STATE OF SOUTH DAKOTA
DEPARTMENT OF HEALTH
PIERRE, SD 57501

Contract Lifecycle Management System

PROPOSALS ARE DUE NO LATER THAN June 16th, 2023, at 5:00pm CST

RFP #: 23-0901001-022

State POC:
Amanda Shoop
Department of Health

EMAIL:
amanda.shoop@state.sd.us

READ CAREFULLY

FIRM NAME:

AUTHORIZED SIGNATURE:

ADDRESS:

TYPE OR PRINT NAME:

CITY/STATE:

TELEPHONE NO:

ZIP (9 DIGITS):

FAX NO:

E-MAIL:

PRIMARY CONTACT INFORMATION

CONTACT NAME:

TELEPHONE NO:

FAX NO:

E-MAIL:

---

1 GENERAL INFORMATION

1.1 BIT STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State of South Dakota's (the "State") standard I/T contract terms listed in Appendix A, along with any additional contract terms as negotiated by the parties. As part of the negotiation process the contract terms listed in Appendix A may be altered or deleted. The offeror must indicate in its response any issues it has with specific contract terms. If the offeror does not indicate that there are any issues with any contract terms, then the State will assume those terms are acceptable to the offeror. There is also a list of technical questions, Security and Vendor Questions which is attached as Appendix B, the offeror must complete. These questions may be used in the proposal evaluation. It is preferred that the offeror's response to these questions is provided as a separate document from the RFP response. If the offeror will be hosting the solution, the file name must be "(Your Name) Hosted Security and Vendor Questions Response". If the solution will be hosted by the State, the file must be named "(Your Name) Security and Vendor Questions Response State Hosted". If the solution is not a hosted solution, the file name must be "(Your Name) Security and Vendor Questions Response". If there are multiple non-hosted solutions, please provide some designation in the file name that indicates which proposal it goes to. This document cannot be a scanned document but must be an original. If the offeror elects to make the Security and Vendor Questions part of its response, the questions must be clearly indicated in the proposal's Table of Contents. A single numbering system must be used throughout the proposal.

1.2 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

The South Dakota Department of Health (SD DOH) executes over 1000 contracts per year and spends approximately 115 million dollars for professional services, supplies, software, and Consultants. Currently, our contract process is fragmented, and we desire to centralize the function for better monitoring, control, authorization, and auditing.

The SD DOH is seeking proposals from qualified vendors to address the requirements stated in this RFP. The purpose of this RFP is to provide the SD DOH with a Contract Lifecycle Management System. In addition, this system may have potential to be developed for statewide agency use.

1.3 ISSUING OFFICE AND RFP REFERENCE NUMBER

The SD DOH is the issuing office for this document and all subsequent addenda relating to it, on behalf of the State of South Dakota, DOH. The reference number for the transaction is RFP# 23-0901001-022. This number must be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	05/12/2023
Deadline for Submission of Written Inquiries	05/19/2023
Responses to offeror Questions	05/26/2023

Proposal Submission	06/16/2023
Proposal Reviews	06/17/2023
BIT Technical Review	July 2023
Demonstrations and presentations (if required)	August 2023
Anticipated Award Decision/Contract Negotiation	09/1/2023

1.5 SUBMITTING YOUR PROPOSAL

All proposals must be completed and received in the SD DOH office 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 hard copy and an electronic copy of the proposal (to include Cost Proposal) shall be submitted.

All proposals must be signed, in ink, by an officer of the offeror, legally authorized to bind the offeror to the proposal and sealed in the form. Proposals that are not properly signed may be rejected. The sealed envelope must be marked with the appropriate RFP Number and Title.

Proposals must be addressed and labeled as follows:

REQUEST FOR PROPOSAL # 23-0901001-022
PROPOSAL TITLE Contract Lifecycle Management System
PROPOSAL DUE June 16th, 2023, 5:00pm CST
Amanda Shoop
South Dakota Department of Health
600 E Capitol Ave
Pierre, SD 57501

Electronic submission shall be sent to Amanda Shoop at amanda.shoop@state.sd.us with RFP# 23-0901001-022 in the Subject line.

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

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

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

1.7 NON-DISCRIMINATION STATEMENT

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

1.8 RESTRICTION OF BOYCOTT OF ISRAEL

For contractors, vendors, suppliers, or subcontractors with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars ($100,000) or more, by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, has not refused to transact business activities, has not terminated business activities, and has not taken other similar actions intended to limit its commercial relations, related to the subject matter of the bid or offer, with a person or entity on the basis of Israeli national origin, or residence or incorporation in Israel or its territories, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.9 RESTRICTION OF PROHIBITED ENTITY

For contractors, vendors, suppliers, or subcontractors who enter into a contract with the State of South Dakota by submitting a response to this solicitation or agreeing to contract with the State, the bidder or offeror certifies and agrees that the following information is correct:

The bidder or offeror, in preparing its response or offer or in considering proposals submitted from qualified, potential vendors, suppliers, and subcontractors, or in the solicitation, selection, or commercial treatment of any vendor, supplier, or subcontractor, is not a prohibited entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Executive Order 2023-02. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for the State to reject the bid or response submitted by the bidder or offeror on this project and terminate any contract awarded based on the bid or response. The successful bidder or offeror further agrees to provide immediate written notice to the contracting executive branch agency if during the term of the contract it no longer complies with this certification and agrees such noncompliance may be grounds for contract termination.

1.10 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.

1.11 OFFEROR INQUIRIES

Offerors may email inquiries concerning this RFP to obtain clarification of requirements. No inquiries will be accepted after the date and time indicated in the Schedule of Activities. Inquiries must be emailed to Amanda Shoop at amanda.shoop@state.sd.us with the Subject line “RFP# 23-0901001-022”.

The DOH will respond to offeror’s inquiries (if required) via e-mail. In addition, all inquiries and the State’s response will be posted on the state’s e-procurement system. 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 the RFP. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.12 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. 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.

1.13 LENGTH OF CONTRACT

The contract will begin on 10/01/2023.
The contract will end on 05/31/2024.
The State will have the opportunity to renew the contract annually. The extension(s) will not be automatic.

1.14 GOVERNING LAW

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

1.15 PRESENTATIONS/DEMONSTRATIONS

At its discretion, the State may require a presentation or demonstration by an offeror to clarify a proposal. However, the State may award a contract based on the initial proposals received without a presentation or demonstration by the offeror. If presentations or demonstrations are required, they will be scheduled after the submission of proposals. Presentations and demonstrations will be made at the offeror's expense.

1.16 DISCUSSIONS

At the State's discretion, the offeror may or may not be invited to have discussions with the State. The discussions can be before or after the RFP has been submitted. Discussions will be made at the offeror's expense.

1.17 NEGOTIATIONS

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 component 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 STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP will include the State's standard terms and conditions as listed below, along with any additional terms and conditions as negotiated by the parties:

2.1 The Contractor will perform those services described in the Scope of Work, attached hereto as Section 3 of the RFP and by this reference incorporated herein.

2.2 The Contractor's services under this Agreement shall start on _______, and end on __ ___, unless terminated sooner pursuant to the terms hereof.

2.3 The Contractor will not use State equipment, supplies or facilities. The Contractor will provide the State with its Employer Identification Number, Federal Tax Identification Number or Social Security Number upon execution of this Agreement.

2.4 The State will make payment for services upon satisfactory completion of the services. The TOTAL CONTRACT AMOUNT is an amount not to exceed $______. The State will not pay Contractor's expenses as a separate item. Payment will be made pursuant to itemized invoices submitted with a signed state voucher. Payment will be made consistent with SDCL chapter 5-26.

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

2.6 The Contractor, at all times during the term of this Agreement, shall obtain and maintain in force insurance coverage of the types and with the limits as follows:

A. Commercial General Liability Insurance:
The Contractor shall maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than $1 million 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. Professional Liability Insurance or Miscellaneous Professional Liability Insurance:
The Contractor agrees to procure and maintain professional liability insurance or miscellaneous professional liability insurance with a limit not less than $1 million.

C. Business Automobile Liability Insurance:
The Contractor shall maintain business automobile liability insurance or equivalent form with a limit of not less than $1 million for each accident. Such insurance shall include coverage for owned, hired and non-owned vehicles.

D. Workers' Compensation Insurance:
The Contractor shall procure and maintain workers' compensation and employers' liability insurance as required by South Dakota law.

Before beginning work under this Agreement, Contractor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement. In the event a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, the Contractor agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Contractor shall furnish copies of insurance policies if requested by the State.

2.7 While performing services hereunder, the Contractor is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

2.8 Contractor agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury to the person or property of third parties, or which may otherwise subject Contractor or the State to liability. Contractor shall report any such event to the State immediately upon discovery.

2.9 Contractor'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. Contractor'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 Contractor to report any event to law enforcement or other entities under the requirements of any applicable law.

2.10 This Agreement may be terminated by either party hereto upon thirty (30) days written notice. In the event the Contractor breaches any of the terms or conditions hereof, this

Agreement may be terminated by the State at any time with or without notice. If termination for such a default is affected by the State, any payments due to Contractor at the time of termination may be adjusted to cover any additional costs to the State because of Contractor's default. Upon termination the State may take over the work and may award another party an agreement to complete the work under this Agreement. If after the State terminates for a default by Contractor it is determined that Contractor was not at fault, then the Contractor shall be paid for eligible services rendered and expenses incurred up to the date of termination.

2.11 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 law or federal funds reductions, 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.

2.12 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.

2.13 This Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota. Any lawsuit pertaining to or affecting this Agreement shall be venued in Circuit Court, Sixth Judicial Circuit, Hughes County, South Dakota.

2.14 The Contractor will comply with all federal, state and local laws, regulations, ordinances, guidelines, permits and requirements applicable to providing services pursuant to this Agreement, and will be solely responsible for obtaining current information on such requirements.

2.15 The Contractor may not use subcontractors to perform the services described herein without the express prior written consent of the State. The Contractor 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 Contractor 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.

2.16 Contractor hereby acknowledges and agrees that all reports, plans, specifications, technical data, miscellaneous drawings, software system programs and documentation, procedures, or files, operating instructions and procedures, source code(s) and documentation, including those necessary to upgrade and maintain the software program, and all information contained therein provided to the State by the Contractor in connection with its performance of services under this Agreement shall belong to and is the property of the State and will not be used in any way by the Contractor without the written consent of the State. Papers, reports, forms, software programs, source code(s) and other material which are a part of the work under this Agreement will not be copyrighted without written approval of the State.

2.17 The Contractor certifies that neither Contractor nor its principals are presently debarred, suspended, proposed for debarment or suspension, or declared ineligible from participating in transactions by the federal government or any state or local government department or agency. Contractor further agrees that it will immediately notify the State if during the term of this Agreement Contractor 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.

2.18 Pursuant to South Dakota Executive Order 2023-02, by entering into this Agreement with the State of South Dakota, the Contractor certifies and warrants that the Contractor is not a prohibited entity, regardless of its principal place of business, that is ultimately owned or controlled, directly or indirectly, by a foreign national, a foreign parent entity, or foreign government from China, Iran, North Korea, Russia, Cuba, or Venezuela, as defined by South Dakota Executive Order 2023-02.

The Contractor agrees that if this certification is false, the State may terminate this Agreement with no further liability to the State. The Contractor further agrees to provide immediate written notice to the State if during the term of the contract it no longer complies with this certification, and the Contractor agrees such noncompliance may be grounds for contract termination.

