performed in a professional and workmanlike manner consistent with industry standards reasonably applicable to such services. The Consultant further warrants that the services will be operational at least 99.99% of the time in any given month during the term of this Agreement. In the event of a service outage, the Consultant will:
A. Promptly and at the Consultant’s expense, use commercial best efforts to restore the services as soon as possible, and
B. Unless the outage was caused by a Force Majeure event refund or credit the State, at the State’s election, the pro-rated amount of fees corresponding to the time Services were unavailable or $100 US funds per incident, whichever is the greater amount. For the purpose of this agreement, an incident, regardless of time required to return to online position and whether re-keying of data is necessary to return, is defined as any significant reduction in the availability of hosted services lasting more than one minute or resulting in data loss, rework, or occurring more than 3 times in a 24 hour time period. For example, being forced offline no more than twice in 24 hours would not be an incident if the user could get back online within 60 seconds and continue work where he or she left off. Being forced off line 3 times in a day would be an incident, regardless. Being forced off line once in a 24 hour period of time, however, that resulted in the user having to rekey data that was lost would be an incident. Entering User authentication to log on shall not be considered data entry.

The Consultant will provide the State with seven days prior notice of scheduled downtime in the provision of services for maintenance or upgrades. To the extent possible, the Consultant will schedule downtime during times of ordinarily low use by the State. In the event of unscheduled or unforeseen downtime for any reason, except as otherwise prohibited by law, the Consultant will promptly notify the State and respond promptly to the State’s reasonable requests for information regarding the downtime.
5. LEGAL REQUESTS FOR DATA
Except as otherwise expressly prohibited by law, the Consultant will:

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

B. Consult with the State regarding its response;

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

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

6. DATA RETENTION AND DISPOSAL
A. Using appropriate and reliable storage media, the Consultant will regularly back up State’s data and retain such backup copies for a minimum of thirty-six months. At the end of that time period and at the State’s election, the Consultant will either securely destroy or transmit to the State repository the backup copies. Upon the State’s request, the Consultant will supply the State with a certificate indicating the nature of the storage media destroyed, the date destroyed, and the method of destruction used.

B. The Consultant will retain logs associated with End User activity for a minimum of seven years, unless the parties mutually agree to a different period.

C. The Consultant will immediately place a “hold” on the destruction under its usual storage media retention policies of storage media that include State’s data in response to an oral or written request from authorized State personnel indicating that those records may be relevant to litigation that the State reasonably anticipates. Oral requests by the State for a hold on storage media destruction will be reproduced in writing and supplied to the Consultant for its records as soon as reasonably practicable under the circumstances. The State will promptly coordinate with the Consultant regarding the preservation and disposition of storage media. The Consultant shall continue to preserve the storage media until further notice by the State. The Consultant will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the methods of disposal of storage media, are appropriate to and fulfill all of the State’s needs. By way of example but not of limitation, all hard drives and tapes used to store State data must, upon destruction be properly disposed of.

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

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

9. SECURITY PROCESSES
The Consultant shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Consultant. For example: virus checking and port sniffing.
10. IMPORT AND EXPORT OF DATA
   The State shall have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Consultant. This includes the ability for the State to import or export data to/from other Consultants.

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

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

   The Consultant indemnifies the state for ordinary, consequential and incidental damages to the Consultant’s computer system and the data it contains that is the result of scanning. Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State’s security scans discover security issues the State may collaborate, at the State’s discretion with, the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements between the State and Consultant. The State will not be charged for any costs incurred by the consultant in these remediation efforts unless agreed to by the State in advance in writing. In the event of conflicting language this clause supersedes any other language in this or any other agreement made between the State and the Consultant.

   The Consultant agrees to work with the State to rectify any serious security issues revealed by the security audit and or security scanning. This includes additional security audits and security scanning that shall be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist.

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

13. WEB SERVICES
   The Consultant shall use Web services exclusively to interface with the State’s data.

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

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

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

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

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

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

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

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

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

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

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

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.

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

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

25. MULTIFACTOR AUTHENTICATION
The Consultant must adhere to the requirements of level 3 authentication assurance for multifactor authentication as defined in NIST 800-63 when performing work under this contract where the Consultant potentially has access to legally protected State data. The Consultant must require that and all its Subcontractors, Agents, Assigns, and Affiliated Entities who potentially have access to legally protected State data also adhere to level 3 authentication assurance as defined in NIST 800-63, and Consultant shall be in breach of this contract if Consultant fails to so require.

26. CONSULTANT TRAINING REQUIREMENTS
The Consultant, Consultant’s employee(s), and Consultant’s Subcontractors, Agents, Assigns, Affiliated Entities and their employee(s), must successfully complete, at the time of hire and annually thereafter, a cyber-security training program. The training must include but is not limited to: i) Legal requirements for handling data, ii) Media sanitation, iii) Strong password protection, iv) Social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, and v) Security incident response, and vi) Personal Health Information.

27. USE OF PRODUCTION DATA IN A DEVELOPMENT OR TESTING ENVIRONMENT
The Consultant cannot use State data which is either legally protected or protected by industry standards in a development or testing environment without prior approval of the State, whether the environments are State or Consultant hosted environments. The Consultant should allow sufficient time for the approval process in their project planning. A detailed explanation of the approval process and requirements can be found in the Information Technology Security Policy which is attached as Exhibit D. The Consultant should make itself aware of the security needs of the protected data before requesting an exception to this policy. The development or test environment must have the same level of security as a production system would have when dealing with the same data. When the production data is no longer needed it must be deleted from the development or test environment. At no time will any protected State data be allowed to be located outside the continental United States. Any development or test environment that is found to have unapproved production data, must be purged immediately and the State Contact notified. The State will decide if this event is to be considered a security incident. Legally protected data is any data protected under Federal or State Statute or regulation. Industry standards are requirements specific to an industry for data handling. An example of data protected by industry standards is payment card industry information (PCI).
STATE OF SOUTH DAKOTA
DEPARTMENT OF SOCIAL SERVICES

Exhibit B

Business Associate Agreement

1. Definitions

General definition:

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

Specific definitions:

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

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

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

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


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

2. Obligations and Activities of Business Associate

Business Associate agrees to:

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

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

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware within five (5) business days of receiving knowledge of such use, disclosure, breach, or security incident;
(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the covered entity as necessary to satisfy covered entity’s obligations under 45 CFR 164.524. Business associate shall cooperate with covered entity to fulfill all requests by individuals for access to the individual’s protected health information that are approved by covered entity. If business associate receives a request from an individual for access to protected health information, business associate shall forward such request to covered entity within ten (10) business days. Covered entity shall be solely responsible for determining the scope of protected health information and Designated Record Set with respect to each request by an individual for access to protected health information;

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

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

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

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

3. Permitted Uses and Disclosures by Business Associate

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

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

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

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

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

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

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

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

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

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

5. Term and Termination

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

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

(c) Obligations of Business Associate Upon Termination.

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

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

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.
6. Miscellaneous
   (a) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

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

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

   (d) Conflicts. In the event of a conflict in between the terms of this Business Associate Agreement and the Agreement to which it is attached, the terms of this Business Associate Agreement shall prevail.
## ATTACHMENT B
### CLAIM LAYOUT

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORK-RECORD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WK-REF-NO</td>
<td>Work Reference Number</td>
<td>PIC X(14).</td>
<td></td>
</tr>
<tr>
<td>WK-ICD-IND</td>
<td>ICD-9 Code</td>
<td>PIC X(1).</td>
<td></td>
</tr>
<tr>
<td>WK-CLAIM-TYP</td>
<td>Claim Type</td>
<td>PIC XX.</td>
<td></td>
</tr>
<tr>
<td>WK-DISP</td>
<td>Dispensation</td>
<td>PIC X(2).</td>
<td></td>
</tr>
<tr>
<td>WK-STATUS</td>
<td>Status</td>
<td>PIC X(2).</td>
<td></td>
</tr>
<tr>
<td>WK-PROVIDER</td>
<td>Provider Name</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-RECIP-KEY</td>
<td>Recipient Key</td>
<td>PIC X(9).</td>
<td></td>
</tr>
<tr>
<td>WK-LEVEL-CARE</td>
<td>Level of Care</td>
<td>PIC X.</td>
<td></td>
</tr>
<tr>
<td>WK-NDC-PROC</td>
<td>NDC Procedure</td>
<td>PIC X(11).</td>
<td></td>
</tr>
<tr>
<td>WK-SVC-FROM-DTE</td>
<td>Service From Date</td>
<td>PIC X(8).</td>
<td></td>
</tr>
<tr>
<td>WK-THRU-DTE</td>
<td>Service To Date</td>
<td>PIC X(8).</td>
<td></td>
</tr>
<tr>
<td>WK-COVRD-7</td>
<td>Covered 7</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-D1</td>
<td>D1</td>
<td>PIC X.</td>
<td></td>
</tr>
<tr>
<td>WK-COVRD-2</td>
<td>Covered 2</td>
<td>PIC XX.</td>
<td></td>
</tr>
<tr>
<td>WK-TENTVE-7</td>
<td>Tentative 7</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-D2</td>
<td>D2</td>
<td>PIC X.</td>
<td></td>
</tr>
<tr>
<td>WK-TENTVE-2</td>
<td>Tentative 2</td>
<td>PIC XX.</td>
<td></td>
</tr>
<tr>
<td>WK-TYPE-OF-BILL</td>
<td>Type of Bill</td>
<td>PIC X(3).</td>
<td></td>
</tr>
<tr>
<td>WK-BILLING-NPI</td>
<td>Billing NPI</td>
<td>PIC X(10).</td>
<td></td>
</tr>
<tr>
<td>WK-PH-RX-NO</td>
<td>Prescription Number</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-PH-METRIC-QTY</td>
<td>Metric-Qty</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-MAC-IND</td>
<td>MAC Indication</td>
<td>PIC X.</td>
<td></td>
</tr>
<tr>
<td>WK-DAYS-SUPPLY</td>
<td>Days of Supply</td>
<td>PIC X(3).</td>
<td></td>
</tr>
<tr>
<td>WK-DEA-NO</td>
<td>DEA Number</td>
<td>PIC X(9).</td>
<td></td>
</tr>
<tr>
<td>WK-PR-PROC-HCPC</td>
<td>Procedure HCPC</td>
<td>PIC X(5).</td>
<td></td>
</tr>
<tr>
<td>WK-PR-DIAG</td>
<td>Procedure Diagnosis</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-PR-SEC-DIAG1</td>
<td>Secondary Diagnosis 1</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-PR-SEC-DIAG2</td>
<td>Secondary Diagnosis 2</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-PR-SEC-DIAG3</td>
<td>Secondary Diagnosis 3</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-PR-SEC-DIAG4</td>
<td>Secondary Diagnosis 4</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-PRIN-DIAG</td>
<td>Principal Diagnosis</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTH-DIAG-1</td>
<td>Other Diagnosis 1</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTH-DIAG-2</td>
<td>Other Diagnosis 2</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTH-DIAG-3</td>
<td>Other Diagnosis 3</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTH-DIAG-4</td>
<td>Other Diagnosis 4</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTH-DIAG-5</td>
<td>Other Diagnosis 5</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTH-DIAG-6</td>
<td>Other Diagnosis 6</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTH-DIAG-7</td>
<td>Other Diagnosis 7</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTH-DIAG-8</td>
<td>Other Diagnosis 8</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTHER-PROC-1</td>
<td>Other Procedure 1</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTHER-PROC-2</td>
<td>Other Procedure 2</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTHER-PROC-3</td>
<td>Other Procedure 3</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTHER-PROC-4</td>
<td>Other Procedure 4</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-OH-OTHER-PROC-5</td>
<td>Other Procedure 5</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-IH-PRIN-DIAG</td>
<td>Institutional Diagnosis</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-IH-OTH-DIAG-1</td>
<td>Other Diagnosis 1</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-IH-OTH-DIAG-2</td>
<td>Other Diagnosis 2</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-IH-OTH-DIAG-3</td>
<td>Other Diagnosis 3</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-IH-OTH-DIAG-4</td>
<td>Other Diagnosis 4</td>
<td>PIC X(7).</td>
<td></td>
</tr>
<tr>
<td>WK-IH-OTH-DIAG-5</td>
<td>Other Diagnosis 5</td>
<td>PIC X(7).</td>
<td></td>
</tr>
</tbody>
</table>
Recipient Layout

00001 ****************************************************************** 00001
00002 **** RECIPIENT ELIGIBILITY RECIPIENT RECORD  *** 000002
00003 ****************************************************************** 000003
00004 01 SD-ELIG-RECIP.  000004
00005 05 R-MMIS-KEY.  000005
00006 10 R-AID-CATEGORY  PIC 99.  000006
00007 10 R-RACE-SEX  PIC 9.  000007
00008 10 R-RESID-CNTY  PIC 99.  000008
00009 10 RECIP-ID-NUMBER.  000009
00010 15 R-APPL-CNTY  PIC 99.  000010
00011 15 R-ID-7.  000011
00012 20 R-CASE-NUMB  PIC 9(5).  000012
00013 20 R-SUB-NUMB  PIC 99.  000013
00014 05 R-NAME  PIC X(35).  000014
00015 05 R-BIRTH-DATE-X.  000015
00016 10 R-BIRTH-CC  PIC 99.  000016
00017 10 R-BIRTH-DATE.  000017
00018 15 R-BIRTH-YY  PIC 99.  000018
00019 15 R-BIRTH-MM  PIC 99.  000019
00020 15 R-BIRTH-DD  PIC 99.  000020
00021 05 R-RACE  PIC 9.  000021
00022 05 R-SEX  PIC 9.  000022
00023 05 R-MED-RESOURCES  PIC XXX.  000023
00024 05 R-MULTI-RACE.  000024
00025 10 R-RACE-WHITE  PIC X.  000025
00026 10 R-RACE-AM-INDIAN  PIC X.  000026
00027 10 R-RACE-BLACK  PIC X.  000027
00028 10 R-RACE-HAWAIIAN  PIC X.  000028
00029 10 R-RACE-ASIAN  PIC X.  000029
00030 05 R-ETHNICITY  PIC X.  000030
00031 05 R-INELIG-ALIEN  PIC X.  000031
00032 05 R-MED-RES-DT  PIC X(8).  000032
00033 05 R-MED-SUSP-DATA.  000033
00034 10 R-RSN-CD  PIC X.  000034
00035 10 R-SUSP-START-DT.  000035
00036 15 R-SUSP-START-CC  PIC XX.  000036
00037 15 R-SUSP-START-YY  PIC XX.  000037
00038 15 R-SUSP-START-MM  PIC XX.  000038
00039 15 R-SUSP-START-DD  PIC XX.  000039
00040 10 R-SUSP-STOP-DT.  000040
00041 15 R-SUSP-STOP-CC  PIC XX.  000041
00042 15 R-SUSP-STOP-YY  PIC XX.  000042
00043 15 R-SUSP-STOP-MM  PIC XX.  000043

00124 02 WK-IH-OTH-DIAG-6  PIC X(7).  00530000
00124 02 WK-IH-OTH-DIAG-7  PIC X(7).  00540000
00124 02 WK-IH-OTH-DIAG-8  PIC X(7).  00550000
00124 02 WK-IH-PRIN-PROC  PIC X(7).  00560000
00124 02 WK-IH-OTH-PROC-1  PIC X(7).  00570000
00124 02 WK-IH-OTH-PROC-2  PIC X(7).  00580000
00124 02 WK-IH-OTH-PROC-3  PIC X(7).  00590000
00124 02 WK-IH-OTH-PROC-4  PIC X(7).  00600000
00124 02 WK-IH-OTH-PROC-5  PIC X(7).  00610000
15 R-SUSP-STOP-DD      PIC XX.    000044
10 R-BLOCK-START-DT.   000045
15 R-BLOCK-START-CC    PIC XX.    000046
15 R-BLOCK-START-YY    PIC XX.    000047
15 R-BLOCK-START-MM    PIC XX.    000048
15 R-BLOCK-START-DD    PIC XX.    000049
10 R-BLOCK-STOP-DT.    000050
15 R-BLOCK-STOP-CC     PIC XX.    000051
15 R-BLOCK-STOP-YY     PIC XX.    000052
15 R-BLOCK-STOP-MM     PIC XX.    000053
15 R-BLOCK-STOP-DD     PIC XX.    000054
00033  05  R-MBI    PIC X(11).   000055
  05  FILLER      PIC X.   000056
00034  05  R-CLAIM-NO.  000057
00035  10 R-CLAIM-1-9   PIC X(9).  000058
00036  10 R-CLAIM-10-11.   PIC X(9).  000059
00037  20 R-CLAIM-10    PIC X.   000060
00038  20 R-CLAIM-11    PIC X.   000061
00039  10 R-CLAIM-12    PIC X.   000062
00040  05  R-SOC-SEC-NO  PIC 9(9).   000063
00041  05  R-SSN-STATUS-CODE PIC 9.   000064
00042  05  R-KINSHIP-CODE  PIC XXX.   000065
00043  05  R-CURRENT-COVERAGE.  000066
00044  10 R-COV-BEGIN-X.  000067
00045  15 R-COV-BEGIN-CC  PIC 99.   000068
00046  15 R-COV-BEGIN.  000069
00047  20 R-COV-BEGIN-YYMM.  000070
00048  25 R-COV-BEGIN-YY  PIC 99.   000071
00049  25 R-COV-BEGIN-MM  PIC 99.   000072
00050  20 R-COV-BEGIN-DD  PIC 99.   000073
00051  10 R-COV-END-X.   000074
00052  15 R-COV-END-CC  PIC 99.   000075
00053  15 R-COV-END.   000076
00054  20 R-COV-END-YYMM.  000077
00055  25 R-COV-END-YY  PIC 99.   000078
00056  25 R-COV-END-MM  PIC 99.   000079
00057  20 R-COV-END-DD  PIC 99.   000080
00058  10 R-CANCL-RSN    PIC XX.   000081
00059  05  R-1ST-PR-COVERAGE.  000082
00060  10 R-1ST-PR-BEGIN-X.  000083
00061  15 R-1ST-PR-BEGIN-CC  PIC 99.   000084
00062  15 R-1ST-PR-BEGIN.  000085
00063  20 R-1ST-PR-BEGIN-YYMM.  000086
00064  25 R-1ST-PR-BEGIN-YY  PIC 99.   000087
00065  25 R-1ST-PR-BEGIN-MM  PIC 99.   000088
00066  20 R-1ST-PR-BEGIN-DD  PIC 99.   000089
00067  10 R-1ST-PR-END-X.  000090
00068  15 R-1ST-PR-END-CC  PIC 99.   000091
00069  15 R-1ST-PR-END.  000092
00070  20 R-1ST-PR-END-YYMM.  000093
00071  25 R-1ST-PR-END-YY  PIC 99.   000094
00072  25 R-1ST-PR-END-MM  PIC 99.   000095
00073  20 R-1ST-PR-END-DD  PIC 99.   000096
00074  10 R-1ST-PR-CANCL-RSN  PIC XX.   000097
00075  10 R-1ST-PR-AID-CAT PIC 99.   000098
00076  05  R-2ND-PR-COVERAGE.  000099
30

00244  10 R-DUP-RECIP-ID-2  PIC X(9).  000268
00245  10 R-DUP-RECIP-ID-3  PIC X(9).  000269
00246  10 R-DUP-RECIP-ID-4  PIC X(9).  000270
00247  10 R-DUP-RECIP-ID-5  PIC X(9).  000271
00248  05 R-IHS-IND    PIC X.  000272
00249  05 FILLER     PIC XX.  000273

Provider Layout

00100  01 NEW-PROV-REC.  00010000
001500  02 PROVIDER-RECORD.  00190000
001600  05 P-PROVIDER.  00200000
001700  10 P-SPECIALTY.  00210000
001800  15 P-TYPE    PIC 99.  00220000
001900  15 FILLER    PIC 9.  00230000
002000  10 P-RANGE    PIC 999.  00240000
002100  10 P-LOCATION     PIC 9.  00250000
002200  05 FILLER    PIC X(10).  00260000
002300  05 P-NCPDP-NO  PIC X(20).  00270000
002400  05 P-DEA-NO   PIC X(20).  00280000
002500  05 P-NAME1    PIC X(30).  00290000
002600  05 P-ALPHA-NAME PIC X(30).  00300000
002700  05 P-ADMIN-NAME PIC X(24).  00310000
002800  05 P-ELIGIBILITY.  00320000
002900  10 P-CURRENT.  00330000
003000  15 P-BEGIN-DTE.  00340000
003100  20 P-BEGIN-CC    PIC 99.  00350000
003200  20 P-BEGIN-DT.  00360000
003300  25 P-BEGIN-YY    PIC 99.  00370000
003400  25 P-BEGIN-MM    PIC 99.  00380000
003500  25 P-BEGIN-DD    PIC 99.  00390000
003600  15 P-END-DTE.  00400000
003700  20 P-END-CC    PIC 99.  00410000
003800  20 P-END-DT.  00420000
003900  25 P-END-YY    PIC 99.  00430000
004000  25 P-END-MM    PIC 99.  00440000
004100  25 P-END-DD    PIC 99.  00450000
004200  15 P-CANCEL PIC 99.  00460000
004300  10 P-1ST-PRIOR.  00470000
004400  15 P-1BEGIN-DTE.  00480000
004500  20 P-1BEGIN-CC    PIC 99.  00490000
004600  20 P-1BEGIN-DT.  00500000
004700  25 P-1BEGIN-YY    PIC 99.  00510000
004800  25 P-1BEGIN-MM    PIC 99.  00520000
004900  25 P-1BEGIN-DD    PIC 99.  00530000
005000  15 P-1END-DTE.  00540000
005100  20 P-1END-CC    PIC 99.  00550000
005200  20 P-1END-DT.  00560000
005300  25 P-1END-YY    PIC 99.  00570000
005400  25 P-1END-MM    PIC 99.  00580000
005500  25 P-1END-DD    PIC 99.  00590000
005600  15 P-1CANCEL PIC 99.  00600000
005700  10 P-2ND-PRIOR.  00610000
005800  15 P-2BEGIN-DTE.  00620000
005900  20 P-2BEGIN-CC PIC 99.  00630000

30
<table>
<thead>
<tr>
<th>Line No.</th>
<th>Field Description</th>
<th>Field Type</th>
<th>Field Length</th>
<th>Field Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>006000</td>
<td>20 P-2BEGIN-DT.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>006400</td>
<td>15 P-2END-DTE.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>006500</td>
<td>20 P-2END-CC</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>006600</td>
<td>20 P-2END-DT.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>007000</td>
<td>15 P-2CANCEL</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>007100</td>
<td>05 P-ELIGIBILITY-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>007200</td>
<td>10 P-3RD-PRIOR.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>007300</td>
<td>15 P-3BEGIN-DTE.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>007400</td>
<td>20 P-3BEGIN-CC</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>007500</td>
<td>20 P-3BEGIN-DT.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>007600</td>
<td>25 P-3BEGIN-YY</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>007700</td>
<td>25 P-3BEGIN-MM</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>007800</td>
<td>25 P-3BEGIN-DD</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>007900</td>
<td>15 P-3END-DTE.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008000</td>
<td>20 P-3END-CC</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008100</td>
<td>20 P-3END-DT.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008200</td>
<td>25 P-3END-YY</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008300</td>
<td>25 P-3END-MM</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008400</td>
<td>25 P-3END-DD</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008500</td>
<td>15 P-3CANCEL</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008600</td>
<td>10 P-4TH-PRIOR.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008700</td>
<td>15 P-4BEGIN-DTE.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008800</td>
<td>20 P-4BEGIN-CC</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008900</td>
<td>20 P-4BEGIN-DT.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>009100</td>
<td>25 P-4BEGIN-MM</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>009300</td>
<td>15 P-4END-DTE.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>009400</td>
<td>20 P-4END-CC</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>009500</td>
<td>20 P-4END-DT.</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>009600</td>
<td>25 P-4END-YY</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>009700</td>
<td>25 P-4END-MM</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>009900</td>
<td>15 P-4CANCEL</td>
<td>PIC 99.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>010000</td>
<td>05 P-CURRENT-YTD-AMTS.</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01040000</td>
<td></td>
</tr>
<tr>
<td>010100</td>
<td>10 P-YTD-TOTAL-PD</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01050000</td>
<td></td>
</tr>
<tr>
<td>010200</td>
<td>10 P-YTD-RETD-RECOV</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01060000</td>
<td></td>
</tr>
<tr>
<td>010300</td>
<td>10 P-YTD-NEG-BAL</td>
<td>PIC S9(7)V99 COMP-3.</td>
<td>01070000</td>
<td></td>
</tr>
<tr>
<td>010400</td>
<td>05 P-PRIOR-YR-AMTS.</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01080000</td>
<td></td>
</tr>
<tr>
<td>010500</td>
<td>10 P-PYR-TOTAL-PD</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01090000</td>
<td></td>
</tr>
<tr>
<td>010600</td>
<td>10 P-PYR-RETD-RECOV</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01100000</td>
<td></td>
</tr>
<tr>
<td>010700</td>
<td>10 P-PYR-NEG-BAL</td>
<td>PIC S9(7)V99 COMP-3.</td>
<td>01110000</td>
<td></td>
</tr>
<tr>
<td>010800</td>
<td>05 P-PRIOR2-YR-AMTS.</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01120000</td>
<td></td>
</tr>
<tr>
<td>010900</td>
<td>10 P-PYR2-TOTAL-PD</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01130000</td>
<td></td>
</tr>
<tr>
<td>011000</td>
<td>10 P-PYR2-RETD-RECOV</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01140000</td>
<td></td>
</tr>
<tr>
<td>011100</td>
<td>10 P-PYR2-NEG-BAL</td>
<td>PIC S9(7)V99 COMP-3.</td>
<td>01150000</td>
<td></td>
</tr>
<tr>
<td>011200</td>
<td>05 P-PRIOR3-YR-AMTS.</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01160000</td>
<td></td>
</tr>
<tr>
<td>011300</td>
<td>10 P-PYR3-TOTAL-PD</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01170000</td>
<td></td>
</tr>
<tr>
<td>011400</td>
<td>10 P-PYR3-RETD-RECOV</td>
<td>PIC S9(9)V99 COMP-3.</td>
<td>01180000</td>
<td></td>
</tr>
<tr>
<td>011500</td>
<td>10 P-PYR3-NEG-BAL</td>
<td>PIC S9(7)V99 COMP-3.</td>
<td>01190000</td>
<td></td>
</tr>
</tbody>
</table>
017200  15  P-HH-PART-START-MM  PIC 99. 01760000
017300  15  P-HH-PART-START-DD  PIC 99. 01770000
017400   05 P-HH-PART-STOP-DATE. 01780000
017500  10  P-HH-PART-STOP-CC  PIC 99. 01790000
017600  10  P-HH-PART-STOP-DTE. 01800000
017700  15  P-HH-PART-STOP-YY  PIC 99. 01810000
017800  15  P-HH-PART-STOP-MM  PIC 99. 01820000
017900  15  P-HH-PART-STOP-DD  PIC 99. 01830000
018000   05 P-HH-PREFERENCE-CODE  PIC X(01). 01840000
018100   05 P-HH-PREF-START-DATE. 01850000
018200  10  P-HH-PREF-START-CC  PIC 99. 01860000
018300  10  P-HH-PREF-START-DTE. 01870000
018400  15  P-HH-PREF-START-YY  PIC 99. 01880000
018500  15  P-HH-PREF-START-MM  PIC 99. 01890000
018600  15  P-HH-PREF-START-DD  PIC 99. 01900000
018700   05 P-HH-PREF-STOP-DATE. 01910000
018800  10  P-HH-PREF-STOP-CC  PIC 99. 01920000
018900  10  P-HH-PREF-STOP-DTE. 01930000
019000  15  P-HH-PREF-STOP-YY  PIC 99. 01940000
019100  15  P-HH-PREF-STOP-MM  PIC 99. 01950000
019200  15  P-HH-PREF-STOP-DD  PIC 99. 01960000
019300   05 P-HH-CLINIC-ID  PIC X(04). 01970000
019400   05 P-HIPAA-ADD-PAY  PIC S9(7)V99 COMP-3. 01980000
019500   05 P-HIPAA-RETD-REV  PIC S9(7)V99 COMP-3. 01990000
019600    05 FILLER  PIC X(9). 02000000
019700    05 P-BIRTH-3  PIC X(1). 02010000
019800    05 P-RATES. 02020000
019900  10 P-PERCENT OCCURS 5 TIMES. 02030000
020000  15 P-PERCENT-RATE  PIC S999V99 COMP-3. 02040000
020100   15 P-PERCENT-DTE. 02050000
020200  20 P-PERCENT-CC  PIC 99. 02060000
020300   20 P-PERCENT-DATE. 02070000
020400  25 P-PERCENT-YY  PIC 99. 02080000
020500  25 P-PERCENT-MM  PIC 99. 02090000
020600  25 P-PERCENT-DD  PIC 99. 02100000
020700  10 P-PER-DIEM OCCURS 5 TIMES. 02110000
020800  15 P-PER-DIEM-RATE  PIC S999V99 COMP-3. 02120000
020900  15 P-PER-DIEM-DTE. 02130000
021000  20 P-PER-DIEM-CC  PIC 99. 02140000
021100  20 P-PER-DIEM-DATE. 02150000
021200  25 P-PER-DIEM-YY  PIC 99. 02160000
021300  25 P-PER-DIEM-MM  PIC 99. 02170000
021400  25 P-PER-DIEM-DD  PIC 99. 02180000
021500  10 P-ICF OCCURS 5 TIMES. 02190000
021600  15 P-ICF-RATE  PIC S999V99 COMP-3. 02200000
021700  15 P-ICF-DTE. 02210000
021800  20 P-ICF-CC  PIC 99. 02220000
021900  20 P-ICF-DATE. 02230000
022000  25 P-ICF-YY  PIC 99. 02240000
022100  25 P-ICF-MM  PIC 99. 02250000
022200  25 P-ICF-DD  PIC 99. 02260000
022300  10 P-SNF OCCURS 5 TIMES. 02270000
022400  15 P-SNF-RATE  PIC S999V99 COMP-3. 02280000
022500  15 P-SNF-DTE. 02290000
022600  20 P-SNF-CC  PIC 99. 02300000
022700  20 P-SNF-DATE. 02310000
023100  10  P-DISPENSING OCCURS 5 TIMES.  
023200  15  P-DISPENSING-FEE    PIC S999V99  COMP-3.  
023300  15  P-DISPENSING-DTE.  
023400  20  P-DISPENSING-CC    PIC 99.  
023500  20  P-DISPENSING-DATE.  
023900  10  P-PACKAGING OCCURS 5 TIMES.  
024100  15  P-PACK-DTE.  
024200  20  P-PACK-CC    PIC 99.  
024300  20  P-PACK-DATE.  
024700  05  P-DRG-RATES.  
024800  10  P-TARGET OCCURS 5 TIMES.  
024900  15  P-TARGET-AMT    PIC S9(5)  COMP-3.  0  
025000  15  P-TARGET-DTE.  
025100  20  P-TARGET-CC    PIC 99.  
025200  20  P-TARGET-DATE.  
025600  10  P-CAPITAL OCCURS 5 TIMES.  
025700  15  P-CAPITAL-COSTS    PIC S9(5)  COMP-3.  
025800  15  P-CAPITAL-DTE.  
025900  20  P-CAPITAL-CC    PIC 99.  
026000  20  P-CAPITAL-DATE.  
026400  05  P-CURRENT-ADD-PAY.  
026600  10  P-CURR-RETD-REVR     PIC S9(7)V99  COMP-3.  
026700  10  P-AP-CCYY.  
026800  15  P-AP-CENTURY    PIC XX.  
026900  15  P-AP-YEAR    PIC XX.  
027000  10  P-AP-RSN-CODE    PIC XX.  
027100  10  P-BAC.  
027200  15  P-PATIENT    PIC X(4).  
027300  15  P-ACCOUNT    PIC X(8).  
027400  15  P-CENTER.  
027500  20  FILLER    PIC X(7).  
027600  20  P-FD-IND     PIC X(5).  
027700  10  P-FED    PIC X(4).  
027800  05  FILLER    PIC X(06).  
027900  05  P-DENTAL-PROV    PIC X(14).  
028000  05  P-SUPPLY-ID    PIC X(10).  
028100  05  P-SUPPLY-ID2    PIC X(7).  
028200  05  P-SURG-CAT    PIC X.  
028300  05  P-IHS-CONTRACT    PIC X.  
02840000
028400 05  FILLER   PIC X(3). 02880000
028500 05  P-LAST-REMIT-DTE. 02890000
028600 10  P-LAST-REMIT-CC  PIC 99. 02900000
028700 10  P-LAST-REMIT-DT. 02910000
028800 15  P-LAST-REMIT-YY  PIC 99. 02920000
028900 15  P-LAST-REMIT-MM  PIC 99. 02930000
029000 15  P-LAST-REMIT-DD  PIC 99. 02940000
029100 05  P-YEAR-BUDGET-AMT  PIC S9(9)V99 COMP-3. 02950000
029200 05  P-FISCAL-YR-END. 02960000
029300 10  P-FY-MM  PIC 99. 02970000
029400 10  P-FY-DD  PIC 99. 02980000
029500 05  P-2ND-SPECIALTY  PIC 999. 03000000
029600 05  P-3RD-SPECIALTY  PIC 999. 03010000
029700 05  P-IRS-NUMBER  PIC 9(9). 03020000
029800 05  P-IRS-NAME  PIC X(31). 03030000
029900 05  FILLER  PIC X(3). 03040000
030000 05  P-1099-IND  PIC X. 03050000
030100 05  FILLER  PIC X(5). 03060000
030200 05  P-LICENSE-NO  PIC X(6). 03070000
030300 05  P-FAC-IND  PIC X. 03080000
030400 05  FILLER  PIC X(10). 03090000
030500 05  P-UPIN  PIC X(6). 03100000
030600 05  P-CATEGORIES-OF-SERVICE. 03110000
030700 10  P-CAT-OF-SERV OCCURS 5 TIMES  PIC 99. 03120000
030800 10  FILLER  PIC X(10). 03130000
030900 05  P-SIA-ADD-DATA OCCURS 2 TIMES. 03140000
031000 10  P-SIA-ADD-ON  PIC S9(4)V99. 03150000
031100 10  P-SIA-EFF-DTE. 03160000
031200 20  P-SIA-CC  PIC 99. 03170000
031300 20  P-SIA-DATE. 03180000
031400 25  P-SIA-YY  PIC 99. 03190000
031500 25  P-SIA-MM  PIC 99. 03200000
031600 25  P-SIA-DD  PIC 99. 03210000
031700* 05  FILLER  PIC X(60). 03220000
031800* 05  FILLER  PIC X(32). 03230000
031900* 05  P-MEDICARE-NUMBERS. 03240000
032000* 10  P-MED-NO OCCURS 10 TIMES  PIC X(6). 03250000
032100 05  P-NUMBER-OF-BEDS  PIC 9(5). 03260000
032200 05  P-LICENSE-DT. 03270000
032300 10  P-LIC-CC  PIC XX. 03280000
032400 10  P-LIC-YY  PIC XX. 03290000
032500 10  P-LIC-MM  PIC XX. 03300000
032600 10  P-LIC-DD  PIC XX. 03310000
032700 05  FILLER  PIC X. 03320000
032800 05  P-EXCEPTION-IND  PIC X. 03330000
032900 05  P-SORT-PREFERENCE  PIC X. 03340000
033000 05  P-CLASS-TYPE  PIC 99. 03350000
033100 05  P-EFT-ABA-NO  PIC 9(9). 03360000
033200 05  P-EFT-ACCT-NO  PIC X(17). 03370000
033300 05  P-EFT-ACCT-TYPE  PIC X. 03380000
033400 05  P-EFT-IND  PIC X. 03390000
033500 05  P-EFT-EFFECT-DTE. 03400000
033600 10  P-EFT-EFFECT-CENTURY  PIC 99. 03410000
033700 10  P-EFT-EFFECT-DATE  PIC 9(6). 03420000
033800 10  P-EFT-EFFECT-RE REDEFINES P-EFT-EFFECT-DATE 03430000
033900 15  P-EFT-EFFECT-YR  PIC XX. 03440000