2.19 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________on behalf of the State, and by and to ___________, on behalf of the Contractor, 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.

2.20 In the event that any court of competent jurisdiction shall hold any provision of this Agreement unenforceable or invalid, such holding shall not invalidate or render unenforceable any other provision hereof.

2.21 All other 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.

3 SCOPE OF WORK

Within the Contract Lifecycle Management System, the SD DOH requires the ability to:

1. Create and manage user roles (to include different security settings). The users of this system are primarily SD DOH employees, but there will be times data will be shared outside the agency. Within the agency, the SD DOH needs the ability to constrain access to the system and create roles for drafters, reviewers, and approvers. The “create and manage user roles” needs to have some flexibility as there is the potential of growth in the size and scope of the agency;

2. House a configurable data visualization dashboard that allows agency staff, and others with permission, to see the progress of a contract through its lifecycle from assignment to staff for request, drafting through different versions, final version, approval, and execution. The ability to drill down into the dashboard to see level detail for each portion.
3. Obtain a centralized contract repository including embedded documents that aligns with DOH organizational structure;
4. Perform contract lifecycle workflows;
5. Include template and clause library to construct consistent and controlled agreements. SD DOH has contract templates that are reviewed and updated annually. Template editing permissions are restricted to certain users. Drafting users will have the capability to select which template is applicable to the contract being drafted.
6. Produce reports based on data from dashboard. SD DOH will require the following types of reports on demand, for example, but not limited to: Total contracts over a period; Contracts by types (professional service, software, hardware, systems, personal service, federal grant contracts, supply, bids); Contracts assigned by division, contract Point of Contact (POC); Contract expenditure reports;
7. Electronically Sign via integration within signature platform;
8. Send e-mail reminders, alerts, or notifications at each contract milestone as defined by DOH;
9. Receive customer service for the system (technical assistance, ongoing training, system updates based on law, technology, and SD DOH changes). SD DOH will require ongoing training based on changes made in the system. In addition, SD DOH will require technical assistance throughout the life of the contract system for users and the administrator(s) of the system. Updates shall be made yearly based upon changes in law and internal structure contract policy changes. SD DOH requests customer service, training and updates be separately identified as a cost in the bid; and
10. Add additional modules, including but not limited to multi-agency use.

3.1 Hosting and Data Access Requirements

The contract doubles as an agreement for the State to own the data tables and is able to manipulate data, run reports as needed, pull code tables, access raw data, and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau and associated platforms. The State prefers the Contract Lifecycle Management System be hosted in the State's Azure tenant. However, as a reminder, the offeror may host the system.

3.2 Single Sign-On Requirements

As part of the State's Identity and Access Management (IAM) strategy, the proposed solution will need to integrate with the State of South Dakota's standard identity management service single sign-on (SSO) which enables custom control of how citizens and state employees sign up, sign in, and manage their profiles.

The SSO supports two industry standard protocols: OpenID Connect and OAuth 2.0 (preferred). This identity management will handle password recovery. Multi-factor Authentication (MFA) is required for all application Administrators and may be required for other users. Microsoft's official documentation on the identity provider the State has implemented can be found at https://docs.microsoft.com/en-us/azure/active-directory-b2c/ and https://docs.microsoft.com/en-us/azure/active-directory-b2c/integrate-with-app-code-samples.

If the offeror is not able to fulfill this identity management standard, they will be excluded from the list.

3.3 Interfaces and Integration

The offeror must describe how the system can adapt to business necessary interfaces using widely adopted open APIs and standards. Additionally, the DOH expects that the offeror will make available/expose software services and publish documentation for those software services that would enable third party developers to interface other business applications. A detailed description of system capability shall be included in the proposal.

4 PROJECT DELIVERABLES/APPROACH/METHODOLOGY

If the State will be hosting the solution the offeror will provide a system diagram. The diagram must be detailed enough that the State can understand the components, the system flow, and system requirements. It is preferred that the diagram be provided as a separate document or attachment. The file must be named “(Your Name) System Diagram and Requirements”. If the offeror elects to make the diagram part of the proposal, then the location of the diagram must be clearly indicated in the Table of Contents.

If the offeror is hosting the solution, provide a diagram giving an overview of the proposed system. It is preferred that this diagram be provided as a separate document or attachment. The file must be named “(Your Name) Hosted System Diagram”. If the offeror elects to make the diagram part of the proposal, then the location of the diagram must be clearly indicated in the Table of Contents.

The offeror should state whether its proposed solution will operate in a virtualized environment. Offeror also should identify and describe all differences, restrictions or limitations of its proposed solution with respect to operation, licensing, support, certification, warranties, and any other details that may impact its proposed solution when hosted in a virtualized environment. This information must be included with the solution diagram for the offeror hosted solution.

This section identifies tasks and deliverables of the project as described in Section 3 above. The selected offeror is responsible for providing the required deliverables. These deliverables will be the basis against which the offeror’s performance will be evaluated.

The offeror is required to include a test system for its application. This test system will be used at the discretion of BIT. All resource costs associated with keeping the test system available must be borne by the project owner or the offeror. Any licensing costs for the test system must be included with the costs.

At BIT’s discretion, any code changes made by the offeror, either during this project or thereafter, will be placed in the above test system first. It is at BIT’s discretion if the code changes are applied by BIT or the offeror. If the code testing delays a project’s timeline, a change management process should be followed, and the State will not be charged for this project change. If the test and production systems are to be hosted by the State, the schedule for the testing of the code changes is to be decided by BIT. Testing of emergency code changes will be scheduled by BIT based on the severity and resource availability.

The test system will be maintained by the offeror as a mirror image of the production system code base. At BIT's discretion, updates to the production system will be made by copying code from the test system after the test system passes BIT certification requirements.

If BIT determines that the application must be shut down on the production system, for any reason, the offeror will, unless approved otherwise by BIT, diagnosis the problem on and make all fixes on the test system. The offeror is expected to provide proof, to BIT, of the actions taken to remediate the problem that led to the application being denied access to the production system before the application can go back into production. This proof can be required by BIT even if the fix passes all BIT certification criteria. BIT is willing to sign a non-disclosure agreement with the offeror if the offeror feels that revealing the fix will put the offeror's intellectual property at risk.

All solutions acquired by the State that are hosted by the offeror, including Software as a Service, or hosted by a third-party for the offeror will be subjected to security scans by BIT or preapproved detailed security scan report provided by the offeror. The scan report sent in with the proposal can be redacted by the offeror. The State's goal at this point is to see if the contents of the report will be acceptable, not to review the contents themselves. If the offeror will be providing a security scan report, one must be sent with the proposal for approval. Approval is not guaranteed. If the scan report is not acceptable, the State must scan the offeror's solution. The actual scanning by the State or the submission of a security scan report will be done if the proposal is considered for further review. A detailed security report must consist of at least:

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

The cost of any scans done by the offeror or the offeror's costs associated with the State's scans must be part of the offeror's bid. If the offeror is sending a security scan report, it should price the product both as if the State was to do the security scan or if the offeror was to do the security scan.

All hardware, website(s), or software purchased by the State and hosted by the State will be subjected to security scans by BIT.

Security scanning will be performed during the software development phase and during pre-production review. These scans and tests can be time consuming and should be allowed for in project planning documents and schedules. Products that do not meet BIT's security and performance requirements will not be allowed to go into production and may be barred from UAT until all issues are addressed to the State's satisfaction. The State urges the use of industry scanning/testing tools and secure development methods be employed to avoid unexpected costs and project delays. Costs to produce and deliver secure and reliable applications are the responsibility of the software entity producing or delivering an application to the State. Unless expressly indicated in writing, the State assumes all price estimates and bids are for the delivery and support of applications and systems that will pass security and performance testing. If the State determines the hardware, website(s), software, and or cloud services have security vulnerabilities that must be corrected, the State will inform the offeror of the nature of the issue and the offeror will be required to respond in writing regarding mitigation plans for the security vulnerabilities. If the product(s) does not pass the initial security scan, additional security scans may be required to reach an acceptable level of security. The offeror must pass a final follow-up security scan for the website(s), software or cloud services for the product(s) to be acceptable products to the State. The State may suspend or cancel payments for hardware, website(s), software, or cloud services that do not pass a final security scan.

Any website or web application hosted by the offeror that generates email cannot use "@state.sd.us" as the originating domain name per state security policy.

As part of this project, the offeror will provide a monitoring tool the State can utilize to monitor the operation of the proposed solution as well as all systems and all subcomponents and connections. It is required that this tool be easy to use and provide a dashboard of the health of the proposed solution. The effectiveness of this monitoring tool will be a component of the acceptance testing for this project.

As part of the project plan, the offeror will include development of an implementation plan that includes a back out component. Approval of the implementation plan by BIT should be a project milestone. Should the implementation encounter problems that cannot be resolved and the implementation cannot proceed to a successful conclusion, the back out plan will be implemented. The Implementation and back out documentation will be included in the project documentation.

The successful offeror will use the approved BIT processes and procedures when planning its project, including BIT's change management process. Work with the respective agency's BIT Point of Contact on this form. The Change Management form is viewable only to BIT employees. The purpose of this form is to alert key stake holders (such as: Operations, Systems Support staff, Desktop Support staff, administrators, Help Desk personnel, client representatives, and others) of changes that will be occurring within state resources and systems to schedule the:

- Movement of individual source code from test to production for production systems
- Implementation of a new system
- A major enhancement to a current system or infrastructure changes that impact clients
- Upgrades to existing development platforms

If as part of the project the state will be acquiring software the proposal should clearly state if the software license is perpetual or a lease. If both are options, the proposal should clearly say so and state the costs of both items separately.

Include in your submission details on your:

- Data loss prevention methodology;
- Identity and access management;
- Security intelligence;
- Annual security training and awareness;
- Manual procedures and controls for security;

- Perimeter controls;
- Security certifications and audits.

If the offeror will have State data on its system(s) or on a third-party's system and the data cannot be sanitized at the end of the project, the offeror's proposal must indicate this and give the reason why the data cannot be sanitized as per the methods in NIST 800-88.

The offeror's solution cannot include any hardware or hardware components manufactured by Huawei Technologies Company or ZTE Corporation or any subsidiary or affiliate of such entities. This includes hardware going on the State's network as well as the offeror's network if the offeror's network is accessing the State's network or accessing State data. This includes Infrastructure as a Service, Platform as a Service or Software as a Service situations. Any company that is considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act, in a United States appropriation bill, an Executive Order, or listed on the US Department of Commerce's Entity List will be included in this ban.

If the offeror's solution requires accounts allowing access to State systems, then the offeror must indicate the number of the offeror's staff or subcontractors that will require access, the level of access needed, and if these accounts will be used for remote access. These individuals will be required to use Multi-Factor Authentication (MFA). The State's costs in providing these accounts will be a consideration when assessing the cost of the offeror's solution. If the offeror later requires accounts that exceed the number of accounts that was originally indicated, the costs of those accounts will be borne by the offeror and not passed onto the State. All State security policies can be found in the Information Technology Security Policy (ITSP) attached to this RFP. The offeror should review the State's security policies regarding authorization, authentication, and, if relevant, remote access (See ITSP 230.67, 230.76, and 610.1). Use of Remote Access Devices (RAD) by contractors to access the State's system must be requested when an account is requested. The offeror should be aware that access accounts given to non-state employees, Non-State (NS) accounts, will be disabled if not used within 90 days. A NS account will be deleted after Y days if it is not used.