35
034000 15 P-EFT-EFFECT-MM PIC XX. 03440000
034100 15 P-EFT-EFFECT-DD PIC XX. 03450000
034200 05 FILLER PIC X(20). 03460000
034300 05 P-LAST-ACTIVITY-INFO. 03470000
034400 10 P-LAST-ACTIVITY-DTE. 03480000
034500 15 P-LAST-ACTIVITY-CC PIC 99. 03490000
034600 15 P-LAST-ACTIVITY-DATE. 03500000
034700 20 P-LAST-ACTIVITY-YY PIC 99. 03510000
034800 20 P-LAST-ACTIVITY-MM PIC 99. 03520000
034900 20 P-LAST-ACTIVITY-DD PIC 99. 03530000
035500 10 P-ENTRY-TIME PIC 9(7) COMP-3. 03540000
035100 10 P-TRAN-ID PIC XXX. 03550000
035200 10 P-OPER-ID PIC XXX. 03560000
035300 10 P-TERM-ID PIC X(4). 03570000
035400 05 P-ADDRESS-AREA. 03580000
035500 10 FILLER PIC X. 03590000
035600 10 P-ADDRESSES. 03600000
035700 15 P-ADDR-SV. 03610000
035800 20 P-ATTN-LN-SV PIC X(30). 03620000
035900 20 P-ADDR-LN1-SV PIC X(30). 03630000
036000 20 FILLER PIC X(30). 03640000
036100 20 P-ADDR-LN3-SV PIC X(30). 03650000
036200 25 P-CITY-SV PIC X(20). 03660000
036300 25 P-STATE-SV PIC XX. 03670000
036400 25 P-ZIP-SV PIC 999. 03680000
036500 30 P-ZIP-SV-5 PIC 9(5). 03690000
036600 30 P-ZIP-SV-4 PIC 9(4). 03700000
036700 20 P-PHONE-SV PIC 999. 03710000
036800 25 P-PH-SV-AREA PIC 999. 03720000
036900 25 P-PH-SV-3 PIC 999. 03730000
037000 25 P-PH-SV-4 PIC 9(4). 03740000
037100 20 P-CITY-COUNTY PIC 999. 03750000
037200 15 P-ADDR-PAYTO. 03760000
037300 20 P-ATTN-LN-PAYTO PIC X(30). 03770000
037400 20 P-ADDR-LN1-PAYTO PIC X(30). 03780000
037500 20 FILLER PIC X(30). 03790000
037600 20 P-ADDR-LN3-PAYTO PIC X(30). 03800000
037700 25 P-CITY-PAYTO PIC X(20). 03810000
037800 25 P-STATE-PAYTO PIC XX. 03820000
037900 25 P-ZIP-PAYTO PIC 999. 03830000
038000 30 P-ZIP-PAYTO-5 PIC 9(5). 03840000
038100 30 P-ZIP-PAYTO-4 PIC 9(4). 03850000
038200 20 P-PAYTO-COUNTY PIC 999. 03860000
038300 20 P-PHONE-PAYTO PIC 999. 03870000
038400 25 P-PH-PAY-AREA PIC 999. 03880000
038500 25 P-PH-PAY-3 PIC 999. 03890000
038600 25 P-PH-PAY-4 PIC 9(4). 03900000
038700 05 P-AGREE-IND PIC X(4). 03910000
038800 05 P-EMC-IND PIC X. 03920000
038900 05 P-EMC-EFF-DTE PIC 999. 03930000
039000 10 P-EMC-EFF-CENTURY PIC 999. 03940000
039100 10 P-EMC-EFF-DATE PIC 9(6). 03950000
039200 10 P-EMC-EFF-RE REDEFINES P-EMC-EFF-DATE. 03960000
039300 15 P-EMC-EFF-YR PIC XX. 03970000
039400 15 P-EMC-EFF-MM PIC XX. 03980000
039500 15 P-EMC-EFF-DD PIC XX. 03990000
<table>
<thead>
<tr>
<th>Line No.</th>
<th>Description</th>
<th>PIC Code</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>039600</td>
<td>05 P-ELEC-REMIT</td>
<td>X.</td>
<td>04000000</td>
</tr>
<tr>
<td>039700</td>
<td>05 P-ELEC-REMIT-DT.</td>
<td></td>
<td>04010000</td>
</tr>
<tr>
<td>039800</td>
<td>10 P-ELEC-RMT-CC</td>
<td>XX.</td>
<td>04020000</td>
</tr>
<tr>
<td>039900</td>
<td>10 P-ELEC-RMT-YY</td>
<td>XX.</td>
<td>04030000</td>
</tr>
<tr>
<td>040000</td>
<td>10 P-ELEC-RMT-MM</td>
<td>XX.</td>
<td>04040000</td>
</tr>
<tr>
<td>040100</td>
<td>10 P-ELEC-RMT-DD</td>
<td>XX.</td>
<td>04050000</td>
</tr>
<tr>
<td>040200</td>
<td>05 P-PAPER-REMIT</td>
<td>X.</td>
<td>04060000</td>
</tr>
<tr>
<td>040300</td>
<td>05 P-PAPER-REMIT-DT.</td>
<td></td>
<td>04070000</td>
</tr>
<tr>
<td>040400</td>
<td>10 P-PAPER-RMT-CC</td>
<td>XX.</td>
<td>04080000</td>
</tr>
<tr>
<td>040500</td>
<td>10 P-PAPER-RMT-YY</td>
<td>XX.</td>
<td>04090000</td>
</tr>
<tr>
<td>040600</td>
<td>10 P-PAPER-RMT-MM</td>
<td>XX.</td>
<td>04100000</td>
</tr>
<tr>
<td>040700</td>
<td>10 P-PAPER-RMT-DD</td>
<td>XX.</td>
<td>04110000</td>
</tr>
<tr>
<td>040800</td>
<td>05 P-XOVR-ONLY</td>
<td>X.</td>
<td>04120000</td>
</tr>
<tr>
<td>040900</td>
<td>05 P-277-UNSOL</td>
<td>X.</td>
<td>04130000</td>
</tr>
<tr>
<td>041000</td>
<td>05 P-277-EFF-DT.</td>
<td></td>
<td>04140000</td>
</tr>
<tr>
<td>041100</td>
<td>10 P-277-EFF-CC</td>
<td>XX.</td>
<td>04150000</td>
</tr>
<tr>
<td>041200</td>
<td>10 P-277-EFF-YY</td>
<td>XX.</td>
<td>04160000</td>
</tr>
<tr>
<td>041300</td>
<td>10 P-277-EFF-MM</td>
<td>XX.</td>
<td>04170000</td>
</tr>
<tr>
<td>041400</td>
<td>10 P-277-EFF-DD</td>
<td>XX.</td>
<td>04180000</td>
</tr>
<tr>
<td>041500</td>
<td>05 P-MC-CLINIC</td>
<td>X(4).</td>
<td>04190000</td>
</tr>
<tr>
<td>041600</td>
<td>05 P-ADD-DATE.</td>
<td></td>
<td>04200000</td>
</tr>
<tr>
<td>041700</td>
<td>10 P-ADD-CC</td>
<td>XX.</td>
<td>04210000</td>
</tr>
<tr>
<td>041800</td>
<td>10 P-ADD-YY</td>
<td>XX.</td>
<td>04220000</td>
</tr>
<tr>
<td>041900</td>
<td>10 P-ADD-MM</td>
<td>XX.</td>
<td>04230000</td>
</tr>
<tr>
<td>042000</td>
<td>10 P-ADD-DD</td>
<td>XX.</td>
<td>04240000</td>
</tr>
<tr>
<td>042100</td>
<td>05 P-EHR-PGM-IND</td>
<td>X(01).</td>
<td>04250000</td>
</tr>
<tr>
<td>042200</td>
<td>05 P-EHR-DATA</td>
<td>OCCURS 6 TIMES.</td>
<td>04260000</td>
</tr>
<tr>
<td>042300</td>
<td>10 P-EHR-PART-YEAR</td>
<td>9(01).</td>
<td>04270000</td>
</tr>
<tr>
<td>042400</td>
<td>10 P-EHR-PMT-DTE.</td>
<td></td>
<td>04280000</td>
</tr>
<tr>
<td>042500</td>
<td>15 P-EHR-PMT-CC</td>
<td>99.</td>
<td>04290000</td>
</tr>
<tr>
<td>042600</td>
<td>15 P-EHR-PMT-DATE.</td>
<td></td>
<td>04300000</td>
</tr>
<tr>
<td>042700</td>
<td>20 P-EHR-PMT-YY</td>
<td>99.</td>
<td>04310000</td>
</tr>
<tr>
<td>042800</td>
<td>20 P-EHR-PMT-MM</td>
<td>99.</td>
<td>04320000</td>
</tr>
<tr>
<td>042900</td>
<td>20 P-EHR-PMT-DD</td>
<td>99.</td>
<td>04330000</td>
</tr>
<tr>
<td>043000</td>
<td>10 P-EHR-PMT-AMT</td>
<td>S9(13)V99.</td>
<td>04340000</td>
</tr>
<tr>
<td>043100</td>
<td>05 P-IHS-INDICATOR-DATA</td>
<td>OCCURS 3 TIMES.</td>
<td>04350000</td>
</tr>
<tr>
<td>043200</td>
<td>10 P-IHS-INDICATOR</td>
<td>X.</td>
<td>04360000</td>
</tr>
<tr>
<td>043300</td>
<td>10 P-IHS-IND-BEG-DTE.</td>
<td></td>
<td>04370000</td>
</tr>
<tr>
<td>043400</td>
<td>20 P-IHS-IND-BEG-CC</td>
<td>99.</td>
<td>04380000</td>
</tr>
<tr>
<td>043500</td>
<td>20 P-IHS-IND-BEG-DATE.</td>
<td></td>
<td>04390000</td>
</tr>
<tr>
<td>043600</td>
<td>25 P-IHS-IND-BEG-YY</td>
<td>99.</td>
<td>04400000</td>
</tr>
<tr>
<td>043700</td>
<td>25 P-IHS-IND-BEG-MM</td>
<td>99.</td>
<td>04410000</td>
</tr>
<tr>
<td>043800</td>
<td>25 P-IHS-IND-BEG-DD</td>
<td>99.</td>
<td>04420000</td>
</tr>
<tr>
<td>043900</td>
<td>10 P-IHS-IND-END-DTE.</td>
<td></td>
<td>04430000</td>
</tr>
<tr>
<td>044000</td>
<td>20 P-IHS-IND-END-CC</td>
<td>99.</td>
<td>04440000</td>
</tr>
<tr>
<td>044100</td>
<td>20 P-IHS-IND-END-DATE.</td>
<td></td>
<td>04450000</td>
</tr>
<tr>
<td>044200</td>
<td>25 P-IHS-IND-END-YY</td>
<td>99.</td>
<td>04460000</td>
</tr>
<tr>
<td>044300</td>
<td>25 P-IHS-IND-END-MM</td>
<td>99.</td>
<td>04470000</td>
</tr>
<tr>
<td>044400</td>
<td>25 P-IHS-IND-END-DD</td>
<td>99.</td>
<td>04480000</td>
</tr>
<tr>
<td>044500</td>
<td>05 FILLER</td>
<td>X(631).</td>
<td>04490000</td>
</tr>
<tr>
<td>044600</td>
<td>05 FILLER</td>
<td>X(682).</td>
<td>04500000</td>
</tr>
<tr>
<td>044700</td>
<td>05 P-DISP-FEE</td>
<td>S9(9)V99. COMP-3.</td>
<td>04510000</td>
</tr>
<tr>
<td>044800</td>
<td>05 P-REQ-PAY-IND</td>
<td>X.</td>
<td>04520000</td>
</tr>
<tr>
<td>044900</td>
<td>05 P-REQ-PAY-DTE.</td>
<td></td>
<td>04530000</td>
</tr>
<tr>
<td>045000</td>
<td>10 P-REQ-PAY-CENTURY</td>
<td>99.</td>
<td>04540000</td>
</tr>
<tr>
<td>045100</td>
<td>10 P-REQ-PAY-DATE</td>
<td>9(6).</td>
<td>04550000</td>
</tr>
</tbody>
</table>
045200  10  P-REQ-PAY-RE REDEFINES P-REQ-PAY-DATE.  04560000
045300   15  P-REQ-PAY-YR   PIC XX.   04570000
045400   15  P-REQ-PAY-MM   PIC XX.   04580000
045500   15  P-REQ-PAY-DD   PIC XX.   04590000
045600   05  P-REMT-PAY-IND PIC X.   04600000
045700   05  P-REMT-PAY-DTE.   04610000
045800  10  P-REMT-PAY-CENTURY  PIC 99. 04620000
045900  10  P-REMT-PAY-DTE.   04630000
046000  10  P-REMT-PAY-RE REDEFINES P-REMT-PAY-DATE.  04640000
046100   15  P-REMT-PAY-YR  PIC XX.   04650000
046200   15  P-REMT-PAY-MM   PIC XX.   04660000
046300   15  P-REMT-PAY-DD   PIC XX.   04670000
046400  05  P-PCP-START-DATE.   04680000
046500  10  P-PCP-START-CENTURY  PIC 99. 04690000
046600  10  P-PCP-START-DT.   04700000
046700   15  P-PCP-START-YY  PIC 99. 04710000
046800   15  P-PCP-START-MM   PIC 99. 04720000
046900   15  P-PCP-START-DD   PIC 99. 04730000
047000  05  P-PCP-END-DATE.   04740000
047100  10  P-PCP-END-CENTURY  PIC 99. 04750000
047200  10  P-PCP-END-DT.   04760000
047300   15  P-PCP-END-YY   PIC 99. 04770000
047400   15  P-PCP-END-MM    PIC 99. 04780000
047500   15  P-PCP-END-DD    PIC 99. 04790000
047600  05  P-PCP-CODE    PIC X.  04800000
047700  05  P-PREPCP-START-DATE.   04810000
047800  10  P-PREPCP-START-CENTURY  PIC 99. 04820000
047900  10  P-PREPCP-START-DT.   04830000
048000   15  P-PREPCP-START-YY  PIC 99. 04840000
048100   15  P-PREPCP-START-MM   PIC 99. 04850000
048200   15  P-PREPCP-START-DD   PIC 99. 04860000
048300  05  P-PREPCP-END-DATE.   04870000
048400  10  P-PREPCP-END-CENTURY  PIC 99. 04880000
048500  10  P-PREPCP-END-DT.   04890000
048600   15  P-PREPCP-END-YY  PIC 99. 04900000
048700   15  P-PREPCP-END-MM    PIC 99. 04910000
048800   15  P-PREPCP-END-DD    PIC 99. 04920000
048900  05  P-PREPCP-CODE    PIC X.  04930000
049000   05  P-CLIA-NO PIC X(10).  04940000
049100   05  P-CLIA-NO2 PIC X(10).  04950000
049200   05  P-CLIA-NO3 PIC X(10).  04960000
049300   05  P-CLIA-NO4 PIC X(10).  04970000
049400   05  P-CLIA-NO5 PIC X(10).  04980000
049500   05  P-ALT-1 PIC X(30).  04990000
049600  05  P-ALT-2 REDEFINES P-ALT-1.  05000000
049700  10  P-NPI-ALT-INDEX.  05010000
049800   15  P-SERVICING-NPI PIC X(10).  05020000
049900   15  P-BILLING-NPI PIC X(10).  05030000
050000  10  FILLER PIC X(10).  05040000
050100  05  P-ALT-3 REDEFINES P-ALT-1.  05050000
050200  10  FILLER PIC X(10).  05060000
050300  10  P-NPI-ALT-INDEX2.  05070000
050400   15  P-BILLING-NPI2 PIC X(10).  05080000
050500   15  P-SERVICING-NPI2 PIC X(10).  05090000
050600   05  FILLER PIC X(08).  05100000
050700  05  P-NPI-REQ PIC X.  05110000
Please return agreement to your BIT Manager or Designated BIT Contact

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

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


Acknowledgement: State of South Dakota Information Technology Security Policy

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

__________________________   ________
Employee or Contractor signature    Date

__________________________   ________
BIT Manager or Contact    Date

Employee or Contractor name and Company name in block capital letters
Information Technology
Security Policy

CONTRACTOR
v 3.1

June 1, 2018
General - Information Technology Security Policy - Introduction ................................................................. 8
  1.1.4.1. General ................................................................................................................................. 14
  1.1.4.2. Chief Information Security Officer .................................................................................. 14
  1.1.4.3. Security Infrastructure Team (SIT) .................................................................................. 15
  1.1.4.4. Security Operations Team (SOT) .................................................................................... 15
  1.1.4.5. BIT Executive Working Group on Cyber Security ............................................................ 15

Administrative - I/T Asset Protection - Background Checks ................................................................. 15
  10.1.4.1. Background Checks ......................................................................................................... 16
  10.1.4.2. Disqualifying Criteria ....................................................................................................... 17
  10.1.4.3. Noncriminal Agency Coordinator (NAC) ...................................................................... 17
  10.1.4.4. Local Agency Security Officer (LASO) ........................................................................... 17
  10.1.4.5. Background Check Interpretation ..................................................................................... 17
  10.1.4.6. Not Guilty Presumption .................................................................................................... 18
  10.1.4.7. Background Check Information Challenge ........................................................................ 18
  10.1.4.8. Corrective Action .............................................................................................................. 18
  10.1.4.9. Training ................................................................................................................................ 18
  10.1.4.10. Emailing Background Check Information ........................................................................... 18

Administrative - I/T Asset Protection - Confidentiality ........................................................................... 18
  10.3.4.1. Confidentiality Agreement ............................................................................................... 19
  10.3.4.2. Security Acknowledgement and Access ........................................................................... 20

Mainframe - Mainframe Security - Overview ......................................................................................... 20
  210.1.4.1. Security of Mainframe Resources .................................................................................. 21
  210.1.4.2. Mainframe Access Granted by Business Need ............................................................. 21
  210.1.4.3. Requesting Mainframe System Access .......................................................................... 21
  210.1.4.4. Mainframe Resource Examples ....................................................................................... 21

Mainframe - Mainframe Security - Mainframe Accounts ................................................................. 21
  210.3.4.1. Unique Account Requirement ....................................................................................... 22
  210.3.4.2. Requests for Mainframe User IDs ...................................................................................... 22
  210.3.4.3. Responsibility Mainframe User IDs and Passwords .......................................................... 22
  210.3.4.4. Department Security Officers ........................................................................................ 22

Mainframe - Mainframe Security - Mainframe Accounts ................................................................. 23
  210.4.4.1. Mainframe User ID Revocation ....................................................................................... 23

Mainframe - Mainframe Security - Disposition of Mainframe Output and Documentation ................. 23
  210.20.4.1. Agency Defined Access to Output .................................................................................. 24
  210.20.4.2. Mainframe Documentation ........................................................................................... 24

Mainframe - Mainframe Security - Mainframe Access ........................................................................... 24
  210.25.3.1. Scope Assumptions ......................................................................................................... 24
  210.25.3.2. Scope Constraints ........................................................................................................... 25
  210.25.4.1. Mainframe Access .......................................................................................................... 25
Server-Server Security-Server Maintenance and Administration ......................................................... 25
  220.1.4.1. State Policies .................................................................................................................. 25
  220.1.5.1. Scope of Server Platforms ............................................................................................ 25
Server-Server Security-File Transfer Protocol .................................................................................... 26
  220.7.4.1. Use of File Transfer Protocol Server ............................................................................. 26
Server-Server Security-Assurance HIPAA Regulations are Met ......................................................... 27
  220.10.4.1. The Data User is Responsible for Adhering to HIPAA Regulations .............................. 27
Server-Server Security-Technical Asset Connections ........................................................................ 27
  220.11.4.1. Requirements for State Connected Devices ................................................................... 28
  220.11.4.2. Exemptions .................................................................................................................. 28
Network-Service-Domain Naming System ......................................................................................... 28
  220.13.4.1. South Dakota Agency Website Naming ......................................................................... 29
  220.13.4.2. Registering a Domain .................................................................................................. 29
Data Center General-Data Center Security-Cloud Based Services and System Information ................. 29
  230.9.4.1. Responsibility for Cloud Based Services and Systems ..................................................... 30
Data Center General-Secure Information Technology Acquisition Policy-Secure Information Technology Acquisition Policy .................................................................................................................... 30
  230.10.4.1. Hardware Maintenance Agreements .............................................................................. 31
Data Center General-Data Center Security-Federal Tax Information ................................................... 31
  230.11.4.1. Federal Tax Information Returns and Return Information ............................................. 32
  230.11.4.2. What is Not Federal Tax Information .............................................................................. 32
  230.11.4.3. Safeguarding Federal Tax Information .......................................................................... 33
  230.11.4.4. Emailing Federal Tax Information .................................................................................. 33
Data Center General-Technical Asset Connections-Domain ................................................................. 33
  230.52.4.1. Protection of External Devices ....................................................................................... 34
Data Center General-Operational-Change Control Process .................................................................. 34
  230.53.4.1. Assessment, Alerts, and Procedures .............................................................................. 34
  230.53.4.2. Routine and Scheduled Changes .................................................................................... 34
  230.53.4.3. Emergency Changes ...................................................................................................... 35
Data Center General-Procedural-Physical Access - Proximity Cards ...................................................... 35
  230.58.4.1. Proximity Card for Non-BIT Employee Access ................................................................. 36
Data Center General-Accountability-Authorization ............................................................................. 36
  230.65.4.1. Administrative Capabilities on Servers ......................................................................... 37
Data Center General-Data Center Security-Accounts Access Control and Authorization ......................... 37
  230.67.4.1. Individual Access Authorization ..................................................................................... 38
  230.67.4.2. Administrative Capabilities ............................................................................................ 38
  230.67.4.3. User Privilege Capabilities ............................................................................................. 38
  230.67.4.4. Least Privilege ................................................................................................................ 38
  230.67.4.5. Administrative Privileges .............................................................................................. 38
Security-Network Discovery-Probing-Exploiting ................................................................. 62
  620.1.4.1. Limiting Tool Functionality .................................................................................. 63
  620.1.4.2. Exploiting Security Controls of Information Systems ........................................ 63
  620.1.4.3. Cracking Application or Passwords ...................................................................... 63
  620.1.4.4. Exemptions ........................................................................................................... 63
Security-Content Control-Internet Filtering .......................................................................... 63
  620.5.4.1. Exemptions ........................................................................................................... 64
  620.5.4.2. Appropriate Use of Administrator Access .............................................................. 64
  620.5.4.3. DDN Content Filtering .......................................................................................... 65
  620.5.4.4. DDN Intranet Content Filtering ............................................................................ 65
  620.5.4.5. Filter Exemption Requests .................................................................................... 65
## ITSP Change Log

<table>
<thead>
<tr>
<th>Policy Number</th>
<th>Policy Title</th>
<th>New</th>
<th>Revised</th>
<th>Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.4.1</td>
<td>Background Checks</td>
<td></td>
<td>06.01.2018</td>
<td></td>
</tr>
<tr>
<td>230.67.4.2</td>
<td>User Privilege Capabilities</td>
<td></td>
<td>06.01.2018</td>
<td></td>
</tr>
<tr>
<td>230.74</td>
<td>Use of Production Data in a Non-Production Environment</td>
<td></td>
<td>06.01.2018</td>
<td></td>
</tr>
</tbody>
</table>
General-Information Technology Security Policy-Introduction

1.1.1. Overview

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

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

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

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

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

Information Technology Security is based on three principles:

- Confidentiality
- Integrity
- Availability

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

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

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

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

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

BIT Mission Statement

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

VISION

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

Goals:

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

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

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

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

Build and Retain a Highly Skilled Workforce.
Improve the effectiveness, productivity, and satisfaction of employees 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 room or locking up the device in a cabinet.
- **Network Access** includes protecting the State Network from unauthorized access via internal methods and from outside our physical offices. Because technology can be manipulated by individuals or workstations to create a detrimental outcome, safeguards must be implemented to prevent, thwart, and repel workstation attacks from inside State Government and the Internet; access protection is not limited to workstations; it includes smartphones, Internet of Thing devices, environmental controls, and network - network connectivity.
- **Workstation Platform** means taking advantage of the inherent feature sets of workstation platforms. For example, user id and password capabilities must be used as intended within the workstation platform.
- **Cyber Strength Evaluation** of business software must apply across in-house developed and third party built or supplied software applications. New applications must be tested before being placed into service and existing applications must be re-evaluated on a regular basis.
- **Cyber security language** is incorporated within all information technology (I/T) requests for proposals and I/T contracts.
- **Information System security** entails designing the necessary security features and permissions to ensure that only legitimized staff have proper resource access. The design must consider areas such as viewers of departmental data to individuals that can add data or update records.
- **Data security** is the protection of the asset; often referred to as the "money in the vault". Insuring that data is only accessible by permitted applications and personnel is the core of the security model. The data could be credit card numbers, social security numbers, health records, or financial information.

**Partners**

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

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

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

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

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

- Participate in information security awareness program activities;
- Read, understand, and follow the policies defined in the Information Technology Security Policy;
- Report all violations, security 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.
- Agreeing that use of State technologies which includes equipment, applications, and resources are for work-related purposes.
- Applying recommended password policies.
- Safeguarding sensitive information whether employee / contractor is in the office or traveling for the State.
- Reporting any unusual requests for information or obvious security incidents to the BIT Help Desk.
- Immediately reporting loss of any State technology devices or data.
- Understanding that everyone is a potential target of nefarious individuals seeking ‘social engineering’ information to be used for illegally accessing State of South Dakota systems and technologies; Hence, be aware that any information provided to outside entities can be dangerous.
- Protecting information technology assets by following policies and procedures.
- 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 clienteles.

1.1.3.1. Scope Assumptions

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

1.1.3.2. Scope Constraints
Contractors are not given any special privileges or dispensations 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 ensure government employees are aware of the risks and expected behaviors towards cyber security.
- Keeping a record of system integrity problems and incidents.
- Maintaining and updating the Information Technology Security Policies.
- Taking such emergency action as is reasonably necessary to provide system control where security is deemed to have been lost or jeopardized.
- Performing periodic security surveys.
- Providing for network security by seeking to preclude misuse of the network of the State to gain or attempt to gain unauthorized access to any system.
- Performing checks of information systems to assess system security and integrity, as well as to determine the use or placement of illegal or improper software or equipment.
- Coordinating the cyber security activities across BIT to 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. Security Infrastructure Team (SIT)

The SIT shall, in coordination with the CISO, recommend technology solutions, written policies and procedures necessary for assuring the security and integrity of State information technology. The SIT shall coordinate with the CISO in creating and implementing a written system to investigate any violations or potential violations of this policy or any policy regarding system security and integrity.

• The CISO shall appoint the Security Infrastructure Team members.
• The SIT shall be chaired by the CISO.
• At a minimum, the SIT communicates internally every two weeks, via a scheduled bi-weekly meeting or via email, the current security posture of the State.
• The SIT shall consist of at least one member from each of the BIT information technology divisions;
• The recommendation is that membership include multiple representation from development, systems integration, desktop support, networking.
• K-12, Regental, Judicial, Legislative, and other government entities can be invited at the discretion of the CISO.

1.1.4.4. Security Operations Team (SOT)

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

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

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

1.1.4.5. BIT Executive Working Group on Cyber Security

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

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

The Group shall meet quarterly at a minimum.

Administrative-I/T Asset Protection-Background Checks

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

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

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

10.1.2. Purpose

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

10.1.3. Scope

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

10.1.3.1. Scope Assumptions

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

10.1.3.2. Scope Constraints

Background checks are not performed for financial or credit information.

10.1.4. Policy

10.1.4.1. Background Checks

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

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

Individuals should plan on the background check taking two to four weeks.
The steps to process the background checks are found in procedures document ITSP 1010.1 Background Checks Procedures.

10.1.4.2. Disqualifying Criteria

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

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

A. An employee or contractor may not have access to confidential data if the individual has been convicted of a felony within 5 years of the date of the most recent criminal background check or any time thereafter.
   1. Employees or contractors involved with technology associated with the division of the South Dakota Lottery must meet the qualifications defined in SDCL 42-7A-14. Primarily, this extends the period beyond completing felony sentencing to 10 years, rather than 5 as defined in A. above.
B. If the employee or contractor has been convicted of a crime not included in Paragraph A, the employee or contractor is not automatically disqualified from having access to confidential data. The determination of whether such an employee or contractor may have access to confidential data will be made on an individual basis. The considerations will include but not be limited to:
   1. The nature of the conviction, particularly if it is a crime of dishonesty, a financial crime, an identity crime, or a crime involving the misuse of confidential information.
   2. The length of time between the offense and the employment decision.
   3. The number of offenses.
   4. The relatedness of the conviction to the duties and responsibilities of the position.
   5. The efforts at maintaining a clean record.
   6. The number of crimes committed.
C. The determination required by Paragraph B will be made by the BIT Chief Information Security Officer (CISO) in consultation with the applicable Division Director.
D. Under no circumstances may an employee or contractor have access to confidential data if the individual is disqualified by this policy.
E. If a position within the BIT requires an employee or contractor to have access to confidential data as an essential part of the job function, the individual's failure to undergo or to successfully pass a criminal background check may result in termination of the employee or contractor.
F. After the adoption of this policy, no employee or contractor may be hired by BIT unless the individual undergoes and successfully passes a criminal background check pursuant to this policy.
G. The hiring of support staff positions and promotions within support staff positions may be excluded from this policy.

10.1.4.3. Noncriminal Agency Coordinator (NAC)

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

10.1.4.4. Local Agency Security Officer (LASO)

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

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

10.1.4.6. Not Guilty Presumption

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

10.1.4.7. Background Check Information Challenge

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

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

10.1.4.8. Corrective Action

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

10.1.4.9. Training

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

10.1.4.10. Emailing Background Check Information

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

Administrative-I/T Asset Protection-Confidentiality

10.3.1. Overview

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

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

10.3.3. Scope

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

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

10.3.3.1. Scope Assumptions

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

10.3.3.2. Scope Constraints

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

10.3.4. Policy

10.3.4.1. Confidentiality Agreement

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

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

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

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

Complying with Legal Obligations

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

10.3.4.2. Security Acknowledgement and Access

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

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

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

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

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

Mainframe-Mainframe Security-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 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-Mainframe Accounts

210.4.1. Overview

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

210.4.2. Purpose

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

210.4.3. Scope

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

210.4.3.1. Scope Assumptions

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

210.4.3.2. Scope Constraints

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

210.4.4. Policy

210.4.4.1. Mainframe User ID Revocation

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

Mainframe-Mainframe Security-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 those who wish to access the BIT Computer Room. It does not necessarily apply to other facilities or rooms administered by BIT personnel.

210.25.4. Policy

210.25.4.1. Mainframe Access

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

Server-Server Security-Server Maintenance and Administration

220.1.1. Overview

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 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. Related Topics

220.1.4.1. State Policies

ITSP 230.72 Payment Card Industry Data Security Standard

220.1.5. Policy

220.1.5.1. 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.
220.10.1. Overview

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

220.10.2. Purpose


220.10.3. Scope

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

220.10.3.1. Scope Assumptions

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

220.10.3.2. Scope Constraints

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

220.10.4. Policy

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

Each user with access to HIPAA data is responsible for understanding federal requirements for data handling and security and accountable for any actions they take that may compromise the security or confidentiality of HIPAA data.

BIT will work with HIPAA authorized agency staff and authorized federal audit staff as well as written federal rules and regulations to assure security and access controls are in place to meet 45 CFR Part 160 and Part 164 and other applicable rules and regulations relating to electronic HIPAA information created, used, transmitted, stored, and destroyed on technology managed by BIT. Where deficiencies are determined to exist, BIT will work with the appropriate resources within the State and the applicable federal audit group to address those.

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

Cloud-based technology providers rely on a wide range of technologies and business models to offer and maintain their services. The security, reliability, portability, resilience, and long-term viability of any given service offering is largely dependent on the technologies and business models in use and the manner in which those technologies and business models are implemented, maintained, and managed.
However, it is impossible to know what the nature of the underlying technologies or business practices may be without a collaborative, detailed, and thoughtful review with the cloud-based technology provider.

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

230.9.2. Purpose

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

230.9.3. Scope

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

230.9.3.1. Scope Assumptions

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

230.9.3.2. Scope Constraints

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

230.9.4. Policy

230.9.4.1. Responsibility for Cloud Based Services and Systems.

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

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

Data Center General-Secure Information Technology Acquisition Policy

230.10.1. Overview

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

230.10.2. Purpose

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

230.10.3. Scope

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

230.10.3.1. Scope Assumptions

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

230.10.3.2. Scope Constraints

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

230.10.4. Policy

230.10.4.1. Hardware Maintenance Agreements

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

Data Center General-Data Center Security-Federal Tax Information

230.11.1. Overview

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

230.11.2. Purpose

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

230.11.3. Scope

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

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

230.11.3.2. **Scope Constraints**

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

230.11.4. **Policy**

230.11.4.1. **Federal Tax Information Returns and Return Information**

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

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

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

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

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

230.11.4.3. Safeguarding Federal Tax Information

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

230.11.4.4. Emailing Federal Tax Information

It is prohibited to email FTI either as an email or as an attachment to an email. Do not open any email that contains FTI but report the occurrence to your supervisor and delete the email.

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 for routine, scheduled and emergency changes. 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, periodic, and emergency 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 afore mentioned tasks. The list is not inclusive. Emergency changes are changes that require immediate attention.

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. Routine and Scheduled Changes

Routine changes include movement of individual source code from test to production for production systems or routine patches to server operating systems. Changes are made or requested through the Help Desk using the normal scheduled processes and timeframes for routine changes. These changes are documented in different ways depending on the normal process and timeframes for the changes. The change is documented by sending an email to the Help Desk and is included in the Change Management Calendar. Program manager approval is...
required. Program Management will periodically review the maintenance calendar. Any problems that come up as a result of routine changes will be documented by the Program Management and reviewed.

Scheduled changes include implementation of a new system, a major enhancement to a current system or infrastructure changes impacting clients as well as upgrades to existing development platforms. Changes are scheduled through the Change Management process and all parties involved with change management are notified. The change is documented by using the Change Management Form and submitted to the BIT Change Management email group. Once the form has been emailed, the Change Management group will review and approve. If staff has questions or issues, they meet with the individual who submitted the request.

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.

230.53.4.3. Emergency Changes

Emergency changes require immediate attention. An example of this situation would be if a network segment is down and is affecting multiple clients or if a production system is inoperable. The corrective action is applied immediately without prior management approval. The problem, the corrective action, and the impact are documented in the trouble ticket as soon as the fix is implemented. A post mortem report is created. No prior program manager approval is required. Staff must inform appropriate Program Management, Division Management, and Commissioner. Management will review the problem and action taken after it is documented in the trouble ticket and post mortem report.

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 Revenue (DOR), 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 longer 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 apply only to 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/Change Responsibilities) 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. Administrative Capabilities

Only individuals authorized as an Administrator will have administrative capabilities on computing equipment within their specific area of responsibility.

230.67.4.3. 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 the BIT Help Desk. Written business justification must be provided with the request by an agency manager for the request to be considered. Technical staff will then need to confirm the justification.

Local privileges will be granted if the:

- BIT developer needs to test applications and the software they use requires administrator privileges.
- Client software requires administrator privileges in order to run.

230.67.4.4. 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.

230.67.4.5. Administrative Privileges

Only authorized BIT staff is granted administrative privileges. These privileges are utilized to modify UID passwords and workstations upon legitimate request.

230.67.4.6. Password Requirements

Must:
- Be changed every ninety days.
- Be at least eight characters.
- Contain at least three of the following four-character groups:
  - English uppercase characters (A through Z).
  - English lowercase characters (a through z).
  - Numerals (0 through 9).
  - Non-alphabetic characters (such as !, $, #, %).
- Must not be one of the twenty-four most recent passwords;
- Must not have been changed within the last seven days.
- Does not contain first name, last name, username.
- Does not contain Social Security Number.
- Does not contain permutations of "password".
- Cannot be a dictionary word.

Individual users’ accounts that do not have administrative access rights will result in passwords expiring after 90-days. Where existing state technology products can support multiple expiration password policies for individual administrators’ accounts that have administrative access rights without altering the general 90-day expiration password policy for individual users’ accounts that do not have administrative access rights, the expiration password policy shall be set to 60-days for such administrators’ accounts that have administrative access rights.

**230.67.4.7. Agency Specific Policy DOR, DSS and DLR Lockout Threshold and Duration**

A lockout threshold shall be set at ten consecutive failed logon attempts with lockout duration of fifteen minutes. An account that has been locked out due to ten consecutive failed logon attempts shall remain in a locked state until it is reset by an authorized administrator. An account that has reached the lockout threshold can be reset at any time by contacting the BIT Help Desk and following the required reset process.

**230.67.4.8. Agency Specific Policy DOR, 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.

**230.67.4.9. 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/](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.
230.67.4.10. Granting of Domain Administrator Privileges

Requests for domain administrator privileges must be submitted to the BIT Help Desk. These requests must be approved by the requester's BIT manager followed by the manager's division director followed by the Chief Security Officer.

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

230.72.1. Overview

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

PCI compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The requirements apply to all payment channels, including retail (in person), mail/telephone order, and e-commerce. The State of South Dakota is Merchant Level C for PCI compliance. To maintain this level the State needs to make sure no credit card information or data associated with the credit card is being stored. Failure of the State to adhere to PCI standards can result in the State losing the ability to use payment cards and can result in fines.

230.72.2. Purpose

To ensure the State is in compliance with PCI security standards

230.72.3. Scope

This covers any use of the State of payment cards for the payment by other entities to the State for goods and/or services.

230.72.3.1. Scope Assumptions

This policy assumes you will need to use payment cards for the reimbursement of the State by other entities for goods and/or services provided by the State.

230.72.3.2. Scope Constraints

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

230.72.4. Policy

230.72.4.1. Payment Card Industry Data Security Standard Requirements

The State of South Dakota is required by the payment card association to be compliant with the PCI security standards, and is committed to providing a secure environment for our customers to protect against both loss and
fraud. The State of South Dakota must comply with PCI requirements for securely processing, storing, transmitting, and disposing of cardholder data. The State will verify annually that all financial acquiring institutions (such as banks) representing the State for PCI processing be certified as PCI compliant. The financial institutions are required to submit a letter to BIT stating they are in compliance with PCI standards.

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

230.73.1. **Overview**

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

230.73.2. **Purpose**

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

230.73.3. **Scope**

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

230.73.3.1. **Scope Assumptions**

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

230.73.3.2. **Scope Constraints**

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

230.73.4. **Policy**

230.73.4.1. **Requests for Proposals**

Requests for Proposals (RFP) for the acquisition of I/T related goods or services will be required to utilize the BIT RFP process. To facilitate this, the agency must inform their BIT Point of Contact when an I/T RFP will be done. Failure to follow the BIT RFP process can result in the delaying of the RFP selection process. If the BIT Security and Vendors Questions were not included with the RFP when it was released then they should be sent out as an amendment to the RFP.

230.73.4.2. **Contracts**

Contracts including information technology components of any manner must go through the BIT contract process. The BIT Security and Vendor Questions must be included as part of the contracts process. If the RFP process was not utilized, the Security and Vendor questions must be evaluated and reviewed before contract negotiations can proceed. Exceptions to this require the BIT Commissioner's or Chief Information Security Officer's approval. It
may also require a signed release from the agency recognizing the risks involved. This step is determined by the BIT CISO.

230.73.4.3. Acquisition of Internet of Things Devices

The acquisition of Internet of Things (IoT) devices that will be attached to the State's infrastructure will follow the processes as outlined in NIST 800-160 System Security Engineering section 3.4 Agreement Processes. In addition, the device must be scanned to the extent possible. Any purchase of IoT devices must include a commitment by the supplier to keep any software associated with the IoT device patched and up to date.

230.73.4.4. Acquisition of Services Involving HIPAA Data

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

230.73.4.5. Security Scanning Requirements

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

230.73.4.6. Hardware Maintenance Agreements

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

Data Center General-Use of Production Data-Use of Production Data in a Non-Production Environment

230.74.1. Overview

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

230.74.2. Purpose

This policy outlines how production data should be handled outside of production environments.
230.74.3. Scope

This policy includes all non-production environments that store or process production data on State or Contractor systems. Any production data moved to a non-production environment before this policy goes into effect is exempt for 60-days from the date this policy is published in the ITSP. After 60-days, unapproved production data in a non-production environment must be purged, or approval to keep the data in the non-production environment must be obtained by using the BIT Moving Live Data Request Form. Any data protected under Federal or State regulation or statute or industry standard is considered protected data.

230.74.3.1. Scope Assumptions

This policy assumes you need to move production data into a non-production environment and are authorized to work with the data in question. All protected data that is masked before being moved is no longer considered to be protected data.

230.74.3.2. Scope Constraints

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

230.74.4. Policy

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

Approval must be obtained before moving production data to a non-production environment. The non-production environment must have the same level of security as the production environment. The BIT Moving Live Data Request Form must be approved before moving the production data into a non-production environment. The approval is valid for six months from the date the last approver signs the form. If the data is needed in the non-production environment longer than six months, another BIT Moving Live Data Request Form must be filled out and approved before the last approval expires.

The use of Federal Tax Information (FTI) in non-production environments requires authorization from the IRS Office of Safeguards by filling out the IRS Live Data Testing Notification Form. The IRS form must be submitted at least 45 days before moving the data. The IRS can take up to 45 days to approve the move. A copy, or link, to the approved IRS form must be attached to the BIT Moving Live Data Request Form. The IRS must approve the move. The use of FTI production data in a non-production environment is limited to tax administration or other authorized IRS purposes including:

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

FTI data may only be disclosed to those requiring the data to perform their official duties. IRS approved sanitization methods must be used after the data is no longer needed. The requester may also be required to sign a form provided by the Data Owner prior to obtaining access to the production FTI. The Federal Parent Locator Service (FPLS) can be a secondary source of FTI. FTI from the FPLS is treated as if the FTI was from the IRS.

- Criminal Justice Information System (CJIS) data can only be moved by the Office of Attorney General (ATG), it cannot be moved by BIT. The ATG must notify the CISO when CJIS data is moved, provide the location of that data, and inform the CISO if dual authorization is required before disposal of the data. After the CJIS data is no longer needed it must be disposed of as stated in ITSP 230.68. The documentation and verification of the disposal of the data will be completed by the ATG.
- Production Payment Card Industry (PCI) data may not be used in non-production environments.
Contractors with access to protected data must sign the Security Acknowledgement Form and have passed a background check before they can have access to the data. Protected State data cannot be moved outside the United States of America or its territories. Protected State data may not be viewed remotely or by Contractors except for the exceptions given in policy 230.74.5.2.

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

**230.74.4.2. Use of Production Data in a Non-Production Environment by Contractors in Contractor Hosted Environments**

The Contractor must follow ITSP 230.74.5.1 in addition to this policy. The Contractor must meet with the Data Owner to see if the project Agreement must be amended before moving the production data. The Contractor's non-production environment will be scanned by the State. If defects are discovered they must be fixed to the State's satisfaction before the data can be moved. If the data is ePHI, the Contractor must have had a risk assessment within the last twelve (12) months, unless given approval by the CISO and the Data Owner to forgo the risk assessment. Any Contractor's staff that have or may have contact with the protected data must have passed a background check, using a process acceptable to the State. A Security Acknowledgement Form must be signed. Before moving FTI or FPLS data, the Contractor must meet with the State Contact as the Data Owner may require the Contractor to complete additional forms. If the Contractor will be moving FTI or FPLS data they must complete the IRS Live Data Testing Notification Form and obtain approval from the IRS. The BIT Moving Live Data Request Form must be approved prior to moving the production data to a non-production environment.

**230.74.4.3. Purging of Data**

If there is unapproved production data in a non-production environment, the production data must be purged. If there is production data in a non-production environment that was moved prior to this policy that was not approved using the BIT Moving Live Data Request Form you must, within 60 days of this policy being published in the ITSP:

- Purge the production data, if you no longer need it in the non-production environment.

  OR

- Get approval for the production data to be in the non-production environment.

Production data must be purged from the non-production environment before the BIT Moving Live Data Request Form approval has expired. It is the responsibility of the requestor of the data move to purge the data.