Regression Testing- Regression testing is the process of testing changes to computer programs to make sure that the older programming still works with the new changes.

Integration Testing- Integration testing is a software development process which program units are combined and tested as groups in multiple ways. In this context, a unit is defined as the smallest testable part of an application. Integration testing can expose problems with the interfaces among program components before trouble occurs in real-world program execution. Integration testing is also known as integration and testing (I&T).

Functional Testing- Functional testing is primarily used to verify that a piece of software is meeting the output requirements of the end-user or business. Typically, functional testing involves evaluating and comparing each software function with the business requirements. Software is tested by providing it with some related input so that the output can be evaluated to see how it conforms, relates or varies compared to its base requirements. Moreover, functional testing also checks the software for usability, such as ensuring that the navigational functions are working as required. Some functional testing techniques include smoke testing, white box testing, black box testing, and unit testing.

Performance Testing- Performance testing is the process of determining the speed or throughput of an application. This process can involve quantitative tests such as measuring the response time or the number of MIPS (millions of instructions per second) at which a system functions. Qualitative attributes such as reliability, scalability and interoperability may also be evaluated. Performance testing is often done in conjunction with load testing.

Load Testing- Load testing is the process of determining the ability of an application to maintain a certain level of effectiveness under unfavorable conditions. The process can involve tests such as ramping up the number of users and transactions until the breaking point is reached or measuring the frequency of errors at your required load. The term also refers to qualitative evaluation of factors such as availability or resistance to denial-of-service (DoS) attacks. Load testing is often done in conjunction with the more general process of performance testing. Load testing is also known as stress testing.

User Acceptance Testing- User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications. UAT is one of the final and critical software project procedures that must occur before newly developed or customized software is rolled out. UAT is also known as beta testing, application testing or end user testing. In some cases, UAT may include piloting of the software.

The State, at its sole discretion, may consider a solution that does include all or any of these deliverables or consider deliverables not originally listed. An offeror **must** highlight any deliverable it does not meet and give any suggested “work-around” or future date that it **will** be able to provide the deliverable.

5 FORMAT OF SUBMISSION

All proposals should be prepared simply and economically and provide a direct, concise explanation of the offeror’s proposal and qualifications. Elaborate brochures, sales literature and other presentations unnecessary to a complete and effective proposal are not desired.

Offerors are required to provide an electronic copy of their response. The electronic copy should be provided in MS WORD or in PDF format, except for the project plan, which must be in MS Project. The submission must be delivered as indicated in Section 1.5 of this document.

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. The offeror should respond to each point in the Scope of Work and Deliverables in the order they were presented.

Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) must direct all questions or comments regarding the RFP or the evaluation to 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 exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should email the buyer of record at amanda.shoop@state.sd.us.

The offeror may be required to submit a copy of its most recent audited financial statements upon the State's request.

The proposal should be page numbered and should have an index or a table of contents referencing the appropriate page number. Each of the sections listed below should be tabbed.

Offerors are cautioned that use of the State Seal in any of their documents is illegal as per South Dakota Codified Law § 1-6-3.1. *Use of seal or facsimile without authorization prohibited--Violation as misdemeanor. No person may reproduce, duplicate, or otherwise use the official seal of the State of South Dakota, or its facsimile, adopted and described in §§ 1-6-1 and 1-6-2 for any for-profit, commercial purpose without specific authorization from the secretary of state. A violation of this section is a Class 1 misdemeanor.*

Proposals should be prepared using the following headings and, in the order that they are presented below. Please reference the section for details on what should be included in your proposal.

Statement of Understanding of Project (5.1)
Deliverables (5.5)
Non-standard Software and/or Hardware (5.6)
Project Plan (5.4)
System Diagram (If not a separate document)
Security and Vendor Questions (If not a separate document)
Response to the State's contract terms
Corporate Qualifications (5.2)
Project Experience (5.3)
Detailed implementation plan (4)
Cost Proposal (6)

5.1 STATEMENT OF UNDERSTANDING OF PROJECT

To demonstrate your comprehension of the project, the offeror should summarize their understanding of what the work is and what the work will entail. This should include, but not be limited to, the offeror's understanding of the purpose and scope of the project, critical success factors and potential problems related to the project, and the offeror's understanding of the deliverables. The offeror should include their specialized expertise, capabilities, and technical competence as demonstrated by the proposed approach and methodology to meet the project requirements. This section should be limited to no more than two pages.

5.2 CORPORATE QUALIFICATIONS

Please provide responses to the each of the following questions in your proposal.

A. What year was your parent company (if applicable) established?

B. What is the business of your parent company?

C. What is the total number of employees in the parent company?

D. What are the total revenues of your parent company?

E. How many employees of your parent company have the skill set to support this effort?

F. How many of those employees are accessible to your organization for active support?

G. What year was your firm established?

H. Has your firm ever done business under a different name and if so, what was the name?

I. How many employees does your firm have?

J. How many employees in your firm are involved in this type of project?

K. How many of those employees are involved in on-site project work?

L. What percent of your parent company's revenue (if applicable), is produced by your firm?

M. Corporate resources available to perform the work, including any specialized services, within the specified time limits for the project

N. Availability to the project locale

O. Familiarity with the project locale

P. Has your firm ever done business with other governmental agencies? If so, please provide references.

Q. Has your firm ever done business with the State of South Dakota? If so, please provide references.

R. Has your firm ever done projects that are like or similar to this project? If so, how many clients are using your solution? Please provide a list of four or more locations of the same approximant nature as the State where your application is in use along with contact names and numbers for those sites. The State of South Dakota has a consolidated IT system. **Either** any references given should be from states with a consolidated IT system, to be acceptable **or** the reference should be a detailed explanation on how you will modify your work plan for a consolidated environment that you are unfamiliar with.

S. Provide the reports of third-party security scans done at the end of the four projects you provided in your proposal response. If there are no audits of these projects then provide, unedited and un-redacted results of such security testing/scanning from third-party companies or tools that has been run within the past 90 days. The

State will sign a non-disclosure agreement, as needed, and redaction of these scan reports can be done within the limits of the State's open records law.

T. What is your Company's web site?

When providing references, the reference must include the following information:

- 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
- Dates of the service/contract
- A brief, written description of the specific prior services performed and requirements thereof

5.3 RELEVANT PROJECT EXPERIENCE

Provide details about four recent projects that the offeror was awarded and then managed through to completion. Project examples should include sufficient detail so the agency fully understands the goal of the project; the dates (from start to finish) of the project; the offeror's scope of work for the project; the responsibilities of the offeror and subcontractors in the project; the complexity of the offeror's involvement in the project; deliverables provided by the offeror; the methodologies employed by the offeror; level and type of project management responsibilities of the offeror; changes that were made and request for changes that differed from the onset of the project; how changes to the project goals, offeror's scope of work, and deliverables were addressed or completed; price and cost data; quality of the work and the total of what the offeror accomplished in the project.

A. Client/Company Name

B. Client Company Address, including City, State and Zip Code

C. Client/Company Contacts(s)
Name
Title
Telephone Number
E-mail address
Fax Number

D. Project Start Date

E. Project Completion Date

F. Project Description and Goals

G. Offeror's Role in Project

H. Offeror's responsibilities

I. Offeror's Accomplishments

J. Description of How Project Was Managed

K. Description of Price and Cost Data from Project

L. Description of special project constraints, if applicable

M. Description of your ability and proven history in handling special project constraints

N. Description of All Changes to the Original Plan or Contract That Were Requested

O. Description of All Changes to the Original Plan or Contract That Offeror Completed

P. Description of How Change Requests Were Addressed or Completed by Offeror

Q. Was Project Completed in a Timeframe That Was According to the Original Plan or Contact? (If "No", provide explanation)

R. Was Project Completed Within Original Proposed Budget? (If "No" provide explanation)

S. Was there any Litigation or Adverse Contract Action regarding Contract Performance? (If "Yes" provide explanation)

T. Feedback on Offeror's Work by Company/Client

U. Offeror's Statement of Permission for the Department to Contact the Client/Company and for the Client's/Company's Contract(s) to Release Information to the Department

5.4 PROJECT PLAN

Provide a project plan that indicates how you will complete the required deliverables and services and addresses the following:

- Proposed project management techniques
- Number of offeror's staff needed
- Tasks to be performed (within phase as applicable)
- Number of hours each task will require
- Deliverables created by each task
- Dates by which each task will be completed (dates should be indicated in terms of elapsed time from project inception)
- Resources assigned to each task
- Required state agency support
- Show task dependencies
- Training (if applicable)

Microsoft Project is the standard scheduling tool for the State of South Dakota. The schedule should be a separate document, provided in Microsoft Excel, and submitted as an attachment to your proposal.

If, as part of this project, the offeror plans to set up or configure the software or hardware and plans to do this outside of South Dakota, even in part, then the offeror needs to provide a complete and detailed project plan on how the offeror plans on migrating to the State's site. Failure to do this is sufficient grounds to disregard the submission, as it demonstrates that the offeror fundamentally does not understand the project. Providing a work plan for the steps above that is complete and detailed maybe sufficient.

5.5 DELIVERABLES

This section should constitute the major portion of the work to be performed. Provide a complete narrative detailing the assessment of the work to be performed, approach and methods to provide the requirements of this RFP, the offeror's ability to fulfill the requirements of this RFP, the offeror's approach, the resources necessary to fulfill the requirements, project management techniques, specialized services, availability to the project locale, familiarity with the project locale and a description of any options or alternatives proposed. This should demonstrate that the offeror understands the desired overall performance expectations. This response should identify each requirement being addressed as enumerated in Section 3. If you have an alternative methodology or deliverables you would like to propose, please include a detailed description of the alternative methodology or deliverables and how they will meet or exceed the essential requirements of the methodology and deliverables described in Section 3.

5.6 NON-STANDARD HARDWARE AND SOFTWARE

State standard hardware and software should be utilized unless there is a reason not to. If your proposal will use non-standard hardware or software, you must first obtain State approval. If your proposal recommends using non-standard hardware or software, the proposal should very clearly indicate what non-standard hardware or software is being proposed and why it is necessary to use non-standard hardware or software to complete the project requirements. The use of non-standard hardware or software requires use of the State's New Product Process. This process can be found through the Standards' page and must be performed by State employees. The costs of such non-standard hardware or software should be reflected in your cost proposal. The work plan should also account for the time needed to complete the New Product Process. See https://bit.sd.gov/bit?id=bit_standards_overview, for lists of the State's standards. The proposal should also include a link to your hardware and software specifications.

If non-standard hardware or software is used, the project plan and the costs stated in Section 6 must include service desk and field support, since BIT can only guarantee best effort support for standard hardware and software. If any software development may be required in the future, hourly development rates must be stated. The project plan must include the development and implementation of a disaster recovery plan since non-standard hardware and software will not be covered by the State's disaster recovery plan. This must also be reflected in the costs.

The offeror must complete the list of technical questions, Security and Vendor Questions which is attached as Appendix B. These questions and the offeror's responses may be used in the proposal evaluation.

5.7 Background Checks

The offeror must include the following statement in its proposal:

(Company name here) acknowledges and affirms that it understands that the (company name here) employees who have access to production Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), any information defined under state statute as confidential or have access to secure facilities will have fingerprint-based background checks. These background checks will be used to check the criminal history records of the State as well as the Federal Bureau of Investigation's records. (Company name here) acknowledges and affirms that this requirement will extend to include any Subcontractor's, Agents, Assigns and or Affiliated Entities employees.