If an individual finds unapproved unmasked protected production data in a non-production environment they must notify their manager, who will notify the Development Director and CISO. The data will be purged, and the Development Director and CISO will be notified when it is purged.

If unapproved unmasked protected production data is found in a non-production environment, the CISO will decide if it is a security incident. The individual(s) responsible for unapproved unmasked protected production data in a non-production environment may be subject to disciplinary action up to and including dismissal. The placing of unapproved unmasked protected production FTI or FPLS data on a non-production environment may subject the individual responsible to legal action as stated in IRS 1075.
230.75.1. Overview

Data classification establishes the agency and BIT responsibilities for handling, maintaining, and meeting required levels of security control for the data.

230.75.2. Purpose

The purpose of this policy is to provide data classification for confidentiality, integrity, and availability.

230.75.3. Scope

These policies include all State data located on State infrastructure or 3rd party infrastructure. These policies also include data owned by Contractors if the data is used by an agency and resides on BIT managed systems. An example is Geographic Information System data. While the data may be owned by the Contractor the agency is considered the data owner for the purposes of these policies. If the data is owned by the Contractor and there are data handling requirements in the contract, the contractual data handling requirements preempts these policies.

230.75.3.1. Scope Assumptions

These policies cover all state data residing on the State's or a Contractor's system and Contractor data residing on state systems. Contractor owned data on a Contractor's system is not included.

230.75.3.2. Scope Constraints

These policies are limited to data and does not cover applications.

230.75.4. Policy

230.75.4.1. Data Classification System

Each agency shall serve as a classification authority for the data and information for which it is considered the data owner. BIT is not the data owner of data it collects or maintains for another State agency to fulfill that agency's mission; the State agency is the data owner.

Data classification is based on four impacts with three security objectives:

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>NO</th>
<th>LOW</th>
<th>MODERATE</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</td>
<td>Information having no confidentiality requirements is information that must be released under open records laws, is public information, or where an agency waives an exception to the open records laws. BIT suggests that the data owner consult their legal staff before classifying information as having no</td>
<td>The unauthorized disclosure of information could have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could have a <strong>severe or catastrophic</strong> adverse effect on reputation, operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The unauthorized disclosure of information could have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could have a <strong>severe or catastrophic</strong> adverse effect on reputation, operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td><strong>Availability</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</td>
<td>Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is always some impact if integrity is not maintained.</td>
<td>There is always some impact if availability is not maintained.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The unauthorized modification or destruction of information could have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The unauthorized modification or destruction of information could have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The unauthorized modification or destruction of information could have a severe or catastrophic adverse effect on reputation, operations, organizational assets, or individuals.</td>
<td>The disruption of access to, use of information or an information system could have a severe or catastrophic adverse effect on reputation, operations, organizational assets, or individuals.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Developed from FIPS 199 Table 1, Page 6

Any data that is Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), Health Information Portability and Accountability Act (HIPAA) or any information defined under State or Federal statute as confidential is automatically considered to be highly confidential. Examples include:

- Public Assistance Records- Highly Confidential.
- Pistol Permits Records- Moderate Integrity.
- Inventory of Emergency Vehicles- Low Availability.

Further information on protected information can be found in the Abbreviations, Definitions, and Term Usage section of the ITSP and [http://intranet.bit.sd.gov/standards/PII.aspx](http://intranet.bit.sd.gov/standards/PII.aspx).

All data on the State's mainframe system is automatically treated by BIT as having high requirements for confidentiality, integrity, and availability.

### 230.75.4.2. Classification of Data Produced under Contract

As part of the contract process the data owner is required to document the classification all data produced or utilized by the project. The data classification is recorded on the Contract MOU Review Checklist and Summary provided by BIT. A copy of which will be kept by BIT and included with a copy of the contract. This includes State data that resides on a Contractor’s system or data that the Contractor generates as part of a project. Also included is any State data utilized by a Contractor while providing Software as a Service (SaaS). The checklist
230.75.4.3. **Data Classification Responsibilities**

It is the data owner's responsibility to:

- Choose a systematic decision process to classify the data.
- Document the classification.
- Determine whether existing laws, regulations or agreements limit or regulate the collection, use, disclosure, access, retention and disposal of state data. Agencies shall use all applicable published requirements, guidelines, and limitations.
- Educate agency staff on the data classification procedures, requirements, and guidelines.
- Based upon the results of the agency's data classification, establish data maintenance guidelines, and communicate them to BIT.
- Establish a process to regularly review the appropriateness of the assigned data classifications and to adjust classifications in the event of:
  - Regulatory changes affecting an agency's management of information under its control.
  - Technologies for which data classification policies do not yet exist.

If the data is Protected Health Information (PHI) BIT recommends that the data owner perform a risk assessment as well as data classification.

It is BIT's responsibility to:

- Assure that proper access controls are implemented, monitored, and audited for building, floor and/or cage access in accordance with the data classification labels assigned by the data owner.
- Submit audit results to the data owners as required by law or regulation.
- Perform regular backups of state data.
- Validate data integrity.
- Restore data from backup media.
- Fulfill the data requirements specified in agency security policies, standards and guidelines pertaining to information security and data protection.
- Retain records of data activity that include information on who accessed the data and what data was accessed as considered appropriate by the federal regulatory agency responsible for establishing security controls for the data.
- Provide appropriate security controls for contractor hosted services according to the data classification labels assigned by the data owners.

**Data Center General-Access to Confidential Data-Multi-Factor Authentication**

230.76.1. **Overview**

The implementation of Multi-Factor Authentication (MFA) improves authorization access to technology systems and enhances cyber security.

MFA provides an additional layer of protection towards the access control aspect of cyber security. MFA is an authorization technology based on at least two pieces of information. This is one additional step in the authentication process beyond the standard set of user id and passwords.
230.76.2. Purpose

The purpose of this policy is to provide direction on MFA use within State government.

230.76.3. Scope

This policy applies to the remote access of protected data, equipment, and sensitive applications by the clients of the State's network.

230.76.3.1. Scope Assumptions

The usage of MFA will meet / fulfill the NIST and IRS audit findings against the State. The solution will meet the MFA needs of protected data, equipment, and sensitive applications.

230.76.3.2. Scope Constraints

This policy applies to access of protected data, equipment, and sensitive applications.

230.76.4. Policy

230.76.4.1. Usage of Multi-Factor Authentication (MFA)

Remote access to protected data such as Federal Tax Information (FTI), Criminal Justice Information System (CJIS) data, or other protected data must be initiated using MFA. Remote access, defined by IRS Publication 1075, is any access to an agency information system by a user communicating through an external network, for example, the Internet.

All core firewalls, switches, and routers will use MFA for any access. MFA will be required for remote access of servers.

230.76.4.2. MFA Tokens

If a user has a mobile device enrolled in the State's standard Mobile Device Management System to gain access to State resources, that mobile device is their second factor of authentication and the user will not be issued a hard token.

Mobile device authentication is the preferred method of secondary authentication.

Hard tokens are only allowed as a user's second factor of authentication if the user does not have a mobile device enrolled in the State's standard Mobile Device Management System. A user may receive and use a hard token as their alternative second factor of authentication upon approval from BIT and at the agency's expense.

Development-I/T Asset Management-System and Services Acquisition and Operation

401.1.1. Overview

The acquisition, development, installation, and operation of all information systems must meet federal requirements necessary to protect Federal Tax Information (FTI).
401.1.2. **Purpose**

The purpose of this policy is to meet federal security requirements to safeguard FTI on any information system that is acquisitioned or developed by BIT.

401.1.3. **Scope**

The scope of this policy includes all information systems developed by BIT, contractors, or any third party that is involved in receiving, processing, storing, or transferring Federal Tax Information (FTI).

401.1.3.1. **Scope Assumptions**

This policy assumes that if the information system receives, processes, stores, or transfers FTI, it will be capable of being security scanned.

401.1.3.2. **Scope Constraints**

The policy only applies to information systems that receive, process, store, or transfer FTI. Security scans are not conducted on mainframe applications and desktop applications. Due to software licensing requirements, some vendor hosted solutions do not allow for BIT to conduct security scans. Vendor hosted solutions must still comply with federal requirements to protect FTI and must meet BIT security requirements specified in contract terms.

401.1.4. **Policy**

401.1.4.1. **Allocation of Resources and Life Cycle Support**

As part of the capital planning and investment control process, BIT will determine, document, and allocate the resources required to adequately protect information systems. Security assessments will be performed as part of the Software Development Life Cycle (SDLC) process.

401.1.4.2. **Information System Security Documentation**

BIT will obtain, protect as required, and make available to authorized personnel, security assessment documentation for the information system. Any newly developed or acquired software, hardware, application, or website will be required to pass a security scan:

- Prior to being moved into production.
- After a significant change.
- Prior to any updates being moved into production.

A report specifying each area reviewed or audited during the assessment process will be completed and filed. The report will include all deficiencies discovered during the assessment. A solution for each deficiency will be noted and a due date for the solution to become effective will be documented. All information regarding security assessments and official records of such will be recorded in the Pegasus system. If BIT is unable to conduct a security scan on a vendor hosted solution, the vendor must meet all security audit and vulnerability assessment requirements deemed appropriate by BIT and provide documentation of such to BIT as specified in contract terms.

401.1.4.3. **Software Usage Restrictions and User Installed Software**
To safeguard FTI, BIT will comply with software usage restrictions, impose, and enforce limitations on user installed software on BIT workstations. Preventing unauthorized installation of non-standard software on BIT workstations and verifying that licensing requirements are met ensures that security controls implemented by BIT are not circumvented.

Software and associated documentation will be used in accordance with software contract agreements and copyright laws. BIT will track the use of software and associated documentation that is protected by quantity licenses to control copying and distribution. BIT will control and document the use of peer-to-peer file sharing technology to ensure that it is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.

Prior to installation on BIT workstations, open source software must go through the BIT moratorium process that includes, but is not limited to, a security assessment.

Only authorized individuals are permitted to install software.

### 401.1.4.4. Developer Configuration Management

BIT requires that information system developers and integrators perform configuration management during information system SDLC and operation as well as manage and control changes to the information system to include:

- Documentation of approved changes to the information system and potential security impacts of the changes.
- Track security flaws and flaw resolution within the system.
- Implementation of only BIT approved changes.

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

#### 401.3.1. Overview

To ensure applications developed by BIT, contractors, or any third-party are protected and monitored to prevent unauthorized use, modification, disclosure, destruction, or denial of access to assets of the State.

#### 401.3.2. Purpose

The purpose of this policy is to ensure that no hosted application, software, or website may be moved into production without passing a security assessment.

#### 401.3.3. Scope

This policy applies to any software, application, or website developed by BIT, contractors, or by any third-party.

#### 401.3.3.1. Scope Assumptions

This policy assumes that if the software, application, or website hosts any type of state government data, it will be capable of being security scanned. The security assessment will include active penetration testing and analysis of an application which can include, but is not limited to, the latest Top 10 categories of the OWASP (Open Web Application Security Project) and NIST (National Institute of Standards and Technology) standards.
401.3.3.2. **Scope Constraints**

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


401.3.4. **Policy**

401.3.4.1. **Security Assessment**

Configurations and installation parameters on all State applications must comply with BIT security management policies, procedures, and standards. All BIT developed software, third-party applications, internally hosted websites, and externally hosted websites must pass a security assessment prior to being accepted into production. The originator of the request to transfer to production will bear the responsibility of verifying that a security assessment has been performed. Written verification from the BIT Security Infrastructure Team (SIT) ([BIT.ENTNETWORKSEC@state.sd.us](mailto:BIT.ENTNETWORKSEC@state.sd.us)) that the software, application, or website has passed the security assessment must be provided. For additional information on how to initiate a security assessment see 1451.5 Security Assessment Procedure.

Security assessments will be performed as part of the SDLC (Software Development Life Cycle) process.

A security assessment of all applications supporting the needs of the Medical Management Information System (MMIS) and the Medicaid eligibility determination system will be conducted annually.

401.3.4.2. **Assessment Report**

A report specifying each area reviewed or audited during the assessment process will be completed and filed. To view the report form, see [Audit findings template follow up](#). The reports shall be reviewed by the BIT SIT on a quarterly basis to ensure all deficiencies have been resolved in a timely manner.

401.3.4.3. **Annual Review**

BIT will form an annual assessment team comprised of individuals who have been identified as having the knowledge and skills to properly assess the requirements for security controls, assessing risk, and understanding the various user needs of the system. These individuals shall also understand the consequences of non-adherence to security controls and processes. The BIT assessment team will conduct an annual assessment of security controls for applications and systems. This assessment will be performed concurrently with annual security discussions and will verify:

- The extent to which security controls are implemented correctly.
- Security controls are operating as intended.
- Security controls meet the life cycle and level of risk security requirements of the applications, websites, software, and systems.

**Development-I/T Asset Management-Data Encryption**

401.5.1. **Overview**
This policy covers rules for storing sensitive data used by applications and systems.

401.5.2. Purpose

The purpose of this policy is to outline what encryption algorithms and encryption tools are acceptable for BIT to use to encrypt columns in the State databases. The policy defines the minimum level of data that is required to be encrypted.

401.5.3. Scope

This policy applies to all new applications and system rewrites.

401.5.3.1. Scope Assumptions

The applications and/or systems referred to herein must have been newly created or rewritten. This also includes applications that will have an updated database or system architecture.

401.5.3.2. Scope Constraints

The applications and/or systems to herein must have been developed or rewritten by the Development division of BIT, contractors employed by BIT, and/or third-party vendors contracted by the State.

401.5.4. Policy

401.5.4.1. Encryption Tools

For a list of acceptable tools see procedure document 1451.1.

401.5.4.2. Encryption Algorithms

Acceptable encryption algorithms are AES 256 or higher and RSA 2048. For the use of any other encryption algorithms see 401.5.8.5 Exceptions.

401.5.4.3. Data that Needs to be Encrypted

Data that is required, but not limited, to be encrypted includes Social Security Numbers (SSNs), Federal Tax Information (FTI), and Protected Health Information (PHI). Other data may be recommended or required depending on the application security reviews that are performed.

401.5.4.4. Compliance Measurements

The BIT Development Enterprise Team will verify compliance to this policy through various methods including, but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

401.5.4.5. Exceptions

Any exceptions to this policy must first be approved in advance by the Application Security Engineer, API Evangelist, and Technology Team Manager.
401.5.4.6. Non-Compliance

Applications that do not meet the requirements of this policy will not be permitted into a production environment until the requirements of this policy have been satisfied.

Development-I/T Asset Management-Authentication, Authorization, and Auditing

401.7.1. Overview

This policy defines how logon screens, roles, and auditing are implemented on websites, applications, and systems.

401.7.2. Purpose

The purpose of this policy is to set the minimum requirements for how to work with and create applications, websites, and systems that require user authentication, role-based authorization of users, and auditing.

401.7.3. Scope

This policy applies to all new applications, websites, and system rewrites.

401.7.3.1. Scope Assumptions

The applications, websites, or systems referred to in this policy include new development and those being rewritten. Any application, website, or system that receives, possesses, stores, or transfers Federal Tax Information (FTI) must follow the policy sections for FTI.

401.7.3.2. Scope Constraints

The applications, websites, or systems referred to in this policy must have been developed or rewritten by the Development division of BIT, contractors employed by BIT, and/or third-party vendors contracted by the State. This policy does not apply to applications or websites hosted by contractors or third-party vendors.

401.7.4. Policy

401.7.4.1. User Authentication, Authorization, and Auditing

If your project uses authentication and authorization of users with different roles it must include the following requirements.

- Web applications that require a logon screen for user authentication must use ASP.NET Identity for:
  - password resets
  - secure storage of passwords
  - role management
  - multifactor authentication
- WinForms and Windows Presentation Foundation (WPF) applications that require user authentication functionality must use Active Directory for logon and role management, if possible.
Mainframe systems that require user authentication functionality must use Resource Access Control Facility (RACF).

An audit log must be created with BIT Login Security API.

A latency timer set between 1-5 seconds must be created with BIT Login Security API.

If custom authentication is required, it must be approved before the project begins, unless an exception has already been granted.

401.7.4.2. Password Requirements

The following password requirements must be built into your project.

1. Enforce a minimum password complexity of:
   • Eight-character minimum and a maximum of 64 characters
   • At least one numeric and at least one special character
   • A mixture of at least one uppercase and at least one lowercase letter
   • Storing and transmitting only encrypted representations of passwords

2. Enforce password minimum lifetime restriction of one day
3. Prohibit Password reuse for 24 generations
4. Allow the use of a temporary password for system logon requiring an immediate change to a permanent password
5. Password-protect system initialization (boot) settings
6. Allow passwords to be copied and pasted into the login.
7. No password hints.
8. No knowledge based authentication (For example, what was the name of your first pet?).

If your project involves FTI it must include the following requirements, in addition to those listed above.

• Enforce non-privileged account passwords to be changed at least every 90 days
• Enforce privileged account passwords to be changed at least every 60 days

401.7.4.3. Invalid Login Attempts for projects using Federal Tax Information

If your project involves FTI, it must include the following requirements.

• Enforce a limit of three consecutive invalid login attempts by a user during a 120-minute period by automatically locking the account for a period of at least 15 minutes.
• Prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.
• Retain the session lock until the user reestablishes access using established identification and authentication procedures.
• The information system must automatically terminate a user session after 30 minutes of inactivity.

401.7.4.4. reCAPTCHA

ReCAPTCHA will be required on all login pages and public facing form submissions unless they are protected by a login page that already uses reCAPTCHA.

401.7.4.5. Tools
401.7.6. Compliance Measurements

The BIT Development Enterprise Team will verify compliance to this policy through various methods including, but not limited to: business tool reports, internal and external audits, and feedback to the Development Enterprise Team.

401.7.7. Exceptions

Any exceptions to this policy must first be approved in advance by the Development Application Security Engineer, Development API Evangelist, and Development Enterprise Team Manager.

401.7.8. Non-Compliance

Projects that do not meet the requirements of this policy will be subject to additional development to add the required functionality listed in this policy to the project before it will be permitted into a production environment.

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 to ensure that the appropriate level of access for the intended functions is granted. All access methods utilized to connect to State networks must be implemented through approved combinations of hardware and software security tools that 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 (605.773.4357) 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 (605.773.4357) 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 (605.773.4357) 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. Any remote access where Federal Tax Information (FTI) and or Criminal Justice Information System (CJIS) data is accessed over the remote connection must be performed using multi-factor authentication. Supported forms for remote access are:

- Secure Sockets Layer (SSL) - an Internet Web Browser with a minimum of 256-bit encryption
- CSG - the Citrix Secure Gateway of the State
- NetMotion - a VPN client maintained by BIT
- Horizon View (VDI)
- Skype for Business - a collaboration system operated by BIT, can be used if and only if a BIT staffer monitors and manages the access during all remote access sessions.

SSL VPNs are not permitted under any circumstances.

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](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 will manage network connectivity platforms for agencies. This responsibility encompasses local networks, wide-area networks, wireless networks, cellular networks, secure remote access networks, and relevant security components.

**610.9.4.3. Disabling Critical Components of Network Security Infrastructure**

Critical components of the BIT network security infrastructure must not be disabled, bypassed, or turned off without prior approval from the Director of the Division of Telecommunications or their designee(s).

**610.9.4.4. Technical Asset or Contractor Connections**

Connection of any contractor and/or their equipment to the DDN or any subsystem requires prior approval from the BIT Commissioner or their designee(s). To request any equipment to be installed or connected to the DDN, requestors will begin by submitting a request to the BIT HELP Desk (605.773.4357) 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 (605.773.4357). 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 (605.773.4357).

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

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 (605.773.4357) 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 (605.773.4357) 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 (605.773.4357) 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. **Limiting Tool Functionality**

Technical tools must be used as directed by the manufacturer or BIT. Utilizing technical tools to cause damage to devices or disrupting the desired data flow across the DDN is prohibited. Authorization to use software such as packet capture, network probing, and network and endpoint discovery tools for troubleshooting activities does not imply that consent has been provided to utilize these tools without limitations. Individuals, identified in name, by the Director of the Division of Telecommunications are permitted to use discretion to expand the functionality of technical tools.

620.1.4.2. **Exploiting Security Controls of Information Systems**

All individuals must not exploit vulnerabilities or deficiencies found in information systems or perform probing of State network devices to damage systems or data. It is not permitted to obtain information that the individual is not authorized to view, to take resources away from other individuals, or to gain access to other systems for which proper authorization has not been granted. Any exploitation of vulnerabilities in information systems and damage from scanning or probing found must be reported using the Detailed Incident form located on the BIT Intranet.

620.1.4.3. **Cracking Application or Passwords**

All individuals are strictly prohibited from "cracking" passwords of the technical assets that exist on the DDN. Exemptions must be approved, in advance, and in writing, by the BIT Chief Security Information Officer. The Security Exemption Request Form at the BIT Intranet (http://intranet.bit.sd.gov/forms) must be used to request an exemption. Individuals, identified in name, by the Director of the Division of Telecommunications are permitted to "crack" passwords.

620.1.4.4. **Exemptions**

Exemptions must be approved, in advance, and in writing, by the BIT Chief Information Security Officer. Activities that are prohibited include, but are not limited to the use of scanning software and utilities, keylogging devices, vulnerability assessment tools, and denial-of-service utilities. Exemptions for probing and exploiting security controls must be submitted to the BIT HELP Desk (605.773.4357) 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, instant messaging (IM), file transfer, file sharing and the Intranet.

620.5.3.1. Scope Assumptions

Content filtering is provided to all users to protect them from the unintentional or deliberate accessing of Internet content that is offensive and inappropriate. Employees, contractors, and devices connected to the DDN must adhere to this policy.

620.5.3.2. Scope Constraints

This policy does not apply to K-12 and Higher Education accounts with administrator privileges. While this policy applies to BIT managed devices and users at our K-12 and Higher Education client locations, it does not apply to the local devices operated by those institutions.

620.5.4. Policy

620.5.4.1. Exemptions

If requesting a filter exemption, then justification is required. Exemptions to this policy must be submitted to BIT via the Security Exemption Request Form at the BIT Intranet (http://intranet.bit.sd.gov/forms). BIT will review the impact to the technology infrastructure of the State for each requested exemption; the period for the review process should not exceed two weeks.

Exemption Details:

- All Internet filtering exemptions must be approved by the BIT Commissioner.
- All requests for the data of an individual pertaining to Internet practices must come from the Department Secretary or Bureau Commissioner of the agency directly to the BIT Commissioner as requests for data are handled at the highest level possible.
- A report on an individual should be completed within two weeks. All requests for data must be approved by the BIT Commissioner.

620.5.4.2. Appropriate Use of Administrator Access

Accounts that are members of the SD Domain Administrators group have administrator access to Active Directory services and systems. Use of those accounts specific to Internet access is strictly prohibited. These include
Administrators, Domain Administrators, and other accounts with a level of access beyond that of a normal user account.

Use of these privileged accounts is restricted to administrative responsibilities and must be prohibited from non-administrative activities. Web browsing or any access to/from the Internet under an Administrator role is strictly prohibited. A malicious website can be used to compromise a workstation or server while online. A compromised asset with elevated Administrative privileges can cause significant additional harm over that of a normal user account.

620.5.4.3. DDN Content Filtering

BIT does not manage filtering of any degree for K-12 schools. BIT does not manage content filtering of any degree for Higher Education facilities. K-12 and Higher Education are completely responsible for the content that is permitted or blocked for their institutions.

620.5.4.4. DDN Intranet Content Filtering

BIT policy shall block access to the following categories, based on standard Web filtering suggestions. These categories are deemed inappropriate:

- Adult/Sexually Explicit Material
- Gambling
- Hacking
- Illegal Drugs
- Personals and Dating
- Malicious Websites
- Phishing
- Tasteless and Offensive Content
- Violence, Intolerance, and Hate
- Weapons
- Web Based Email
- Peer to Peer (P2P) File Sharing

620.5.4.5. Filter Exemption Requests

If access to a blocked Internet site is necessary for reasons related to work expectations or data is needed to understand the Internet surfing habits of an individual, the Department Secretary, Bureau Commissioner, or Executive Leadership must submit a request directly to the BIT Commissioner through the BIT HELP Desk (605.773.4357). 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 (605.773.4357). The content-filtering category database of the filtering solution is updated daily.

Requests must include:

- The name(s) of the requestor
- The phone number(s) of the requestor
- The SD Domain UID(s) of the requestor
- The site for which access is required or the scope of the data requested for an individual
• The length of time required for access to the site or the time-period to be recorded in a report.
Abstraction Technologies
The removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services. See also Directory, IP Address, and Relative Pathing.

Access Attempts
When a user tries but fails to connect to an application or database so that they can make use of the resource.

Accreditation (also referred to as Vulnerability Assessment)
Scanning of a system looking for security vulnerabilities.

Accreditation Boundary
All components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected. If a set of information resources is identified as an information system, the resources should:
• Generally, be under the same direct management control.
• Have the same function or mission objective and essentially the same operating characteristics and security needs.
• Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments.)

ADABAS
Software AG's database management system (DBMS). ADABAS organizes and accesses data according to relationships among data fields. The relationships among data fields are expressed by ADABAS files, which consist of data fields and logical records.

Ad hoc Networking (WANET or MANET)
A decentralized type of wireless network, considered ad hoc because it does not rely on a pre-existing infrastructure, such as routers or access points.

Adverse Event
An observable occurrence where there is unauthorized use of system privileges, unauthorized access to State data, execution of malware, physical intrusions, or electronic intrusions that may include network, applications, servers, workstations, and social engineering of staff.

Agency
An association, authority, board, commission, committee, council, department, division, task force or office within the Executive Branch of State government. Includes the staff of that individual department.

Application
A complete and self-contained program or group of programs designed to perform a function for the user.

Application Scans
Scans performed by BIT against business software applications to identify security vulnerabilities. This includes applications BIT writes and software that is procured from other software companies.
Application Server
A type of server designed to install, either on workstations or other servers, operate, host applications, and associated services for end users and I/T services. It facilitates the hosting and delivery of applications, which are used by multiple and simultaneously connected local or remote users.

Authorized Developer
An individual which has been granted permission and access to systems by an administrator of said system so that they can build and create software and applications.

Authorized Persons
The vendor’s and their employees, contractors, subcontractors, or other agents who need and have been granted access to the State’s data or IT facilities to enable the Vendor to perform the services required.

Back Door
Access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes during development. Attackers can use back doors that they detect, or install themselves, to gain access to an application or database for malicious purposes.

Blocked mail
Incoming emails which are being stopped at the mail gateway because they are or appear to be phishing emails, spam, or they have malicious attachments.

Bluetooth
The wireless communication technology that conforms to the Bluetooth computing and telecommunications industry specification. This specification describes how mobile phone, landline phones, computers, and mobile devices can easily exchange information by using a short-range wireless connection.

Browser
A software application used to locate, retrieve, and display content from the World Wide Web, including Web pages, images, video, and other files.

Brute Force Attack
A hacker sets up an automated process against login pages to repeatedly test the user id or password. If they guess a correct combination, they have gained access to the system.

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

Business Associate (BA)
A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity or another Business Associate. Business associate functions and activities include: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Business associate services are: legal,
actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. BIT is considered a Business Associate of DSS, DOH, DHS, and BHR.

Business Associate Agreement (BAA)
An agreement with a third party or vendor to assure the State that the vendor is appropriately protecting confidential client information and data. If a governmental agency is the BA of another governmental agency who is the covered entity a MOU maybe substituted for a BAA. See also Regulated data and Health Information Portability and Accountability Act.

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

Circuit
A theoretical structure simulating electrical and data paths.

Closed Source
Proprietary software where the state does not hold the copyright.

Cloud Service
Services made available to users on demand via the internet from a cloud computing provider’s server as opposed to being provided by the State’s on-premise servers. See also Infrastructure as a Service and Platform as a Service.

Code
The instructions commonly used in a program that cause a computer to perform a specific task.

Commercial off the Shelf Software
Closed source software that is purchased and used by the State with no changes made by the vendor.

Communication Protocols
The agreed upon format for data that allows the data to be sent between computers.

Connectivity
The ability of hardware devices or software packages to transmit data between other devices or packages.

Content Filtering
Using a program to screen and exclude from access or availability, Web pages or email that is deemed objectionable.

Contractor
Regarding a signatory to a contract or agreement, the terms Contractor, Consultant, and Vendor are equivalent. Subcontractors, Agents, Assigns and/or Affiliated Entities are not signatories to the contract or agreement. The ITSP may be attached to the contract or agreement and all policies in the ITSP apply to all.

Covered Entity
A HIPAA covered entity is any organization or corporation that directly handles Personal Health Information (PHI) or Personal Health Records (PHR). The most
common examples of covered entities include hospitals, doctors’ offices, and health insurance providers. DSS, DOH, and BHR are covered entities. See also Business Associate, Regulated data and Health Information Portability and Accountability Act.

**Cracking passwords**
The process of recovering passwords from data that have been stored in or transmitted by a computer system.

**Credentials**
Credentials are a UID plus additional information and data such as a password, account number, or access code. Examples are:
- RACF
- NATURAL

**Data and Information Types**
Data is measured, collected, reported, and analyzed. Data as a general concept refers to the fact that some existing information or knowledge is represented or coded in some form suitable for better usage or processing. Pieces of data are individual pieces of information.

**Data and Information Types: Confidential**
Any data or information, other than trade secrets, that is materially sensitive in nature, whether manual or electronic, which is valuable and not generally known to the public. Identified here, are few examples, this list is not inclusive. Personally Identifiable Information which is not in the public domain, and if improperly disclosed could be used to steal the identity of an individual, violate the right of an individual to privacy or otherwise harm the individual or business to include, but is not limited to social security numbers, tax payer identification numbers, and any other department determined data that is not in the public domain or intended for release to the public domain and if improperly disclosed might:
- Cause a significant or severe degradation in mission capability.
- Cause loss of organizational integrity or public confidence.
- Result in significant or major damage to organizational assets.
- Damage the integrity of the State.
- Result in significant or major financial loss.
- Result in significant, severe, or catastrophic harm to individuals.

**Data and Information Types: Federal Tax 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.

**Data and Information Types: Personally Identifiable Information (PII)**
Any information about an individual that is maintained or collected by an agency, including:
ITSP Terms and Acronym Directory

• Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
• Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Data and Information Types: Protected
Very specific types of data regulated by law, which includes but is not limited to PCI, FERPA, HIPAA, GLBA, ITAR and EAR.
• FERPA: Education records are protected by FERPA (Family Educational Rights and Privacy Act). For example, tax records of parents and students, class lists, grade rosters, records of advising sessions, grades, and financial aid applications.
• HIPAA: Certain health information and data is protected by HIPAA (Health Information Portability and Accountability Act) if it is individually identifiable and held or transmitted by a covered entity. For example, health records, patient treatment information and data, health insurance billing information and data.
• GLBA: Financial records are protected by GLBA (Gramm-Leach Bliley Financial Services Modernization Act).
• ITAR and EAR: Export Controlled Research is protected by ITAR (International Traffic in Arms Regulations) and EAR (Export Administration Regulations). For example, dual-use technology used for scientific advancement as well as military applications, see SDCL 1-27-1.5

Data and Information Types: Return Information
Any information and data collected, or generated, by the IRS with regard to any person’s liability, or possible liability, under the Internal Revenue Code (IRC).
Return information and data includes, but is not limited to:
• Information and data, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense;
• Information and data extracted from a return, including names of dependents or the location of business, the taxpayer’s name, address, and identification number. Information and data collected by the IRS about any person’s tax affairs, even if identifiers, such as name, address, and identification number are deleted. FTI may include PII. FTI may include the following PII elements:
  • The name of a person with respect to whom a return is filed
  • His or her mailing address
  • His or her taxpayer identification number
  • Email addresses
  • Telephone numbers
  • Social Security Numbers
  • Bank account numbers
  • Date and place of birth
  • Mother’s maiden name
  • Biometric data (e.g., height, weight, eye color, fingerprints)
  • Any combination of the preceding.
Returns are forms submitted on paper or electronically with return information to the IRS by, or on behalf of, or with respect to any person or entity. Examples can include Forms 1040, 941, 1120 and other informational forms, such as 1099 or W-2.
Data and Information Types: Sensitive
Any information and data not available to the public via the Freedom of Information Act or the State Open Records Laws SDCL 1-27.

Data and Information Types: Trade Secret
Any scientific or technical information and data, design, process, procedure, formula, pattern, compilation, program, device, method, technique, process, strategic planning information or improvement whether manual or electronic that is:
• Valuable and not generally known to the public, including, but not limited to, workstation software programs;
• Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use;
• The subject of efforts that are reasonable under the circumstances to maintain its secrecy, see SDCL 1-27-30

Database
An organized collection of data that supports the processing of the data to provide information.

Data Breach
The unauthorized access by a non-authorized person(s) that result in the use, disclosure, corruption, or theft of State’s data.

Data Mining
The analysis of a data base to extract patterns that can be used to learn more about the user; usually used for marketing purposes

Dataset
A collection of related sets of information and data that is composed of separate elements but can be manipulated as a unit by a workstation.

DDN Intranet
The private, internal network of State government. Executive, judicial branch and constitutional offices connect to the internal aspect of the DDN. The DMZ, K12, REED are examples of external aspects of the DDN.

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

Digital Dakota Network (DDN)
The name of the Statewide workstation network including, but not limited to, data, video, and VoIP services that connects many entities together, including the local and wide area networks of the Executive & Judicial branches, K12 schools and Board of Regents.

Directory
The service that identifies all resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, computers, and peripheral devices such as printers. The directory service allows a user on a network to access any resource without knowing where or how it is physically connected.
Distributed Denial of Service (DDOS)
A botnet is a series of computers compromised. A DDOS attack utilizes one or more botnets to target a single computer or website. The massive amount of botnet traffic overloads the recipient with more data than it can handle, resulting in service delays or outages. The counts indicate the number of attacks targeting the Board of Regents, K12 public schools and State government.

Domain Name
A name owned by a person or organization and consisting of an alphabetical or alphanumerical sequence followed by a suffix. It is used as an Internet address to identify the location of specific Web pages.

Dynamic Naming System (DNS)
An automated means of translating Internet URLs into the equivalent IP address (translating web addresses from near-English into the URL’s digital address).

Easter Egg
A secret message buried in an application.

Employee
Anyone employed directly by the State of South Dakota or employed by any third-party company (contractor or subcontractor) that has a contract to provide work for a State government agency. Contractors and Employees are treated identically throughout the Information Technology Security Policy.

End User Data
Data that is not state data but is non-public or personal data provided by an entity other than the state and is used by someone other than the state.

External Network
Any network that resides outside of the established security perimeter.

Extranet
A controlled private network that allows access to an authorized set of customers.

Fail Over
The process that takes place when a computing resource fails and the functions are automatically moved to another computing resource.

Federal Parent Locator System (FPLS)
The FPLS is an assembly of systems operated by Office of Child Support Enforcement (OCSE), to assist states in locating noncustodial parents, putative fathers, and custodial parties for the establishment of paternity and child support obligations, as well as the enforcement and modification of orders for child support, custody, and visitation. It also identifies support orders or support cases involving the same parties in different states. The FPLS helps federal and state agencies identify over-payments and fraud, and assists with assessing benefits.

Federal Tax Information (FTI)
Tax returns or tax return information received from the IRS or secondary source. Information, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person for any tax, penalty, interest, fine, forfeiture, or other imposition or offense and (2) Information extracted from a return, including names of dependents or the (2) location of business (3) The taxpayer’s name, address, and identification number (4)
ITSP Terms and Acronym Directory

Information collected by the IRS about any person’s tax affairs, even if identifiers, such as name, address, and identification number are deleted.

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

Firewall
A set of related programs, located on a state network gateway server that protects the resources of the state’s network from un-authorized users from other networks.

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

Hot Spot
A physical location where people may obtain Internet access.

Hypervisor
A program that is running one or more virtual machines on a single physical server. See also virtualization.

Identity Theft
When a hacker gains access to enough personal information about someone that they can impersonate one to acquire financing in that person’s name or can gain access to data networks as that person.

Inbound Traffic
Network traffic that originates outside of the enterprise network with a destination inside the network.

Individually Identifiable Health Information (Also known as Personal or Personally Identifiable Health Information)
Is information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Information system
A computer, storage, networking and other physical devices, infrastructure, and processes to create, process, store, secure and exchange all forms of electronic data.

Infrastructure
The technology (hardware and software) that comprise the computer network, phone network, and connections to the Internet including the computer and storage environments.
Infrastructure-as-a-Service
The capability provided to the state to provision, process, and store networks and other fundamental deployments and run arbitrary software, which can include operating systems and applications. The state does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components, for example, host firewalls.

Internet of Things (IoT)
The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to connect and exchange data.

IP Address
The address of a connected device on the State’s IP network. Every desktop and laptop computer, server, scanner, printer, modem, router, smartphone, and tablet is assigned an IP address.

Load Balancing
Dividing the amount of work that a computer has to do between two or more computers so that more work gets done in the same amount of time and, in general, all users get served faster.

MAC Address
A 12-digit hexadecimal address that is preprogrammed into a computer’s network adapter that uniquely identifies that computer on the network.

Malicious Phishing
Email messages disguised to entice the user to enter personal information, network, or banking account information. This information will be sent to the attacker who will use it to steal the user’s identity, money, or to access the state network using the user’s network log-in information to steal data. State Facilitated Phishing is internal phishing of employees to test and evaluate our education and training efforts.

Malicious Software
A program that gives a hacker control of your computer.

Malware
A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim.

Metadata
Data that describes other data. For example, the date modified field in a listing of files is metadata.

Mobile Applications
Applications running on a mobile device like a smart phone or tablet.

Mobile Device
A portable, wireless computing device that is small enough to be used while held in the hand.
Mobile Wi-Fi
A wireless router that acts as a mobile wireless network outbound spot.

NATURAL
A programming language created by Software AG used to interface with ADABAS (Adaptable Data Base System).

Network
A group of computer systems and hardware devices linked together to facilitate the communication between the devices, the sharing of resources, and that make the exchange of information easier.

Non-Public Data
Data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, ordinance, or administrative rule from access by the general public as public information.

On Premise
The IT infrastructure, applications or data that is located at State facilities. Cloud services, SaaS, PaaS, and IaaS would not be considered to be on premise.

Open Source
Software where the copyright holder allows anyone to study, change and distribute the software to anyone for any purpose without paying a licensing fee.

Operating System
A program that controls the operation of a computer and directs the processing of other programs.

Outbound Traffic
This is traffic that originates inside an enterprise network and has a destination outside of the network.

Payment Card Industry (PCI)
Credit card security specifications created by the credit card industry.

Peripherals
Devices that are utilized to enter data and information into a workstation or retrieve data and information from a workstation.

Personally Identifiable Information (PII)
Data that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers, for example, Social Security, driver’s license, and passport numbers. PII also includes financial account information, including account number, credit or debit card numbers, or protected health information (PHI) relating to a person.

Platform
The type of computer system the network is running on. The state has three; the Windows based platform, the mainframe system, and the AS 400 system.
Platform-as-a-Service (PaaS)
The capability provided to the state to deploy onto the cloud infrastructure state-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The state does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Portable Device
Any computing device that can easily be carried that is designed to be held and used in the hands. Portable devices include laptops, tablets, and smartphones. A portable device may also be called a handheld device or mobile device. See also Remote Access Device (RAD).

Portable storage device
A computer media storage device that is capable of being physically transported, including but not limited to USB/flash drives/thumb drives, external hard drives, tapes, CDs, DVDs, and cameras.

Power over Ethernet (POE) switches
A network switch that has Power over Ethernet injection built in.

Presentation Layers
The layer that translates between multiple data formats used by computers that are trying to communicate. The internal communication functions of a computer system are conceptualized by being partitioned into layers, each layer having different functions.

Processor
The actual circuit that processes the instructions that drive a computer.

Production Environment
The setting where applications are run using actual client data as opposed to test environment which is the setting where applications are run using test data.

Program
A sequence of instructions that can be interpreted and executed by a computer.

Protected Data
Data protected by any law, regulation, or industry standard.