6 COST PROPOSAL

Cost proposals must be submitted for evaluation. Offerors may submit multiple cost proposals. All costs related to the provision of the required services must be included in each cost proposal offered.

The offeror must submit a statement in the Proposal that attests the offeror’s willingness and ability to perform the work described in this RFP for the price being offered.

6.1 STAFFING

Name	Role	Total Hours on Project	Total Hours on Site	Hourly Rate	Total
				Total:	

6.2 TRAVEL AND EXPENDITURE TABLE

Name	Method of Travel	Cost per trip	Number of Trips	Total Cost
			Total:	

Name	Lodging Cost per night	Numbe r of Nights	Lodging Cost	Per diem	Numbe r of Days	Per diem Cost	Total Cost
Totals:							

6.3 OTHER COSTS

Show any other costs such as: software, hardware, ongoing costs, etc. Customer service, training and updates must be separately identified as a cost in the bid.

	One Time	Year 1	Year 2	Year 3	Totals
Hardware					
Software					
Maintenance					
License Fees					
Training					
Other…					
Totals					

6.4 ADDITIONAL WORK

The offeror may be expected to perform additional work as required by any of the State signatories to a contract. This work can be made a requirement by the State for allowing the application to go into production. This additional work will not be considered a project change chargeable to the State if it is for reasons of correcting security deficiencies, meeting the functional requirements established for the application, unsupported third-party technologies, or excessive resource consumption. The cost for additional work should be included in your proposal.

7 PROPOSAL EVALUATION AND AWARD PROCESS

7.1 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:

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

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

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

7.1.4 Availability to the project locale;

7.1.5 Familiarity with the project locale;

7.1.6 Proposed project management techniques; and

7.1.7 Ability and proven history in handling special project constraints

7.1.8 Ability to stay within DOH budget

- $90,000 implementation and training
- $25,000 on-going costs

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.5.1 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 offeror. The agency may then negotiate with the next highest ranked offeror.

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

8 BEST AND FINAL OFFERS

The State reserves the right to request best and final offers. If so, the State will initiate the request for best and final offers; best and final offers may not be initiated by an offeror. Best and final offers may not be necessary if the State is satisfied with the proposals received.

If best and final offers are sought, the State will document which offerors will be notified and provide them opportunity to submit best and final offers. Requests for best and final offers will be sent stating any specific areas to be covered and the date and time in which the best and final offer must be returned. Conditions, terms, or price of the proposal may be altered or otherwise changed, provided the changes are within the scope of the request for proposals and instructions contained in the request for best and final offer. If an offeror does not submit a best and final offer or a notice of withdrawal, the offeror's previous proposal will be considered that offeror's best and final proposal. After best and final offers are received, final evaluations will be conducted.

9 SCANNING

The offeror acknowledges that the State will conduct a security and vulnerability scan as part of the review of the offeror’s RFP. This scan will not include a penetration test. The State will use commercially available, industry standard tools to scan a non-production environment with non-production data at mutually agreeable times.

The offeror should fill in the information below and sign the form. The offeror’s employee signing this form must have the authority to allow the State to do a security scan. If no security contact is given the State will assume that the State can scan at any time. **At the state’s option, any RFP response that does not include a completed and signed form may be dropped from consideration. If there is State data protected by federal or state law or regulation or industry standard involved, the State is more likely to consider a security scan necessary for an RFP to be considered.** Except for State staff, the State will only provide scan information to the offeror’s security contact. At the State’s option, the State will conduct the scan at a location named by the offeror. The offeror can only request, not require, naming the scanning location. The State may consider a comprehensive, complete and recent risk assessment as satisfying the scanning requirement. If required, the State will sign a non-disclosure agreement before scanning or receiving the risk assessment.

Offeror’s name: ________________________

Offeror’s security contact’s name: ________________________

Security contact’s phone number: ________________________

Security contact’s email address: ________________________

Web address URL or Product Name _____________________. The State will contact the security contact to arrange for a test log for scanning.

Offeror’s employee acknowledging the right to scan:

Name (Print): ______________________

Title: ________________________________

Date: _______________________________

Signature: ___________________________

Appendix A – Included I/T Contract Terms and Conditions

Adapt the BIT standard contract language

Appendix B – Security and Vendor Questions

Exhibit A
Bureau of Information and Telecommunications
Required IT Contract Terms

Any contract resulting from this RFP will include the State's required IT terms and conditions as listed below, along with any additional terms and conditions as negotiated by the parties. Due to the changing landscape of IT security and data privacy, the State reserves the right to add additional IT terms and conditions or modify the IT terms and conditions listed below to the resulting contract:

Pursuant to South Dakota Codified Law § 1-33-44, the Bureau of Information and Telecommunications ("BIT") oversees the acquisition of office systems technology, software, and services; telecommunication equipment, software, and services; and data processing equipment, software, and services for departments, agencies, commissions, institutions, and other units of state government. As part of its duties as the Executive Branch's centralized IT agency, BIT requires the contract terms and conditions of this Exhibit XX. For purposes of this Exhibit, [Vendor Name] will be referred to as the "Vendor."

It is understood and agreed to by all parties that BIT has reviewed and approved only this Exhibit. Due to the ever-changing security and regulatory landscape in IT and data privacy, before renewal of this Agreement BIT must review and approve the clauses found in this Exhibit as being the then current version of the clauses and if any additional required clauses are needed. Changes to clauses in this Exhibit must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible.

The Parties agree, when used in this Exhibit, the term "Vendor" will mean the Vendor and the Vendor's employees, subcontractors, agents, assigns, and affiliated entities.

Section I. Confidentiality of Information

For purposes of this paragraph, "State Proprietary Information" will include all information disclosed to the Vendor by the State. The Vendor will 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. The Vendor must 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 third party consultants except those who have a need to access such information and who have agreed to obligations of confidentiality at least as strict as those set out in this Agreement. The Vendor 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. The Vendor must protect the 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. The Vendor agrees to return all information received from the State to the State's custody upon the end of the term of this Agreement, unless otherwise agreed in a writing signed by both parties. State Proprietary Information will not include information that:

A. was in the public domain at the time it was disclosed to the Vendor,
B. was known to the Vendor without restriction at the time of disclosure from the State,
C. that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information,
D. was independently developed by the Vendor without the benefit or influence of the State's information, and
E. becomes known to the Vendor without restriction from a source not connected to the State of South Dakota.

State's Proprietary Information can include names, social security numbers, employer numbers, addresses and other data about applicants, employers or other clients to whom the State provides services of any kind. The Vendor understands that this information is confidential and protected under State law. The Parties mutually agree that neither of them nor any subcontractors, agents, assigns, or affiliated entities will disclose the contents of this 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. The Vendor acknowledges that the State and its agencies are public entities and thus may be 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 South Dakota open records or open meetings laws.

Section II. Cyber Liability Insurance

The Vendor will maintain cyber liability insurance with liability limits in the amount of $________ to protect any and all State data the Vendor receives as part of the project covered by this agreement including State data that may reside on devices, including laptops and smart phones, utilized by Vendor employees, whether the device is owned by the employee or the Vendor. If the Vendor has a contract with a third-party to host any State data the Vendor receives as part of the project under this Agreement, then the Vendor will include a requirement for cyber liability insurance as part of the contract between the Vendor and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include State Data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-party Vendor. The cyber liability insurance will cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this Agreement, the Vendor will furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and which provide that such insurance may not be canceled, except on 30 days prior written notice to the State. The Vendor will furnish copies of insurance policies if requested by the State. The insurance will stay in effect for three years after the work covered by this Agreement is completed.

Section III. Rejection or Ejection of Vendor

The State, at its option, may require the vetting of any of the Vendor, and the Vendor's subcontractors, agents, Assigns, or affiliated entities. The Vendor is required to assist in this process as needed.

The State reserves the right to reject any person from participating in the project or require the Vendor to remove from the project any person the State believes is detrimental to the project or is considered by the State to be a security risk. The State will provide the Vendor with notice of its determination, and the reasons for the rejection or removal if requested by the Vendor. If the State signifies that a potential security violation exists with respect to the request, the Vendor must immediately remove the individual from the project.

Section IV. Domain Name Ownership

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

Section V. Software Functionality and Replacement

The software licensed by the Vendor to the State under this Agreement will provide the functionality as described in the software documentation, which the Vendor agrees to provide to the State prior to or upon the execution of this Agreement.

The Vendor agrees that:

A. If, in the opinion of the State, the Vendor reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or renamed product, the State will be entitled to license such software product at no additional license or maintenance fee.

B. If, in the opinion of the State, the Vendor releases an option, future product, purchasable product or other release that has substantially the same functionality as the software product licensed to the State, and it ceases to provide maintenance for the older software product, the State will have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the Vendor discontinues the licensed product and recommends movement to a new product as a replacement option regardless of any additional functionality the replacement product may have over the licensed product.

Section VI. Federal Intellectual Property Bankruptcy Protection Act

The Parties agree that the State will be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto. The State also maintains its termination privileges if the Vendor enters bankruptcy.

Section VII. Non-Disclosure and Separation of Duties

The Vendor will enforce separation of job duties and require non-disclosure agreements of all staff that have or can have access to State Data or the hardware that State Data resides on. The Vendor will limit staff knowledge to those staff who duties that require them to have access to the State Data or the hardware the State Data resides on.

Section VIII. Cessation of Business

The Vendor will notify the State of impending cessation of its business or that of a tiered provider and the Vendor's contingency plan. This plan should include the immediate transfer of any previously escrowed assets and data and State access to the Vendor's facilities to remove or destroy any state-owned assets and data. The Vendor will implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Vendor 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 Vendor 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 Vendor 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.

Section IX. Legal Requests for Data

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

A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Vendor seeking State Data maintained by the Vendor,
B. Consult with the State regarding the Vendor's 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.

Section X. eDiscovery

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

Section XI. Audit Requirements

The Vendor warrants and agrees it is aware of and complies with all audit requirements relating to the classification of State Data the Vendor stores, processes, and accesses. Depending on the data classification, this may require the Vendor to grant physical access to the data hosting facilities to the State or a federal agency. The Vendor will notify the State of any request for physical access to a facility that hosts or processes State Data by any entity other than the State.

Section XII. Annual Risk Assessment

The Vendor will conduct an annual risk assessment or when there has been a significant system change. The Vendor will provide verification to the State's contact upon request that the risk assessment as taken place. At a minimum, the risk assessment will include a review of the:

A. Penetration testing of the Vendor's system;
B. Security policies and procedures;
C. Disaster recovery plan;

D. Business Associate Agreements; and
E. Inventory of physical systems, devices, and media that store or utilize ePHI for completeness.

If the risk assessment provides evidence of deficiencies, a risk management plan will be produced. Upon request by the State, the Vendor will send a summary of the risk management plan to the State's contact. The summary will include completion dates for the risk management plan's milestones. Upon request by the State, the Vendor will send updates on the risk management plan to the State's contact. Compliance with this Section may be met if the Vendor provides proof to the State that the Vendor is FedRAMP Certified and has maintained FedRAMP Certification.

Section XIII. Independent Audit

The Vendor will disclose any independent audits that are performed on any of the Vendor's systems tied to storing, accessing, and processing State Data. This information on an independent audit(s) must be provided to the State in any event, whether the audit or certification process is successfully completed or not. The Vendor will provide a copy of the findings of the audit(s) to the State. Compliance with this Section may be met if the Vendor provides a copy of the Vendor's SOC 2 Type II report to the State upon request.

Section XIV. Service Level Agreements

The Vendor warrants and agrees that the Vendor has provided to the State all Service Level Agreements (SLA) related to the deliverables of the Agreement. The Vendor further warrants that it will provide the deliverables to the State in compliance with the SLAs.

Section XV. Access Attempts

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

Section XVI. Access to State Data

Unless this Agreement is terminated, the State's access to State Data amassed pursuant to this Agreement will not be hindered if there is a:

A. Contract dispute between the parties to this Agreement,
B. There is a billing dispute between the parties to this Agreement, or
C. The Vendor merges with or is acquired by another company.

Section XVII. Password Protection

All aspects of the Vendor's products provided to the State pursuant to this Agreement will be password protected. If the Vendor provides the user with a preset or default password, that password cannot include any Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), or any information defined under federal or state law, rules, or regulations as confidential information or fragment thereof. On an annual basis, the Vendor will document its password policies for all Vendor employees to ensure adequate password protections are in place. The process used to reset a password must include security questions or Multifactor Authentication. Upon request, the Vendor will provide to the State the Vendor's password policies, logs, or administrative settings to demonstrate the password policies are actively enforced.

Section XVIII. Provision of Data

State Data is any data produced or provided by the State as well as any data produced or provided for the State by the Vendor or a third-party.

Upon notice of termination by either party or upon reaching the end of the term of this Agreement, the Vendor will provide the State all current State Data in a non-proprietary format. In addition, the Vendor agrees to extract any information (such as metadata, which includes data structure descriptions, data dictionary, and data) stored in repositories not hosted on the State's IT infrastructure in a format chosen by the State. If the State's chosen format is not possible, the Vendor will extract the information into a text file format and provide it to the State.

Upon the effective date of the termination of this Agreement, the Vendor will again provide the State with all current State Data in a non-proprietary format. In addition, the Vendor will again extract any information (such as metadata) stored in repositories not hosted on the State's IT infrastructure in a format chosen by the State. As before, if the State's chosen format is not possible, the Vendor will extract the information into a text file format and provide it to the State.

Section XIX. Threat Notification

A credible security threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach any aspect of a system that is holding State Data or a product provided by the Vendor. Upon becoming aware of a credible security threat with the Vendor's product(s) and or service(s) being used by the State, the Vendor or any subcontractor supplying product(s) or service(s) to the Vendor needed to fulfill the terms of this Agreement will notify the State within two business days of any such threat. If the State requests, the Vendor will provide the State with information on the threat.

Section XX. Adverse Event

The Vendor must notify the State contact within three days if the Vendor becomes aware that an Adverse Event has occurred. An Adverse Event is the unauthorized use of system privileges, unauthorized access to State Data, execution of malware, physical intrusions and electronic intrusions that may include network, applications, servers, workstations, and social engineering of staff. If the Adverse Event was the result of the Vendor's actions or inactions, the State can require a risk assessment of the Vendor the State mandating the methodology to be used as well as the scope. At the State's discretion a risk assessment may be performed by a third party at the Vendor's expense. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

Section XXI. Browser

The system, site, or application must be compatible with Vendor supported versions of Edge, Chrome, Safari, and Firefox browsers. Silverlight, QuickTime, PHP, Adobe ColdFusion, and Adobe Flash will not be used in the system, site, or application. Adobe Animate CC is allowed if files that require third-party plugins are not required.

Section XXII. Security Acknowledgment Form

The Vendor will be required to sign the Security Acknowledgement Form which is attached to this Agreement as Exhibit ______. 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 Vendor by the State contact before work on the contract may begin. This Security Acknowledgment Form constitutes the agreement of the Vendor to be responsible and liable for ensuring that the Vendor, the Vendor's employee(s), and subcontractor's, agents, assigns and affiliated entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy (ITSP). 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 Vendor does not sign another Security Acknowledgement Form covering any employee(s) and any subcontractor's, agent's, assign's, 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 Vendor's, Vendor's employee(s), or subcontractor's, agent's, assign's, 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 Vendor or subcontractors, agents, assigns, or affiliated entities and in accordance with the Vendor's or subcontractor's, agent's, assign's, and affiliated entities' personnel policies. Regardless of the actions taken by the Vendor and subcontractors, agents, assigns, and affiliated entities, the State will retain the right to require at the State's discretion the removal of the employee(s) from the project covered by this Agreement.

Section XXIII. Information Technology Standards

Any service, software, or hardware provided under this Agreement will comply with State standards which can be found at https://bit.sd.gov/bit?id=bit_standards_overview.

Section XXIV. Product Usage

The State cannot be held liable for any additional costs or fines for mutually understood product usage over and above what has been agreed to in this Agreement unless there has been an audit conducted on the product usage. This audit must be conducted using a methodology agreed to by the State. The results of the audit must also be agreed to by the State before the State can be held to the results. Under no circumstances will the State be required to pay for the costs of said audit.

Section XXV. Security

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

By signing this Agreement, the Vendor warrants that:

A. All Critical, High, Medium, and Low security issues are resolved. Critical, High, Medium, and Low can be described as follows:

1. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
2. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.
3. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
4. **Low** - Vulnerabilities identified by the State as needing to be resolved that are not Critical, High, or Medium issues.

B. Assistance will be provided to the State by the Vendor in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Vendor will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.

Section XXVI. Security Scanning

The State routinely applies security patches and security updates as needed to maintain compliance with industry best practices as well as state and federal audit requirements. Vendors who do business with the State must also subscribe to industry security practices and requirements. Vendor s must include costs and time needs in their proposals and project plans to assure they can maintain currency with all security needs throughout the lifecycle of a project. The State will collaborate in good faith with the Vendor to help them understand and support State security requirements during all phases of a project’s lifecycle but will not assume the costs to mitigate applications or processes that fail to meet then-current security requirements.

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

Section XXVII. Malicious Code

A. The Vendor warrants that the Agreement deliverables contain no code that does not support an application requirement.
B. The Vendor warrants that the Agreement deliverables contains no malicious code.
C. The Vendor warrants that the Vendor will not insert into the Agreement deliverables or any media on which the Agreement deliverables is delivered any malicious or intentionally destructive code.
D. In the event any malicious code is discovered in the Agreement deliverables, the Vendor must provide the State at no charge with a copy of or access to the applicable Agreement deliverables that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this Section are in addition to other additional remedies available to the State.

Section XXVIII. Denial of Access or Removal of Application or Hardware from Production

During the life of this Agreement the application and hardware can be denied access to or removed from production at the State's discretion. The reasons for the denial of access or removal of the application or hardware from the production system may include but not be limited to security, functionality, unsupported third-party technologies, or excessive resource consumption. Denial of access or removal of an application or hardware also may be done if scanning shows that any updating or patching of the software and or hardware produces what the State determines are unacceptable results.

The Vendor will be liable for additional work required to rectify issues concerning security, functionality, unsupported third-party technologies, and excessive consumption of resources if it is for reasons of correcting security deficiencies or meeting the functional requirements originally agreed to for the application or hardware. At the discretion of the State, contractual payments may be suspended while the application or hardware is denied access to or removed from production. The reasons can be because of the Vendor's actions or inactions. Access to the production system to perform any remedying of the reasons for denial of access or removal of the software and hardware, and its updating and or patching will be made only with the State's prior approval.

It is expected that the Vendor will provide the State with proof of the safety and effectiveness of the remedy, update, or patch proposed before the State provides access to the production system. The State will sign a non-disclosure agreement with the Vendor if revealing the update or patch will put the Vendor's intellectual property at risk. If the remedy, update, or patch the Vendor proposes is unable to present software or hardware that meets the State's requirements, as defined by the State, which may include but is not limited to security, functionality, or unsupported third party technologies, to the State's satisfaction within 30 days of the denial of access to or removal from the production system and the Vendor does not employ the change management process to alter the project schedule or deliverables within the same 30 days then at the State's discretion the Agreement may be terminated.

Section XXIX. Movement of Product

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

Section XXX. Use of Product on Virtualized Infrastructure and Changes to that Infrastructure

The State operates a virtualized computing environment and uses software-based management and resource capping. The State retains the right to use and upgrade as deemed appropriate its hypervisor and operating system technology and related hardware without additional license fees or other charges provided the State assures the guest operating system(s) running within that hypervisor environment continue to present computing resources to the licensed product in a consistent manner. The computing resource allocations within the State's hypervisor software-based management controls for the guest operating system(s) executing the product will be the only consideration in licensing compliance related to computing resource capacity.

Section XXXI. Load Balancing

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

Section XXXII. Backup Copies

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

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

Section XXXIII. Use of Abstraction Technologies

The Vendor's application must use abstraction technologies in all applications, that is the removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services.

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

Section XXXIV. Scope of Use

A. There will be no limit on the number of locations, or size of processors on which the State can operate the software.
B. There will be no limit on the type or version of operating systems upon which the software may be used.

Section XXXV. License Agreements

The Vendor warrants that it has provided to the State and incorporated into this Agreement all license agreements, End User License Agreements (EULAs), and terms of use regarding its software or any software incorporated into its software before execution of this Agreement. Failure to provide all such license agreements, EULAs, and terms of use will be a breach of this Agreement at the option of the State. The parties agree that neither the State nor its end users will be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph will control and supersede the language of any such agreements to the contrary.

Section XXXVI. Web and Mobile Applications

A. The Vendor's application is required to:

1. 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,
2. encrypt data in transport and at rest using a mutually agreed upon encryption format,
3. close all connections and close the application at the end of processing,
4. have documentation that is in grammatically complete text for each call and defined variables (i.e., using no abbreviations and using complete sentences) sufficient for a native speaker of English with average programming skills to determine the meaning or intent of what is written without prior knowledge of the application,
5. have no code not required for the functioning of application,
6. 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,
7. 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,
8. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation,
9. 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),
10. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Vendor's application,
11. access no data outside what is defined in the "About" information for the Vendor's application,
12. conform to Web Content Accessibility Guidelines 2.0,
13. have Single Sign On capabilities with the State's identity provider,

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

Section XXXVII. Intended Data Access Methods

The Vendor's application will not allow a user, external to the State's domain, to bypass logical access controls required to meet the application's functional requirements. All database queries using the Vendor's application can only access data by methods consistent with the intended business functions.

If the State can demonstrate the application flaw, to the State's satisfaction, then the Vendor will rectify the issue, to the State's satisfaction, at no cost to the State.

Section XXXVIII. Application Programming Interface

Vendor documentation on application programming interface must include a listing of all data types, functional specifications, a detailed explanation on how to use the Vendor's application programming interface and tutorials. The tutorials must include working sample code.

Section XXXIX. Access to Source and Object Code

The Vendor will provide access to source and object code for all outward facing areas of the system where information is presented, shared, or received whether via browser-based access and programmatic-based access including but not limited to application program interfaces (APIs) or any other access or entry point accessible via the world wide web, modem, or other digital process that is connected to a digital network, radio-based or phone system.

Section XL. Data Location and Offshore Services

The Vendor must provide its services to the State as well as storage of State Data solely from data centers located in the continental United States. The Vendor 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 without prior written permission from the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

Section XLI. Vendor Training Requirements

The Vendor, Vendor's employee(s), and Vendor's subcontractors, agents, assigns, affiliated entities and their employee(s), must successfully complete, at the time of hire a cyber-security training program. The training must include but is not limited to:

A. legal requirements for handling data,
B. media sanitation,
C. strong password protection,
D. 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
E. security incident response.