Protected Health Information (PHI)
Individually identifiable health information that is:
- Transmitted by electronic media.
- Maintained in electronic media.
- Transmitted or maintained in any other form or medium.
PHI excludes individually identifiable health information in:
- Education records covered by the Family Educational Rights and Privacy Act
- Employment records held by a covered entity in its role as employer.
PHI includes but is not limited to the patient's name, address, patient's doctor, patient's clinic, diagnosis, and prescribed medication.
Reaccreditation
The periodic rescanning of a system looking for security vulnerabilities.

Relative Pathing
A location that is relative to the current directory or folder. By making pathing relative rather than hard coded in an application is less likely to “break” the application because it is looking for a location that has been changed.

Remote Access Device (RAD)
RADs include smartphones like iPhones, Windows and Android phones; mobile computing devices like 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.

Rouge Access Point
A wireless access point (WAP) that has been installed on a secure network without authorization.

Router
A networking device that forwards data packets between computer networks.

Sanitization
A process by which data is irreversibly removed from media or the media is permanently destroyed.

Script
A list of commands used by a program to automate processes on a computer.

Security Activity
Activity meant to enhance and maintain a high level of security. This includes scanning network and email communications with sources and destinations that are outside of the state network. It also includes installing upgraded security software and hardware including: anti-virus software, firewalls, content-filtering software, and intrusion detection software.

Security Incident
A violation of any BIT security policies, privacy policies, or contract agreements involving sensitive information, or the imminent threat of a violation.

Security Infrastructure Team (SIT)
The BIT SIT shall, in coordination with the CISO, recommend technology solutions, written policies and procedures necessary for assuring the security and integrity of State information technology.

Security Operations Team (SOT)
The BIT SOT meets daily to review any cyber security findings or issues with the State Infrastructure within the previous day.
Server
A computer that contains a program that awaits and fulfills requests from other programs in the same or other computers. A given application in a computer may function as a source of requests for services from other programs and also as a server of requests from to other programs.

Service Level Agreement
A written agreement between both the State and the Vendor that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed, and (6) any remedies for performance failures.

SIM card
A smart card that stores a subscriber’s personal identifier, billing information, and data.

Software-as-a-Service (SaaS)
Refers to the capability provided to the State to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The State does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Software Development Life Cycle (SDLC)
A software development methodology used by BIT.

State
Refers to the government of the State of South Dakota when capitalized.

State Contact
The person or persons designated in writing by the State to receive general project communications, adverse event notifications, security incident notifications, or breach notifications.

State Data
Means all data created or in any way originating with the State, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State’s hardware, the Vendor’s hardware or exists in any system owned, maintained, or otherwise controlled by the State or by the Vendor.

State Proprietary Information
The state data plus any other record, information, or document, in any format, that originated with the state.

Statement of Work
A written statement in a solicitation document or contract that describes the State’s service requirements.
**Structure Query Language**
A computer language that is used to manage data, where the data is presented as a set of related tables, and to make queries of a database.

**Social engineering**
Manipulating individuals to provide confidential information or access to a secured site. Purposely “conning” individuals for the purpose of obtaining information to allow for nefarious cyber activities. The tendency of our culture in SD is to be helpful and thus makes us very vulnerable to being socially engineered.

**Software patches**
Changes made to applications to fix security vulnerabilities or impaired functionality.

**Spoofing**
Refers to various practices that conceal the identity of a user account, an email account, or a computer’s Internet Protocol (IP) address that is taking some action. For example, email spoofing involves forging the header of an email message so that the message appears to come from someone other than the true sender.

**System**
A set of interrelating or interdependent component parts forming framework, either software or hardware, connected together to facilitate the flow of data or information.

**Test Environment**
The setting where applications are run using test data as opposed to production environment which is the setting were applications are run using actual client data.

**Time Bomb**
A program that will stop functioning once a set time is reached.

**Trojan Horse**
A malicious program that gives a hacker access to a computer system were the program is disguised as something safe but hides a malicious program.

**User Identification (UID)**
A user, identifier, or account utilized for access control to specify which technical assets and resources an individual or entity can access. Examples are:
- USERID
- A User ID
- SD Domain Account

**Virtual Private Network (VPN)**
A method to encrypt data that is sent or received over the public Internet.

**Virtualization**
The creation of a virtual version of something, such as an operating system, a server, a storage device, or network resources. By allowing multiple virtual versions of something on the same physical server more efficient use is made of network resources.
**Web Probing**
An intelligence gathering effort to gather background information and to identify configuration files and directories of servers providing web content.

**Web Server**
A computer that acts as a server that serves up Web pages and applications.

**Web Server attacks**
Attacks against the servers that connect the state network to the Internet as well as servers that host (store and run) websites. These attacks can be to access data that is not meant to be accessible through the websites via direct probes and software injections from malicious hosts. They can also be meant to prevent users from accessing the websites or the servers. Incidents is the number of successful compromises and Hack Scans are the number of infiltration attempts.

**Wi-Fi**
The 802.11b standard for wireless networking. A standard for delivering digital information over high-frequency, wireless local area networks.

**Wireless Access Point (WAP)**
A networking hardware device that allows a Wi-Fi device to connect to a wired network.

**Wiring closet**
A small room commonly found in institutional buildings where electrical connections are made.

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

**Worm**
A malicious program that reproduces itself so it can spread from one computer to others.

### ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>ADABAS</td>
<td>Adaptable Data Base System</td>
</tr>
<tr>
<td>BA</td>
<td>Business Associate</td>
</tr>
<tr>
<td>BAA</td>
<td>Business Associate Agreement</td>
</tr>
<tr>
<td>BHR</td>
<td>South Dakota Bureau of Human Resources</td>
</tr>
<tr>
<td>BIT</td>
<td>Bureau of Information &amp; Telecommunications</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial off the Shelf Software</td>
</tr>
<tr>
<td>DBMS</td>
<td>Database Management System</td>
</tr>
<tr>
<td>DDN</td>
<td>Digital Dakota Network</td>
</tr>
</tbody>
</table>
## ITSP Terms and Acronym Directory

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DDOS</strong></td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td><strong>DMZ</strong></td>
<td>De-Militarized Zone</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>Dynamic Naming System</td>
</tr>
<tr>
<td><strong>DOH</strong></td>
<td>South Dakota Department of Health</td>
</tr>
<tr>
<td><strong>DSN</strong></td>
<td>Data Source Name</td>
</tr>
<tr>
<td><strong>DSS</strong></td>
<td>South Dakota Department of Social Services</td>
</tr>
<tr>
<td><strong>EAR</strong></td>
<td>Export Administration Regulations</td>
</tr>
<tr>
<td><strong>FERPA</strong></td>
<td>Family Educational Rights and Privacy Act</td>
</tr>
<tr>
<td><strong>FPLS</strong></td>
<td>Federal Parent Locator System</td>
</tr>
<tr>
<td><strong>FTI</strong></td>
<td>Federal Tax Information</td>
</tr>
<tr>
<td><strong>FTP</strong></td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td><strong>GLBA</strong></td>
<td>Gramm-Leach Bliley/Financial Services Modernization Act</td>
</tr>
<tr>
<td><strong>HIPPA</strong></td>
<td>Health Information Portability and Accountability Act</td>
</tr>
<tr>
<td><strong>IaaS</strong></td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td><strong>IEEE</strong></td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td><strong>IoT</strong></td>
<td>Internet of Things</td>
</tr>
<tr>
<td><strong>IPv4</strong></td>
<td>Internet Protocol version 4</td>
</tr>
<tr>
<td><strong>IPv6</strong></td>
<td>Internet Protocol version 6</td>
</tr>
<tr>
<td><strong>IRS</strong></td>
<td>Internal Revenue Service</td>
</tr>
<tr>
<td><strong>ITAR</strong></td>
<td>International Traffic in Arms Regulations</td>
</tr>
<tr>
<td><strong>MANET</strong></td>
<td>Mobile Ad Hoc Network</td>
</tr>
<tr>
<td><strong>MIFI</strong></td>
<td>Mobile Wi-Fi</td>
</tr>
<tr>
<td><strong>MMIS</strong></td>
<td>Medicaid Management Information System</td>
</tr>
<tr>
<td><strong>MOU</strong></td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td><strong>NIST</strong></td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td><strong>OWASP</strong></td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td><strong>PaaS</strong></td>
<td>Platform-as-a-Service</td>
</tr>
</tbody>
</table>
ITSP Terms and Acronym Directory

PCI
Payment Card Industry

PII
Personally Identifiable Information

RAD
Remote Access Device

RADIUS
Remote Authentication Dial-In User Service

SaaS
Software-as-a-Service

SDLC
Software Development Life Cycle

SLA
Service Level Agreement

SNMP
Simple Network Management Protocol

SOC
Security Operations Center

SOT
Security Operations Team

SOW
Statement of Work

SSID
Service Set Identifier

SQL
Structure Query Language

TACACS+
Terminal Access Controller Access Control System Plus

UAT
User Assurance Testing

UID
User Identification

VOIP
Voice Over Internet Protocol

VPN
Virtual Private Network

WAN
Wide Area Network

WANET
Wireless Ad Hoc Network

WAP
Wireless Access Point
Attachment C
Security and Vendor Questions

Vendors: The following questions are asked to help BIT determine the best ways to integrate your product with the State’s technology infrastructure. Some questions may not apply but please review all of them. You will see that this is divided into sections to help identify the point of the questions.

Use the last column as needed to explain your answers. Please note that many questions explicitly ask you to explain your response.

Where we feel that a Yes/No/NA response is not appropriate, the cell has been greyed out, and comments are expected. Do not skip.

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

### Section: System Security - Applicable to All Proposals
The following questions pertain to all vendors, contractors or third-parties engaged in this system, and pertain to relevant security practices for your system, coding, and business processes.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>DAT</td>
<td>Is a user required to change their password? How often? What are the complexity requirements for the passwords? (BIT password requirements are available in Section 230.67.4.4 of the Information Technology Security Policy which can be supplied upon request).</td>
<td>YES</td>
</tr>
<tr>
<td>A2</td>
<td>DEV TEL</td>
<td>Will the system implement its own level of security?</td>
<td>YES</td>
</tr>
<tr>
<td>A3</td>
<td>DAT TEL</td>
<td>Will the system provide Internet security functionality on public portals using encrypted network/secure socket layer connections in line with current recommendations of the Open Web Application Security Project (OWASP)?</td>
<td>YES</td>
</tr>
<tr>
<td>A4</td>
<td>TEL</td>
<td>Will the system provide Internet security functionality on a public portal to include firewalls?</td>
<td>YES</td>
</tr>
<tr>
<td>A5</td>
<td>PMO</td>
<td>Will the system distinguish between local versus global administrators where local administrators have rights to user management only for the program area that they are associated with and global administrators have rights for the entire system?</td>
<td>YES</td>
</tr>
<tr>
<td>A6</td>
<td>DAT TEL</td>
<td>Does the application contain mitigations for risks associated to uncontrolled login attempts (response latency, re-Captcha, lockout, IP filtering, Multi Factor authentication)? Which mitigations are in place? What are the optional mitigations?</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>A7</td>
<td>DAT TEL</td>
<td>Are account credentials hashed and encrypted when stored?</td>
<td></td>
</tr>
<tr>
<td>A8</td>
<td>DAT TEL</td>
<td>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. Scanning would also take place annually as well as when there are code changes. Are either of these an issue? If so, please explain.</td>
<td></td>
</tr>
<tr>
<td>A9</td>
<td>DAT</td>
<td>Will SSL traffic be decrypted and inspected?</td>
<td></td>
</tr>
<tr>
<td>A10</td>
<td>PMO</td>
<td>Will organizations other than the State of South Dakota have access to our data?</td>
<td></td>
</tr>
<tr>
<td>A11</td>
<td>PMO</td>
<td>Will the State’s data be protected?</td>
<td></td>
</tr>
<tr>
<td>A12</td>
<td>DEV TEL</td>
<td>Describe the training your company offers related to defining security requirements, secure architecture and design, secure coding practices, and security testing.</td>
<td></td>
</tr>
<tr>
<td>A13</td>
<td>DEV TEL</td>
<td>Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?</td>
<td></td>
</tr>
<tr>
<td>A14</td>
<td>DEV</td>
<td>Are there some requirements for security that are “structured” as part of general releasability of a product and others that are “as needed” or “custom” for a particular release?</td>
<td></td>
</tr>
<tr>
<td>A15</td>
<td>TEL</td>
<td>What process is utilized by your company to prioritize security related enhancement requests?</td>
<td></td>
</tr>
<tr>
<td>A16</td>
<td>TEL</td>
<td>What threat assumptions were made, if any, when designing protections for the software and information assets processed?</td>
<td></td>
</tr>
<tr>
<td>A17</td>
<td>TEL</td>
<td>How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?</td>
<td></td>
</tr>
<tr>
<td>A18</td>
<td>TEL</td>
<td>What security criteria, if any, are considered when selecting third-party suppliers?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>A19</td>
<td>TEL</td>
<td>How has the software been measured/assessed for its resistance to identified, relevant attack patterns such as Common Vulnerabilities &amp; Exposures (CVE®) or Common Weakness Enumerations (CWEs)? How have the findings been mitigated?</td>
<td></td>
</tr>
<tr>
<td>A20</td>
<td>TEL</td>
<td>Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available.</td>
<td></td>
</tr>
<tr>
<td>A21</td>
<td>DAT</td>
<td>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?</td>
<td></td>
</tr>
<tr>
<td>A22</td>
<td>DAT</td>
<td>Has the product undergone any penetration testing? If yes, when, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated?</td>
<td></td>
</tr>
<tr>
<td>A23</td>
<td>DEV</td>
<td>Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)? If yes, please explain.</td>
<td></td>
</tr>
<tr>
<td>A24</td>
<td>DAT</td>
<td>Does your company publish a security section on its website? If so, do security researchers have the ability to report security issues?</td>
<td></td>
</tr>
<tr>
<td>A25</td>
<td>DAT</td>
<td>Does your company have an executive-level officer responsible for the security of your company’s software products and/or processes?</td>
<td></td>
</tr>
<tr>
<td>A26</td>
<td>DAT</td>
<td>Are security requirements developed independently of the rest of the requirements engineering activities? Or are they integrated into the mainstream requirements activities?</td>
<td></td>
</tr>
<tr>
<td>A27</td>
<td>DAT</td>
<td>Does the software have any security critical dependencies or need additional controls from other software (e.g., operating system, directory service, application), firmware, or hardware? If yes, please describe.</td>
<td></td>
</tr>
<tr>
<td>A28</td>
<td>DAT</td>
<td>What risk management measures are used during the software’s design to mitigate risks posed by use of third-party components?</td>
<td></td>
</tr>
<tr>
<td>A29</td>
<td>DAT</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>A30</td>
<td>DEV</td>
<td>Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle? Explain.</td>
<td></td>
</tr>
<tr>
<td>A31</td>
<td>TEL</td>
<td>What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?</td>
<td></td>
</tr>
<tr>
<td>A32</td>
<td>DAT</td>
<td>Is two-factor authentication used for administrative control of all security devices and critical information systems?</td>
<td></td>
</tr>
<tr>
<td>A33</td>
<td>DAT TEL</td>
<td>Do you have an automated security event management system?</td>
<td></td>
</tr>
<tr>
<td>A34</td>
<td>DAT</td>
<td>Are security logs and audit trails protected from tampering or modification?</td>
<td></td>
</tr>
<tr>
<td>A35</td>
<td>DAT</td>
<td>It is State policy that if your system connects to another system providing SaaS, IaaS, or PaaS that this system has a security scan. The State would want to scan a test system; not a production system. Is this an issue? If so, please explain.</td>
<td></td>
</tr>
<tr>
<td>A36</td>
<td>DAT x</td>
<td>A) Will the system support authentication?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>B) Does the system give clues about valid username or password content or structure, for example when a user forgets their username or after a failed login attempt?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C) Are usernames and passwords generated by the system using user-specific information such as last name or birthdate? If Yes to these, please explain.</td>
<td></td>
</tr>
<tr>
<td>A37</td>
<td>DEV</td>
<td>Are security-specific regression tests performed during the development process? If yes, how frequently are the tests performed?</td>
<td></td>
</tr>
<tr>
<td>A38</td>
<td>TEL</td>
<td>What type of firewalls (or application gateways) do you use? How are they monitored/managed?</td>
<td></td>
</tr>
<tr>
<td>A39</td>
<td>TEL</td>
<td>What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?</td>
<td></td>
</tr>
<tr>
<td>A40</td>
<td>DAT TEL</td>
<td>What are your procedures for intrusion detection, incident response, and incident investigation/escalation?</td>
<td></td>
</tr>
<tr>
<td>A41</td>
<td>DAT</td>
<td>How do you control physical and electronic access to the log files? Are log files consolidated to single servers?</td>
<td></td>
</tr>
<tr>
<td>A42</td>
<td>DAT TEL</td>
<td>Describe your security testing processes.</td>
<td></td>
</tr>
<tr>
<td>A43</td>
<td>DAT TEL</td>
<td>Do you have a BYOD policy that allows your staff to put any sort of sensitive or legally protected State data on their device personal device(s) or other non-company owned system(s)?</td>
<td></td>
</tr>
<tr>
<td>A44</td>
<td>DAT TEL</td>
<td>Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data? If yes, please explain your practices on multifactor authentication including the authentication level used as defined in NIST 800-63 in your explanation. If no, do you plan on going to multifunction authentication? If so, when?</td>
<td></td>
</tr>
<tr>
<td>A45</td>
<td>PMO</td>
<td>Will this system provide the capability to track data entry/access by the person, date and time?</td>
<td></td>
</tr>
<tr>
<td>A46</td>
<td>DAT DEV PMO TEL</td>
<td>Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.</td>
<td></td>
</tr>
</tbody>
</table>
| A47  | DAT TEL | a. Do you have a SOC 2 audit report?  
|    |   | b. Is the audit done annually?  
|    |   | c. Does the audit cover all 5 of the trust principles?  
|    |   | d. Does the audit include subservice providers?  
|    |   | e. Has the auditor always been able to attest to an acceptable audit result?  
|    |   | f. Will you provide a copy of your latest SOC 2 audit upon request, a redacted version is acceptable. |
| A48  | DAT TEL | Are you providing a device or software that is a part of the Internet of Things (IoT)? If yes, what is your process for ensuring the
software on your IoT devices that are connected to the state’s system, either permanently or intermittently, are maintained and/or updated?

**Section: Hosting**

*Only for vendor/cloud hosted applications, systems, databases and any other technology not hosted on the State’s infrastructure.*

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>B1</td>
<td>PMO</td>
<td>Typically the State of South Dakota prefers to host all systems. In the event that the State decides that it would be preferable for the vendor to host the system, is this an option?</td>
<td>YES NO NA</td>
</tr>
<tr>
<td>B2</td>
<td>PMO</td>
<td>Are there expected periods of time where the application will be unavailable for use?</td>
<td></td>
</tr>
<tr>
<td>B3</td>
<td>DAT</td>
<td>If you have agents or scripts executing on servers of hosted applications and what are the procedures for reviewing the security of these scripts or agents?</td>
<td></td>
</tr>
<tr>
<td>B4</td>
<td>DAT</td>
<td>What are the procedures and policies used to control access to the servers? How are audit logs maintained?</td>
<td></td>
</tr>
<tr>
<td>B5</td>
<td>DAT</td>
<td>Do you have a formal disaster recovery plan? Please explain what actions will be taken to recover from a disaster? Are warm or hot backups available?</td>
<td></td>
</tr>
<tr>
<td>B6</td>
<td>DAT</td>
<td>What are the set of controls to ensure separation of data and security information between different customers that are physically located in the same data center? On the same host server?</td>
<td></td>
</tr>
<tr>
<td>B7</td>
<td>DAT</td>
<td>What are your data backup policies and procedures? How frequently are your backup procedures verified?</td>
<td></td>
</tr>
<tr>
<td>B8</td>
<td>DAT</td>
<td>Are you or if the data is being hosted by a subservice provider are they FedRAMP certified?</td>
<td></td>
</tr>
</tbody>
</table>
If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with:
- Security for their I/T systems;
- Staff vetting;
- Staff security training?

If yes, summarize the contractual requirements.