Section XLII. Banned Hardware and Software

The Vendor will not provide to the State any computer hardware or video surveillance hardware, or any components thereof, or any software that was manufactured, provided, or developed by a covered entity. As used in this paragraph, "covered entity" means the following entities and any subsidiary, affiliate, or successor entity and any entity that controls, is controlled by, or is under common control with such entity: Kaspersky Lab, Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or any entity that has been identified as owned or controlled by, or otherwise connected to, People's Republic of China. The Vendor will immediately notify the State if the Vendor becomes aware of credible information that any hardware, component, or software was manufactured, provided, or developed by a covered entity.

Section XLIII. Use of Portable Devices

The Vendor must prohibit its employees, agents, affiliates, and subcontractors from storing State Data on portable devices, including personal computers, except for devices that are used and kept only at the Vendor's data center(s). All portable devices used for storing State Data must be password protected and encrypted.

Section XLIV. Remote Access

The Vendor will prohibit its employees, agents, affiliates, and subcontractors from accessing State Data remotely except as necessary to provide the services under this Agreement and consistent with all contractual and legal requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication. If the State Data that is being remotely accessed is legally protected data or considered sensitive by the State, then:

A. The device used must be password protected,
B. The data is not put onto mobile media (such as flash drives),
C. No non-electronic copies are made of the data, and
D. A log must be maintained by the Vendor detailing the data which was accessed, when it was accessed, and by whom it was accessed.

The Vendor must follow the State's data sanitization standards, as outlined in this Agreement's Data Sanitization clause, when the remotely accessed data is no longer needed on the device used to access the data.

Section XLV. Data Encryption

If State Data will be remotely accessed or stored outside the State's IT infrastructure, the Vendor warrants that the data will be encrypted in transit (including via any web interface) and at rest at no less than AES256 level of encryption with at least SHA256 hashing.

Section XLVI. Rights, Use, and License of and to State Data

The parties agree that all rights, including all intellectual property rights, in and to State Data will remain the exclusive property of the State. The State grants the Vendor a limited, nonexclusive license to use the State Data solely for the purpose of performing its obligations under this Agreement. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

Protection of personal privacy and State Data must be an integral part of the business activities of the Vendor to ensure there is no inappropriate or unauthorized use of State Data at any time. To this end, the Vendor must safeguard the confidentiality, integrity, and availability of State Data and comply with the following conditions:

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

B. The Vendor will not copy, disclose, retain, or use State Data for any purpose other than to fulfill its obligations under this Agreement.

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

Section XLVII. Third Party Hosting

If the Vendor has the State's data hosted by another party, the Vendor must provide the State the name of this party. The Vendor must provide the State with contact information for this third party and the location of their data center(s). The Vendor must receive from the third party written assurances that the State's data will always reside in the continental United States and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party's employees or contractors. If during the term of this Agreement the Vendor changes from the Vendor hosting the data to a third-party hosting the data or changes third-party hosting provider, the Vendor will provide the State with 180 days' advance notice of this change and at that time provide the State with the information required above.

Section XLVIII. Securing of Data

All facilities used to store and process State Data will employ industry 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 Vendor'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.

Section XLIX. Security Processes

The Vendor will 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 Vendor. For example: virus checking and port sniffing.

Section L. Import and Export of Data

The State will have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Vendor. This includes the ability for the State to import or export data to/from other vendors.

Section LI. System Upgrades

The Vendor must provide advance notice of 30 days to the State of any major upgrades or system changes the Vendor 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 Vendor's systems for vulnerabilities after a system upgrade. These vulnerability scans can include penetration testing of a test system at the State's discretion.

Section LII. Use of Production Data in a Non-Production Environment

The Vendor cannot use protected State Data, whether legally protected or protected by industry standards, in a non-production environment. Any non-production environment that is found to have legally protected 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 production data" is any data protected under federal or state statute or regulation. "Industry standards" are data handling requirements specific to an industry. An example of data protected by industry standards is payment card industry information (PCI). Protected data that is de-identified, aggregated, or hashed is no longer considered to be legally protected.

Section LIII. Banned Services

The Vendor warrants that any hardware or hardware components used to provide the services covered by this Agreement were not manufactured by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

Section LIV. Multifactor Authentication for Hosted Systems

If the Vendor is hosting on their system or performing Software as a Service where there is the potential for the Vendor or the Vendor's subcontractor to see protected State Data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Vendor's MFA, at a minimum must adhere to the requirements of *Level 3 Authentication Assurance for MFA* as defined in NIST 800-63.

south dakota
bit
bureau of
information &
telecommunications

Contractor Agreement to Comply with BIT Information Technology Security Policy

Please return agreement to your designated BIT Contact

Pursuant to the terms of the Agreement between the Contractor and the State, the Contractor is required to sign this Contractor Agreement to Comply with the BIT Information Technology Security Policy (the "Policy") on behalf of its current and future employees who will be responsible for fulfilling the requirements of the Agreement. The Contractor is responsible for ensuring that each Contractor employee complies with all information security policies and procedures found within the Policy. By signature below, the Contractor hereby acknowledges and agrees to the following:

1. In providing services under a contract, the Contractor will use non-public State of South Dakota technology infrastructure or information;
2. The Contractor will protect technology and information assets of the State from unauthorized activities including but not limited to access, disclosure, modification, deletion, and usage;
3. The Contractor agrees to follow state and federal regulations in regard to confidentiality and handling of data;
4. The Contractor has read and agrees to abide by the Policy, which is attached to the Agreement;
5. The Contractor will discuss with a state contact any violation of the Policy;
6. The Contractor understands that any individual found to have violated the Policy is subject to privilege revocation and, at the State's discretion, may be considered a breach of the Agreement with the State;
7. Access to the technology infrastructure of the State or the State's information is a privilege which may be changed or revoked at the discretion of BIT management;
8. Access to the technology infrastructure of the State automatically terminates upon contract termination unless otherwise agreed upon in writing by the parties; and
9. The Contractor shall promptly report violations of the Policy to the State Contact and BIT Help Desk (605-773-4357).

Acknowledgement: State of South Dakota Information Technology Security Policy

Contractor: The individual signing this form on behalf of their entire company affirms that he/she has the authority to commit the Contractor and all its employees to follow the terms of this agreement.

Contractor Signature   Date   BIT Contact   Date

Printed Contractor name and Company name

Appendix (Attachment) ______
Security and Vendor Questions

Agencies: The following questions facilitate agencies acquiring technology that meets state security standards. These questions will assist in improving the quality and the timeliness of the procurement. The Bureau of Information and Telecommunications (BIT) recommends that you utilize your BIT Point of Contact (POC) to set up a planning meeting to review the project and these questions. Understanding the background and context of the questions greatly improves realizing the purpose of the questions. Again, the purpose of the questions is to ensure the product/service being procured will meet the technology and security standards of the state.

If you do not know the details of the technologies the vendor will propose, it is best to keep the question set as broad as possible. If there is a detailed knowledge of what will be proposed, a narrowed set of questions may be possible. Vendors are invited to mark any question that does not apply to their technology as NA (Not Applicable).

Vendors: The following questions help the state determine the best way to assess and integrate your product or service technology with the state's technology infrastructure. Some questions may not apply to the technology you use. In such cases, simply mark the question as NA (Not Applicable). The questions are divided into sections to help identify the point of the questions.

Use the last column as needed to explain your response. Also note, many questions require you to explain your response. The more detailed the response, the better we can understand your product or service.

Where we feel that a Yes/No/NA response is not appropriate, the cell has been grayed out. **If the vendor answers a question by referencing another document or another part of the RFP response, the vendor must provide the page number and paragraph where the information can be found.**

The "BIT" column corresponds to the division within BIT that will be the primary reviewers. If you have questions about the meaning or intent of a question, we can contact the BIT division on your behalf. DC = Data Center; DEV = Development; TEL = Telecommunications; POC = Point of Contract.

System/Product: **The following questions are relevant for all vendors or third parties engaged in this hardware, software, application, or service.**			
			Response
#	**BIT**	**Question**	**Select all that apply**
1	DC DEV	Is your proposed solution a cloud-based solution or an on-prem solution?	☐ State Hosted On-prem (dedicated VM/infrastructure) ☐ State Cloud Provider (PaaS Solution) ☐ Vendor Hosted
2	DC DEV TEL	What type of access is required by vendor or proposed solution to state hosted or external resources?	☐ Not Required ☐ VPN ☐ API ☐ SFTP ☐ Other: (Please state)
3	DC	What type of access is required by vendor to maintain and support the solution?	☐ Not Required ☐ Citrix (For On-prem) ☐ State Cloud Access ☐ Other: (Please state)
4	TEL	If an on-prem solution, which of the following will apply?	☐ IoT Hardware ☐ Non-Windows or non-domain joined solution ☐ Windows-based domain joined hardware ☐ Other: (Please state)
5	DC TEL	Does your proposed solution include/require additional devices connected to the application for activities such as scanning or printing?	☐ Yes ☐ No

6	DC	Does the proposed solution include the use of email?	☐ Yes ☐ No
7	POC TEL	Will there be any desktop software installs, policies, or software required on state managed computers as part of this product?	☐ Yes ☐ No If "Yes", please define:
8	POC	If there are desktop software installs, please provide a link to the licensing requirements or a copy of the licensing requirements.	Please provide link below, if applicable:
9	POC	Will any hardware or peripherals need to be attached to or added to state managed computers?	☐ Yes ☐ No If "Yes", please define:
10	POC	Will any browser plugins be required to install, access, or use this product?	☐ Yes ☐ No If "Yes", please define:
11	POC	Will any products that connect or interact with a state managed computer or network be required as part of this product or project?	☐ Yes ☐ No If "Yes", please define:
12	POC	Will any Bluetooth or RF frequency devices be required as part of this product or project?	☐ Yes ☐ No If "Yes", please define:
13	POC	What operating system is the software/hardware compatible with?	☐ Microsoft Windows 10 ☐ Microsoft Windows 11 ☐ Other (please specify): ☐ N/A

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

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
A1	DC	Does the solution require user authentication, and does that authentication solution support OpenID Connect or OAUTH2 to provide single sign-on?				
A2	DC TEL x	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)?				
A3	POC	Will the system have role-based access?				
A4	DC TEL	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?				

A5	DC TEL	Are account credentials hashed and encrypted when stored?				
A6	DC TEL x	The protection of the State's system and data is of upmost importance. Security scans must be done if: • An application will be placed on the State's system. • The State's system connects to another system. • The contractor hosts State data. • The contractor has another party host State data the State will want to scan that party. **The State would want to scan a test system; not a production system and will not do penetration testing.** The scanning will be done with industry standard tools. Scanning would also take place annually as well as when there are code changes. Are either of these an issue? If so, please explain.				
A7	DC	Will SSL traffic be decrypted and inspected before it is allowed into your system?				
A8	POC x	Will organizations other than the State of South Dakota have access to our data?				
A9	DEV TEL	Do you have developers that possess software security related certifications (e.g., the SANS secure coding certifications)?				
A10	DEV	Are there some requirements for security that are "structured" as part of general release readiness of a product, and others that are "as needed" or "custom" for a particular release?				
A11	TEL	What threat assumptions were made, if any, when designing protections for the software and information assets processed?				
A12	TEL	How do you minimize the threat of reverse engineering of binaries? Are source code obfuscation techniques used?				
A13	TEL	What security criteria, if any, are considered when selecting third party suppliers?				
A14	TEL	How has the software been measured/assessed for its resistance to publicly known vulnerabilities and/or attack patterns identified in the Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumerations (CWEs)? How have the findings been mitigated?				

A15	TEL	Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? If so, please describe what evaluation assurance level (EAL) was achieved, what protection profile the product claims conformance to, and indicate if the security target and evaluation report are available.				
A16	DC TEL	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?				
A17	DC TEL x	Has the product undergone any vulnerability and/or penetration testing? If yes, how frequently, by whom, and are the test reports available under a nondisclosure agreement? How have the findings been mitigated?				
A18	DC	Does your company have an executive-level officer responsible for the security of your company's software products and/or processes?				
A19	DC	How are software security requirements developed?				
A20	DC	What risk management measures are used during the software's design to mitigate risks posed by use of third-party components?				
A21	DC	What is your background check policy and procedure? Are your background checks fingerprint based?				
A22	DEV	Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the software development life cycle? Explain.				
A23	TEL	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?				
A24	DC TEL	Do you have an automated Security Information and Event Management system?				
A25	DC TEL	What types of event logs do you keep and how long do you keep them?				
		a. System events				
		b. Application events				
		c. Authentication events				
		d. Physical access to your data center(s)				
		e. Code changes				

		f. Other:	▨	▨		
A26	DC	How are security logs and audit trails protected from tampering or modification? Are log files consolidated to single servers?				
A27	DEV	a. Are security specific regression tests performed during the development process?				
		b. If yes, how frequently are the tests performed?	▨	▨		
A28	TEL	What type of firewalls (or application gateways) do you use? How are they monitored/managed?	▨	▨		
A29	TEL	What type of Intrusion Detection System/Intrusion Protection Systems (IDS/IPS) do you use? How are they monitored/managed?	▨	▨		
A30	DC TEL	What are your procedures for intrusion detection, incident response, and incident investigation and escalation?	▨	▨		
A31	DC TEL	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)?				
A32	DC TEL	Do you require multifactor authentication be used by employees and subcontractors who have potential access to legally protected State data or administrative control? 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 implementing multifactor authentication? If so, when?	▨	▨		
A33	POC	Will this system provide the capability to track data entry/access by the person, date, and time?				
A34	DC DEV POC TEL	Will the system provide data encryption for sensitive or legally protected information both at rest and transmission? If yes, please provide details.				
A35	DC	a. Do you have a SOC 2 or ISO 27001 audit report?				
		b. Is the audit performed annually?				
		c. If it is SOC 2 audit report, does it cover all 5 of the trust principles?				
		d. If it is a SOC 2 audit report, what level is it?				
		e. Does the audit include cloud service providers?				
		f. Has the auditor always been able to attest to an acceptable audit result?				

		g. Will you provide a copy of your latest SOC 2 or ISO 27001 audit report upon request? A redacted version is acceptable.				
A36	DC	Do you or your cloud service provider have any other security certification beside SOC 2 or ISO 27001, for example, FedRAMP or ITTRUST?				
A37	DC TEL	Are you providing a device or software that can be defined as being Internet of Thing (IoT)? Examples include IP camera, network printer, or connected medical device. 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?				
A38	DC	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?	▨	▨		
A39	DC	What are your policies and procedures for hardening servers?	▨	▨		
A40	DC TEL	**(Only to be used when medical devices are being acquired.)** Please give the history of cybersecurity advisories issued by you for your medical devices. Include the device, date, and the nature of the cybersecurity advisory.	▨	▨		
A41	DC POC	Does any product you propose to use or provide the State include software, hardware, or hardware components manufactured by any company on the US Commerce Department's Entity List?				
A42	DC	Describe your process for monitoring the security of your suppliers.	▨	▨		

Section B. Hosting
The following questions are relevant to any hosted applications, systems, databases, services, and any other technology. The responses should not assume a specific hosting platform, technology, or service but instead the response should address any hosting options available for the proposed solution.

For state-hosted systems that reside in a state-managed cloud:
To minimize impacts to project schedules, vendors are required to provide architectural plans, resource needs, permission plans, and all interfaces – both internal to the state and internet facing for cloud hosted systems. The documentation provided will be reviewed as part of the initial assessment process. If selected for award of a contract, and once the state has approved the submitted materials, a test environment will be provided after contract signature. Systems will be reviewed again before being moved to a production environment. Any usage or processes that are deemed out of compliance with what was approved or represent excessive consumption or risk will require remediation before being moved to production.

						Response
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
B1	POC	Are there expected periods of time where the application will be unavailable for use?				
B2	DC	If you have agents or scripts executing on servers of hosted applications what are the procedures for reviewing the security of these scripts or agents?	▨	▨		

B3	DC	What are the procedures and policies used to control access to your servers? How are audit logs maintained?	▨	▨		
B4	DC DEV POC TEL	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? What are the Recovery Time Objectives and Recovery Point Objectives?				
B5	DC	Explain your tenant architecture and how tenant data is kept separately?	▨	▨		
B6	DC	What are your data backup policies and procedures? How frequently are your backup procedures verified?	▨	▨		
B7	DC DEV TEL	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?				
		a. If yes, summarize the contractual requirements.	▨	▨		
		b. If yes, how do you evaluate the third-party's adherence to the contractual requirements?	▨	▨		
B8	DC	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?				
B9	DC	a. Do you use a security checklist when standing up any outward facing system?				
		b. Do you test after the system was stood up to make sure everything in the checklist was correctly set?				
B10	DC	How do you secure Internet of Things (IoT) devices on your network?	▨	▨		
B11	DC TEL	Do you use Content Threat Removal to extract and transform data?				
B12	DC TEL	Does your company have an endpoint detection and response policy?				
B13	DC TEL	Does your company have any real-time security auditing processes?				
B14	TEL	How do you perform analysis against the network traffic being transmitted or received by your application, systems, or data center? What benchmarks do you maintain and monitor your systems against for network usage and performance? What process(es) or product(s) do you use to complete this analysis, and what results or process(es) can you share?	▨	▨		
B15	TEL	How do you monitor your application, systems, and data center for security events, incidents, or information? What process(es) and/or product(s) do you use to complete this analysis, and what results or process(es) can you share?				
B16	DC	What anti-malware product(s) do you use?	▨	▨		

	TEL					
B17	DC TEL	What is your process to implement new vendor patches as they are released and what is the average time it takes to deploy a patch?				
B18	DC TEL	Have you ever had a data breach? If so, provide information on the breach.				
B19	POC	Is there a strategy for mitigating unplanned disruptions and what is it?				
B20	DC TEL	What is your process for ensuring the software on your IoT devices that are connected to your system, either permanently or intermittently, is maintained and updated?				
B21	POC	Will the State of South Dakota own the data created in your hosting environment?				
B22	DEV	What are your record destruction scheduling capabilities?				

Section C: Database

The following questions are relevant to any application or service that stores data, irrespective of the application being hosted by the state or the vendor.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
C1	DC	Will the system require a database?				
C2	DC	If a Database is required, what technology will be used (i.e. Microsoft SQL Server, Oracle, MySQL)?				
C3	DC	If a SQL Database is required does the cost of the software include the cost of licensing the SQL Server?				
C4	POC	Will the system data be exportable by the user to tools like Excel or Access at all points during the workflow?				
C5	DC DEV	Will the system infrastructure include a separate OLTP or Data Warehouse Implementation?				
C6	DC DEV	Will the system infrastructure require a Business Intelligence solution?				

Section D: Contractor Process

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

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed**
D1	DC POC	Will the vendor provide assistance with installation?				
D2	DC DEV POC TEL	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?				
D3	DEV	What types of functional tests are/were performed on the software during its development (e.g., spot checking, component-level testing, and integrated testing)?				
D4	DEV	Are misuse test cases included to exercise potential abuse scenarios of the software?				

D5	TEL	What release criteria does your company have for its products regarding security?	▨	▨		
D6	DEV	What controls are in place to ensure that only the accepted/released software is placed on media for distribution?	▨	▨		
D7	DC DEV	a. Is there a Support Lifecycle Policy within the organization for the software				
		b. Does it outline and establish a consistent and predictable support timeline?				
D8	DC	How are patches, updates, and service packs communicated and distributed to the State?	▨	▨		
D9	DEV	What services does the help desk, support center, or (if applicable) online support system offer when are these services available, and are there any additional costs associated with the options?	▨	▨		
D10	DC	a. Can patches and service packs be uninstalled?				
		b. Are the procedures for uninstalling a patch or service pack automated or manual?				
D11	DC DEV	How are enhancement requests and reports of defects, vulnerabilities, and security incidents involving the software collected, tracked, prioritized, and reported? Is the management and reporting policy available for review?	▨	▨		
D12	DC	What are your policies and practices for reviewing design and architecture security impacts in relation to deploying patches, updates, and service packs?	▨	▨		
D13	DC	Are third-party developers contractually required to follow your configuration management and security policies and how do you assess their compliance?				
D14	DEV	What policies and processes does your company use to verify that your product has its comments sanitized and does not contain undocumented functions, test/debug code, or unintended, “dead,” or malicious code? What tools are used?	▨	▨		
D15	DEV	How is the software provenance verified (e.g., any checksums or signatures)?	▨	▨		
D16	DEV	a. Does the documentation explain how to install, configure, and/or use the software securely?				
		b. Does it identify options that should not normally be used because they create security weaknesses?				
D17	DEV	a. Does your company develop security measurement objectives for all phases of the SDLC?				
		b. Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?				
D18	DC	a. Is testing done after changes are made to servers?				
		b. What are your rollback procedures in the event of problems resulting from installing a patch or service pack?	▨	▨		
D19	DC	What are your procedures and policies for handling and destroying sensitive data on electronic and printed media?	▨	▨		

D20	DC TEL	How is endpoint protection done? For example, is virus prevention used and how are detection, correction, and updates handled?	▨	▨		
D21	DC TEL	Do you perform regular reviews of system and network logs for security issues?				
D22	DC	Do you provide security performance measures to the customer at regular intervals?				
D23	DC POC	What technical, installation, and user documentation do you provide to the State? Is the documentation electronically available and can it be printed?	▨	▨		
D24	DC DEV POC	a. Will the implementation plan include user acceptance testing?				
		b. If yes, what were the test cases?	▨	▨		
		c. Do you do software assurance?				
D25	DC DEV POC TEL	Will the implementation plan include performance testing?				
D26	DEV POC	Will there be documented test cases for future releases including any customizations done for the State of South Dakota?				
D27	DEV POC	If the State of South Dakota will gain ownership of the software, does the proposal include a knowledge transfer plan?				
D28	DEV POC	Has your company ever conducted a project where your product was load tested?				
D29	DC	Please explain the pedigree of the software. Include in your answer who are the people, organization, and processes that created the software.	▨	▨		
D30	DC	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.	▨	▨		
D31	DC DEV TEL	Does your company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? **Provide a brief explanation**. Will the supplier indemnify the acquirer from these issues in the license agreement? **Provide a brief explanation.**				
D32	DEV	Summarize the processes (e.g., ISO 9000, CMMi), methods, tools (e.g., IDEs, compilers), techniques, etc. used to produce and transform the software.				
D33	DEV	a. Does the software contain third-party developed components?				
		b. If yes, are those components scanned by a static code analysis tool?	▨	▨		
D34	DC DEV TEL	What security design and security architecture documents are prepared as part of the SDLC process? How are they maintained? Are they available to/for review?	▨	▨		

D35	DEV	Does your organization incorporate security risk management activities as part of your software development methodology? If yes, please provide a copy of this methodology or provide information on how to obtain it from a publicly accessible source.				
D36	DC	Does your company 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.				
D37	DC TEL	How are trouble tickets submitted? How are support issues, specifically those that are security-related escalated?				
D38	DC DEV	Please describe the scope and give an overview of the content of the security training you require of your staff, include how often the training is given and to whom. Include training specifically given to your developers on secure development.				
D39	DC TEL x	It is State policy that all 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?				
D40	POC TEL x	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 contractor'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 contractor selection criteria. Is this acceptable?				
D41	DC DEV POC TEL x	(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, when are you planning on doing one?				
		c. If you have not done a risk assessment, would you be willing to do one for this project?				
D42	DEV POC	Will your website conform to the requirements of Section 508 of the Rehabilitation Act of 1973?				