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

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

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

<table>
<thead>
<tr>
<th>B9</th>
<th>DAT</th>
<th>DEV</th>
<th>TEL</th>
</tr>
</thead>
</table>
|    | If any cloud services are provided by a third-party, do you have contractual requirements with them dealing with:  
  · Security for their I/T systems;  
  · Staff vetting;  
  · Staff security training? |
|    | If yes, summarize the contractual requirements. |
|    | If yes, how do you evaluate the third-party’s adherence to the contractual requirements? |

<table>
<thead>
<tr>
<th>B10</th>
<th>DAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>If your application is hosted by you or a third party, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal? If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B11</th>
<th>DAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Do you use a security checklist when standing up any outward facing system?</td>
<td></td>
</tr>
<tr>
<td>b. Do you test after the system was stood up to make sure everything in the checklist was correctly set?</td>
<td></td>
</tr>
<tr>
<td>c. Will you provide the State with a copy of your checklist?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B12</th>
<th>DAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are your Internet of Things (IoT) devices segmented from your network?</td>
<td></td>
</tr>
</tbody>
</table>

---

**Section: Database**

**Applies to any application that stores data.**

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>DAT</td>
<td>Will the system require a database?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>DAT</td>
<td>Will the system infrastructure require database replication?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>DAT</td>
<td>Will the system require transaction logging for database recovery?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td>DAT</td>
<td>How does data enter the system (transactional or batch or both)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C5</td>
<td>PMO</td>
<td>Is the system data exportable by the user for use in tools like Excel or Access?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Vendor and Security Questions last revised April 18, 2018
### Vendor Process - Applicable to all proposals

The following questions pertain to all vendors, contractors or third-parties engaged in this system, and pertain to relevant business practices.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
<th>Explain answer as needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>DAT PMO</td>
<td>Will the vendor provide assistance with installation?</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>D2</td>
<td>DAT DEV PMO TEL</td>
<td>Does your company have a policy and process for supporting/requiring professional certifications? If so, how do you ensure certifications are valid and up-to date?</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>D3</td>
<td>TEL</td>
<td>In preparation for release, are undocumented functions in the software disabled, test/debug code removed, and source code comments sanitized?</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>D4</td>
<td>DEV</td>
<td>What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing and integrated testing)?</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>D5</td>
<td>TEL</td>
<td>Who and when are security tests performed on the product? Are tests performed by an internal test team, by an independent third party, or by both?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D6</td>
<td>DEV</td>
<td>Are misuse test cases included to exercise potential abuse scenarios of the software?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D7</td>
<td>TEL</td>
<td>What release criteria does your company have for its products with regard to security?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D8</td>
<td>DEV</td>
<td>What controls are in place to ensure that only the accepted/released software is placed on media for distribution?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D9</td>
<td>DAT</td>
<td>Is there a Support Lifecycle Policy within the organization for the software in question? Does it outline and establish a consistent and predictable support timeline?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D10</td>
<td>DAT</td>
<td>How will patches and/or Service Packs be distributed to the Acquirer?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D11</td>
<td>DEV</td>
<td>What services does the help desk, support center, or (if applicable) online support system offer and when are these services available?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D12</td>
<td>DAT</td>
<td>How extensively are patches and Service Packs tested before they are released?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D13</td>
<td>DAT</td>
<td>Can patches and Service Packs be uninstalled? Are the procedures for uninstalling a patch or Service Pack automated or manual?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D14</td>
<td>DAT</td>
<td>How are reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, and prioritized?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D15</td>
<td>DAT</td>
<td>How do you set the relative severity of defects and how do you prioritize their remediation?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D16</td>
<td>DAT</td>
<td>What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D17</td>
<td>DAT</td>
<td>Are third-party developers contractually required to follow your configuration management policies?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D18</td>
<td>DEV</td>
<td>What policies and processes does your company use to verify that software components do not contain unintended, “dead,” or malicious code? What tools are used?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D19</td>
<td>DEV</td>
<td>How is the software provenance verified (e.g. any checksums or signatures)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>D20</strong></td>
<td><strong>DEV</strong></td>
<td>Does the documentation explain how to install, configure, and/or use the software securely? Does it identify options that should not normally be used because they create security weaknesses?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D21</strong></td>
<td><strong>DAT</strong></td>
<td>Does your company’s defect classification scheme include security categories?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D22</strong></td>
<td><strong>DAT</strong></td>
<td>Is a validation test suite or diagnostic available to validate that the application software is operating correctly and in a secure configuration following installation?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D23</strong></td>
<td><strong>DEV</strong></td>
<td>Does your company develop security measurement objectives for phases of the SDLC? Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D24</strong></td>
<td><strong>DEV</strong></td>
<td>How is the assurance of software produced by third-party developers assessed?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D25</strong></td>
<td><strong>DEV</strong></td>
<td>Does your company have a vulnerability management and reporting policy? Is it available for review?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D26</strong></td>
<td><strong>DAT</strong></td>
<td>What are the procedures for evaluating any vendor security alerts and installing patches and Service Packs?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D27</strong></td>
<td><strong>DAT</strong></td>
<td>Is testing done after changes are made to servers? What are your rollback procedures in the event of problems resulting from installing a patch or Service Pack?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D28</strong></td>
<td><strong>DAT</strong></td>
<td>What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D29</strong></td>
<td><strong>DAT</strong></td>
<td>How are virus prevention, detection, correction, and updates handled for the products?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D30</strong></td>
<td><strong>DAT</strong></td>
<td>Do you perform regular reviews of system and network logs for security issues?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D31</strong></td>
<td><strong>DAT</strong></td>
<td>Do you provide security performance measures to the customer at regular intervals?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D32</strong></td>
<td><strong>DAT</strong></td>
<td>Is there an installation guide available and will you provide a copy to the State?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>D33</strong></td>
<td><strong>DAT DEV PMO</strong></td>
<td>Will the implementation plan include user acceptance testing?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D34</strong></td>
<td><strong>DAT DEV PMO TEL</strong></td>
<td>Will the implementation plan include performance testing?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D35</strong></td>
<td><strong>DAT DEV PMO TEL</strong></td>
<td>What technical documentation will be provided to the State?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D36</strong></td>
<td><strong>DEV PMO</strong></td>
<td>Will there be documented test cases for future releases including any customizations done for the State of South Dakota?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D37</strong></td>
<td><strong>PMO</strong></td>
<td>Is the user manual electronically available and can the manual be printed?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D38</strong></td>
<td><strong>PMO</strong></td>
<td>Describe your Support and on-line assistance options and any additional costs associated with the options.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D39</strong></td>
<td><strong>DAT PMO</strong></td>
<td>Is there a method established to communicate availability of system updates?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D40</strong></td>
<td><strong>DEV PMO</strong></td>
<td>If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D41</strong></td>
<td><strong>DEV PMO</strong></td>
<td>Has your company ever conducted a project where your product was load tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D42</strong></td>
<td><strong>DEV PMO</strong></td>
<td>Have you ever created a User Acceptance Test plan and test cases? If yes, what were the test cases? Do you do software assurance?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D43</strong></td>
<td><strong>PMO</strong></td>
<td>Is there a strategy for mitigating unplanned disruptions and what is it?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D44</strong></td>
<td><strong>DAT</strong></td>
<td>Please explain the pedigree of the software. Include in your answer who are the people, organization and processes that created the software.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D45</strong></td>
<td><strong>DAT</strong></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D46</td>
<td>TEL</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D47</td>
<td>DEV</td>
<td>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)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D48</td>
<td>DAT, DEV</td>
<td>Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D49</td>
<td>DAT, DEV, TEL</td>
<td>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?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D50</td>
<td>DEV</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D51</td>
<td>DAT</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D52</td>
<td>DEV</td>
<td>When does security testing occur during the SDLC (e.g., unit level, subsystem, system, certification and accreditation)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D53</td>
<td>DAT, TEL</td>
<td>How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D54</td>
<td>DAT, TEL</td>
<td>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?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D55</td>
<td>DAT</td>
<td>How frequently is the security tests performed? Are the tests performed by internal resources or by a third party?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D56</td>
<td>DAT DEV</td>
<td>Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D57</td>
<td>DAT TEL</td>
<td>What is your process for ensuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D58</td>
<td>DAT TEL</td>
<td>It is State policy that all Vendor/Contractor Remote Access to systems for support and maintenance on the State Network will only be allowed through Citrix Netscaler. Would this affect the implementation of the system?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D59</td>
<td>PMO TEL</td>
<td>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?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| D60 | DAT DEV PMO TEL | (For PHI only) a. Have you done a risk assessment? If yes, will you share it?  
b. If you have not done a risk assessment, would you be willing to do one based on the Health and Human Services assessment tool (https://www.healthit.gov/providers-professionals/security-risk-assessment-tool)? If yes, will you share it? The State is willing to sign a Non-disclosure Agreement before viewing any risk assessment.  
c. If you have not done a risk assessment, when are you planning on doing one? |
| D61 | DEV PMO | Will your web site and/or web application conform to the accessibility requirements of the Web Content Accessibility Guidelines 2.0? If not discuss what steps you take to make your web site and/or web application accessible. The guidelines can be found at http://www.w3.org/TR/WCAG20/.
### Section: Software Development - Applicable to All Proposals

The following questions pertain to the tools and third-party components used to develop your product.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
<th>Explain answer as needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>DEV PMO x</td>
<td>What is the development technologies used for this system? Please indicate version as appropriate</td>
<td>YES  NO  NA</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASP.Net</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VB.Net</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C#.Net</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>.NET Framework</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Java/JSP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MS SQL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E2</td>
<td>DAT TEL</td>
<td>Is this a browser based User Interface?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E3</td>
<td>DEV PMO</td>
<td>Will the system have any workflow requirements?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E4</td>
<td>DAT</td>
<td>Can the system be implemented via Citrix?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E5</td>
<td>DAT</td>
<td>Will the system print to a Citrix compatible networked printer?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E6</td>
<td>TEL</td>
<td>If your application does not run under the latest Microsoft operating system, what is your process for updating the application?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E7</td>
<td>DEV</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E8</td>
<td>TELx</td>
<td>Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, JavaFX, Microsoft Silverlight, PHP or QuickTime? If yes, explain?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vendor and Security Questions last revised April 18, 2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E9</td>
<td>DEV</td>
<td>In order to connect to other applications or data, will the State be required to develop custom interfaces?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E10</td>
<td>DEV</td>
<td>In order to fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E11</td>
<td>DEV</td>
<td>Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E12</td>
<td>DAT</td>
<td>If the product is hosted at the State, will there be any third-party application(s) or system(s) installed or embedded to support the product (for example, database software, run libraries)? If so, please list those third-party application(s) or system(s).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E13</td>
<td>DEV</td>
<td>What coding and/or API standards are used during development of the software?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E14</td>
<td>DEV</td>
<td>Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E15</td>
<td>DEV</td>
<td>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?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E16</td>
<td>DEV</td>
<td>Does the exception-handling mechanism provide more than one option for responding to a fault? If so, can the exception handling options be configured by the administrator or overridden?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E17</td>
<td>DEV</td>
<td>What percentage of code coverage does your testing provide?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E18</td>
<td>DAT</td>
<td>A) Will the system infrastructure involve the use of email?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>B) Will the system infrastructure require an interface into the State’s email infrastructure?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C) Will the system involve the use of bulk email distribution to State users? Client users? In what quantity will emails be sent, and how frequently?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E19</td>
<td>TEL</td>
<td>A) Does your application use Java?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>B) If yes, is it locked into a certain version?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>C) Will it use the latest version of Java?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>D) If so, what is your process for updating the application?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>BIT</td>
<td>Question</td>
<td>Response</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-----</td>
<td>--------------------------------------------------------------------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>E20</td>
<td>DAT</td>
<td>Explain how and where the software validates (e.g., filter with white listing) inputs from untrusted sources before being used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E21</td>
<td>TEL</td>
<td>Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user)? Is it designed to isolate and minimize the extent of damage possible by a successful attack?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E22</td>
<td>TEL</td>
<td>Does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E23</td>
<td>DEV</td>
<td>Do you use open source software or libraries? If yes, do you check for vulnerabilities in your software or library that are listed in:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. Common Vulnerabilities and Exposures (CVE) database?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. Open Source Vulnerability Database (OSVDB)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. Open Web Application Security Project (OWASP) Top Ten?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Section: Infrastructure - Applicability to all systems**

This pertains to how your system interacts with the State's technology infrastructure.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>YES</th>
<th>NO</th>
<th>NA</th>
<th>Explain answer as needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>TEL</td>
<td>Is there a workstation install requirement?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F2</td>
<td>DAT</td>
<td>Will the system infrastructure have a special backup requirement?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F3</td>
<td>DAT</td>
<td>Will the system infrastructure have any processes that require scheduling?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F4</td>
<td>DAT</td>
<td>The State expects to be able to move your product without cost for Disaster Recovery purposes and to maintain high availability. Will this be an issue?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F5</td>
<td>TEL</td>
<td>Will the network communications meet Institute of Electrical and Electronics Engineers (IEEE) standard TCP/IP (IPv4, IPv6) and use either standard ports or State-defined ports as the State determines?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F6</td>
<td>DAT</td>
<td>It is State policy that all systems must be compatible with BIT’s dynamic IP addressing solution (DHCP). Would this affect the implementation of the system?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F7</td>
<td>TEL</td>
<td>It is State policy that all software must be able to use either standard Internet Protocol ports or Ports as defined by the State of South Dakota BIT Network Technologies. Would this affect the implementation of the system? If yes, explain.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F8</td>
<td>DAT</td>
<td>It is State policy that all HTTP/SSL communication must be able to be run behind State of South Dakota content switches and SSL accelerators for load balancing and off-loading of SSL encryption. If need is determined by the State, would this affect the implementation of the system? If yes, explain.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F9</td>
<td>DAT</td>
<td>The State has a virtualize first policy that requires all new systems to be configured as virtual machines. Would this affect the implementation of the system? If yes, explain.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F10</td>
<td>TEL</td>
<td>It is State policy that all access from outside of the State of South Dakota’s private network will be limited to set ports as defined by the State and all traffic leaving or entering the State network will be monitored. Would this affect the implementation of the system? If yes, explain.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F11</td>
<td>TEL</td>
<td>It is State policy that systems must support NAT and PAT running inside the State Network. Would this affect the implementation of the system? If yes, explain.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F12</td>
<td>TEL</td>
<td>It is State policy that systems must not use dynamic TCP or UDP ports unless the system is a well-known one that is state firewall supported (FTP, TELNET, HTTP, SSH, etc.). Would this affect the implementation of the system? If yes, explain.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F13</td>
<td>DAT</td>
<td>The State of South Dakota currently schedules routine maintenance from 0400 to 0700 on Tuesday mornings for our non-mainframe environments and once a month from 0500 to 1200 for our mainframe environment. Systems will be offline during this scheduled maintenance time periods. Will this have a detrimental effect to the system?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F14</td>
<td>DEV PMO</td>
<td>Does your product run on Citrix Metaframe?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
<td>------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F15</td>
<td>PMO TEL</td>
<td>Please describe the types and levels of network access your system/application will require. This should include, but not be limited to: TCP/UDP ports used, protocols used, source and destination networks, traffic flow directions, who initiates traffic flow, whether connections are encrypted or not, and types of encryption used. Vendor should specify what access requirements are for user access to the system and what requirements are for any system level processes. Vendor should describe all requirements in details and provide full documentation as to the necessity of the requested access.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F16</td>
<td>PMO TEL</td>
<td>List any hardware or software you propose to use that is not State standard, the standards can be found at <a href="http://bit.sd.gov/">http://bit.sd.gov/</a>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F17</td>
<td>DAT</td>
<td>If your application is hosted on the State’s infrastructure, will it require a dedicated environment?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F18</td>
<td>DEV PMO</td>
<td>Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F19</td>
<td>DAT</td>
<td>Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F20</td>
<td>DAT</td>
<td>What are your policies and procedures for hardening servers?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F21</td>
<td>DAT TEL</td>
<td>Explain or provide a diagram of the architecture for the application including security mitigation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F22</td>
<td>TEL TEL</td>
<td>What is your process for ensuring default remote login protocols and default passwords are disabled on Internet of Things (IoT) devices that are connected to your system either permanently or intermittently?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F23</td>
<td>DAT</td>
<td>Can the system be integrated with our enterprise Active Directory to ensure access is controlled?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F24</td>
<td>TEL TEL</td>
<td>It is State policy that no equipment can be connected to State Network without direct approval of BIT Network Technologies. Would this affect the implementation of the system?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**F25** 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

**F26** All network systems must operate within the current configurations of the State of South Dakota’s firewalls, switches, IDS/IPS and desktop security infrastructure. Would this affect the implementation of the system?

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

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

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

---

**Section: Business Process - Applicability to all proposals**

These questions relate to how your business model interacts with the State of South Dakota.

<table>
<thead>
<tr>
<th>#</th>
<th>BIT</th>
<th>Question</th>
<th>Response</th>
<th>Explain answer as needed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **G1** | **DAT** | If your application is hosted on a dedicated environment within the State's infrastructure, are all costs for your software licenses in addition to third-party software (i.e. MS-SQL, MS Office, and Oracle) included in your cost proposal?  
If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized? |
| **G2** | **PMO** | Explain the software licensing model. |
| **G3** | **DAT** | Is on-site assistance available? If so, is there a charge? |
| **DEV** | **PMO** | Will you provide customization of the system if required by the State of South Dakota?  
If yes, are there any additional costs for the customization? |
<p>| <strong>G4</strong> | <strong>PMO</strong> | Will the source code for the system be put in escrow for the State of South Dakota? If yes, will you pay the associated escrow fees? |
| <strong>G5</strong> | <strong>PMO</strong> | Explain the basis on which pricing could change for the State based on your licensing model. |
| <strong>G6</strong> | <strong>PMO</strong> | 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? |
| <strong>G7</strong> | <strong>PMO</strong> | Will the State of South Dakota own the data created in your hosting environment? |
| <strong>G8</strong> | <strong>PMO</strong> | Will the State acquire the data at contract conclusion? |
| <strong>G9</strong> | <strong>PMO</strong> | Will the State’s data be used for any other purposes other than South Dakota’s usage? |
| <strong>G10</strong> | <strong>PMO</strong> | Has your company ever filed for Bankruptcy under U.S. Code Chapter 11? If so, please provide dates for each filing and describe the outcome. |
| <strong>G11</strong> | <strong>DAT</strong> | Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain. |</p>
<table>
<thead>
<tr>
<th>G13</th>
<th>DAT</th>
<th>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).</th>
</tr>
</thead>
<tbody>
<tr>
<td>G14</td>
<td>DAT</td>
<td>Will you provide on-site support 24x7 to resolve security incidents?</td>
</tr>
<tr>
<td>G15</td>
<td>DEV</td>
<td>What training programs, if any, are available or provided through the supplier for the software? Do you offer certification programs for software integrators? Do you offer training materials, books, computer-based training, online educational forums, or sponsor conferences related to the software?</td>
</tr>
<tr>
<td>G16</td>
<td>DAT TEL</td>
<td>Are help desk or support center personnel internal company resources or are these services outsourced to third parties?</td>
</tr>
<tr>
<td>G17</td>
<td>DAT</td>
<td>Are any of the services you plan to use located offshore (examples include data hosting, data processing, help desk and transcription services)?</td>
</tr>
<tr>
<td>G18</td>
<td>DAT</td>
<td>Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?</td>
</tr>
<tr>
<td>G19</td>
<td>DAT</td>
<td>What are your customer confidentiality policies? How are they enforced?</td>
</tr>
<tr>
<td>G20</td>
<td>DAT</td>
<td>Are you ISO 27001 certified? Is the certification done annually? Will you provide a copy of your certification report?</td>
</tr>
<tr>
<td>G21</td>
<td>DAT</td>
<td>(Use if PHI is involved) Are you HITRUST certified? Is the certification done annually? Will you provide a copy of your assessment?</td>
</tr>
<tr>
<td>G22</td>
<td>DAT PMO x</td>
<td>Will this application now or possibly in the future share PHI with other entities on other networks, be sold to another party or be accessed by anyone outside the US?</td>
</tr>
<tr>
<td>G23</td>
<td>DAT</td>
<td>If the product is hosted at the State, will there be a request to include an application to monitor license compliance?</td>
</tr>
<tr>
<td>G24</td>
<td>DAT PMO</td>
<td>Is telephone assistance available for both installation and use? If yes, are there any additional charges?</td>
</tr>
</tbody>
</table>