Section E: Software Development
The following questions are relevant to the tools and third-party components used to develop your application, irrespective of the application being hosted by the State or the vendor.

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed.**
E1	DEV POC x	What are the development technologies used for this system? Please indicate version as appropriate.				
		ASP.Net				
		VB.Net				

		C#.Net				
		.NET Framework				
		Java/JSP				
		MS SQL				
		Other				
E2	DC TEL	Is this a browser-based user interface?				
E3	DEV POC	Will the system have any workflow requirements?				
E4	DC	Can the system be implemented via Citrix?				
E5	DC	Will the system print to a Citrix compatible networked printer?				
E6	TEL	If your application does not run under the latest Microsoft operating system, what is your process for updating the application?				
E7	DEV	Identify each of the Data, Business, and Presentation layer technologies your product would use and provide a roadmap outlining how your release or update roadmap aligns with the release or update roadmap for this technology.				
E8	TEL x	Will your system use Adobe Air, Adobe Flash, Adobe ColdFusion, Apache Flex, Microsoft Silverlight, PHP, Perl, Magento, or QuickTime? If yes, explain?				
E9	DEV	To connect to other applications or data, will the State be required to develop custom interfaces?				
E10	DEV	To fulfill the scope of work, will the State be required to develop reports or data extractions from the database? Will you provide any APIs that the State can use?				
E11	DEV POC	Has your company ever integrated this product with an enterprise service bus to exchange data between diverse computing platforms?				
E12	DC	a. 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)?				
		b. If yes, please list those third-party application(s) or system(s).				
E13	DEV	What coding and/or API standards are used during development of the software?				
E14	DEV	Does the software use closed-source Application Programming Interfaces (APIs) that have undocumented functions?				
E15	DEV	How does the software's exception handling mechanism prevent faults from leaving the software, its resources, and its data (in memory and on disk) in a vulnerable state?				
E16	DEV	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?				
E17	DEV	What percentage of code coverage does your testing provide?				
E18	DC	a. Will the system infrastructure involve the use of email?				
		b. Will the system infrastructure require an interface into the State's email infrastructure?				

		c. Will the system involve the use of bulk email distribution to State users? Client users? In what quantity will emails be sent, and how frequently?				
E19	TEL x	a. Does your application use any Oracle products?				
		b. If yes, what product(s) and version(s)?				
		c. Do you have support agreements for these products?				
E20	DC	Explain how and where the software validates (e.g., filter with whitelisting) inputs from untrusted sources before being used.				
E21	TEL	a. Has the software been designed to execute within a constrained execution environment (e.g., virtual machine, sandbox, chroot jail, single-purpose pseudo-user)?				
		b. Is it designed to isolate and minimize the extent of damage possible by a successful attack?				
E22	TEL	Does the program use run-time infrastructure defenses (such as address space randomization, stack overflow protection, preventing execution from data memory, and taint checking)?				
E23	TEL	If your application will be running on a mobile device, what is your process for making sure your application can run on the newest version of the mobile device's operating system?				
E24	DEV	Do you use open-source software or libraries? If yes, do you check for vulnerabilities in your software or library that are listed in:				
		a. Common Vulnerabilities and Exposures (CVE) database?				
		b. Open-Source Vulnerability Database (OSVDB)?				
		c. Open Web Application Security Project (OWASP) Top Ten?				

F. Infrastructure

The following questions are relevant to how your system interacts with the State's technology infrastructure. If the proposed technology does not interact with the State's system, the questions can be marked "NA".

						Response
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed.**
F1	DC	Will the system infrastructure have a special backup requirement?				
F2	DC	Will the system infrastructure have any processes that require scheduling?				
F3	DC	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?				
F4	TEL x	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?				
F5	DC x	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?				

F6	TEL x	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.				
F7	DC	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. The State encryption is also PCI compliant. Would this affect the implementation of your system? If yes, explain.				
F8	DC x	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.				
F9	TEL x	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.				
F10	TEL	It is State policy that systems must support Network Address Translation (NAT) and Port Address Translation (PAT) running inside the State Network. Would this affect the implementation of the system? If yes, explain.				
F11	TEL x	It is State policy that systems must not use dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (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.				
F12	DC	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?				
F13	POC TEL	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. The Contractor should specify what access requirements are for user access to the system and what requirements are for any system level processes. The Contractor should describe all requirements in detail and provide full documentation as to the necessity of the requested access.				
F14	POC x	List any hardware or software you propose to use that is not State standard, the standards can be found at http://bit.sd.gov/standards/.				

F15	DC	Will your application require a dedicated environment?				
F16	DEV POC	Will the system provide an archival solution? If not, is the State expected to develop a customized archival solution?				
F17	DC TEL	Provide a system diagram to include the components of the system, description of the component, and how the components communicate with each other.				
F18	DC	Can the system be integrated with our enterprise Active Directory to ensure access is controlled?				
F19	TEL x	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?				
F20	DC x	Will the server-based software support: a. Windows server 2016 or higher				
		b. IIS7.5 or higher				
		c. MS SQL Server 2016 standard edition or higher				
		d. Exchange 2016 or higher				
		e. Citrix XenApp 7.15 or higher				
		f. VMWare ESXi 6.5 or higher				
		g. MS Windows Updates				
		h. Carbon Black				
F21	TEL x	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?				
F22	DC	All systems that require an email interface must use SMTP Authentication processes managed by BIT Datacenter. Mail Marshal is the existing product used for SMTP relay. Would this affect the implementation of the system?				
F23	DC TEL	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 regarding this process?				
F24	DC TEL	What physical access do you require to work on hardware?				
F25	DC	How many of the vendor's staff and/or subcontractors will need access to the state system, will this be remote access, and what level of access will they require?				

Section G: Business Process
The following questions pertain to how your business model interacts with the State's policies, procedures, and practices. If the vendor is hosting the application or providing cloud services, questions dealing with installation or support of applications on the State's system can be marked "NA".

			Response			
#	**BIT**	**Question**	**YES**	**NO**	**NA**	**Explain answer as needed.**
G1	DC	a. 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?				
		b. If so, will you provide copies of the licenses with a line-item list of their proposed costs before they are finalized?				
G2	POC	Explain the software licensing model.	▨	▨		
G3	DC DEV POC	Is on-site assistance available? If so, what is the charge?				
G4	DEV POC	a. Will you provide customization of the system if required by the State of South Dakota?				
		b. If yes, are there any additional costs for the customization?				
G5	POC	Explain the basis on which pricing could change for the State based on your licensing model.	▨	▨		
G6	POC	Contractually, how many years price lock will you offer 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?	▨	▨		
G7	POC	Will the State acquire the data at contract conclusion?				
G8	POC	Will the State's data be used for any other purposes other than South Dakota's usage?				
G9	DC	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.				
G10	DC	Has civil legal action ever been filed against your company for delivering or failing to correct defective software? Explain.				
G11	DC	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).	▨	▨		
G12	DC	Will you provide on-site support 24x7 to resolve security incidents? If not, what are your responsibilities in a security incident?				
G13	DEV	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?	▨	▨		
G14	DC TEL	Are help desk or support center personnel internal company resources or are these services outsourced to third parties? Where are these resources located?	▨	▨		
G15	DC	Are any of the services you plan to use located offshore (examples include data hosting, data processing, help desk, and transcription services)?				
G16	DC	Is the controlling share (51%+) of your company owned by one or more non-U.S. entities?				
G17	DC	What are your customer confidentiality policies? How are they enforced?	▨	▨		
G18	DC POC	Will this application now or possibly in the future share PHI with other entities on other networks, be				

	x	sold to another party or be accessed by anyone outside the US?				
G19	DC	If the product is hosted at the State, will there be a request to include an application to monitor license compliance?				
G20	DC POC	Is telephone assistance available for both installation and use? If yes, are there any additional charges?				
G21	DC TEL	What do you see as the most important security threats your industry faces?				

Information Technology Security Policy

Contractor Version 6.0

March 2022

General-Information Technology Security Policy-Introduction 7

1.1.4.1. General 12

1.1.4.2. Chief Information Security Officer 12

1.1.4.3. Security Infrastructure Team (SIT) 13

1.1.4.4. Security Operations Team (SOT) 13

1.1.4.5. BIT Executive Working Group on Cyber Security 13

Administrative-I/T Asset Protection-Background Checks 14

10.1.4.1. Background Checks 14

10.1.4.2. Disqualifying Criteria 15

10.1.4.3. Noncriminal Agency Coordinator (NAC) 15

10.1.4.4. Local Agency Security Officer (LASO) 15

10.1.4.5. Background Check Interpretation 16

10.1.4.6. Not Guilty Presumption 16

10.1.4.7. Background Check Information Challenge 16

10.1.4.8. Corrective Action 16

10.1.4.9. Training 16

10.1.4.10. Emailing Background Check Information 16

Administrative-I/T Asset Protection-Confidentiality 16

10.3.4.1. Confidentiality Agreement 17

10.3.4.2. Security Acknowledgement and Access 18

Administrative-I/T Asset Protection-Governance of Regulated Data within Information Systems 18

10.11.4.1. Acquisitions 19

10.11.4.2. Contracts with Third Parties 19

10.11.4.3. Third Party Management Requirements (HIPAA, IRS) - DSS 20

Mainframe-Mainframe Security-Mainframe Accounts 20

210.3.4.1. Unique Account Requirement 20

210.3.4.2. Requests for Mainframe User IDs 20

210.3.4.3. Responsibility for Mainframe User IDs and Passwords 21

Mainframe-Mainframe Security-Mainframe Accounts 21

210.4.4.1. Mainframe User ID Revocation 21

Mainframe-Mainframe Security-Mainframe Access 21

210.25.4.1. Mainframe Access 22

Server-Server Security-Server Maintenance and Administration 22

220.1.4.1. Visibility of Server and Framework Patching Status 23

Server-Server Security-File Transfer Protocol 23

220.7.4.1. Use of File Transfer Protocol Server 24

Server-Server Security-Assurance HIPAA Regulations are Met 24

220.10.4.1. The Data User is Responsible for Adhering to HIPAA Regulations 24

Data Center General-Data Center Security-Cloud Based Services and System Information 25

230.9.4.1. Responsibility for Cloud Based Services and Systems. 25

Data Center General-Data Center Security-Federal Tax Information and Federal Parent Locator Service Information 26

230.11.4.1. Federal Tax Information Returns and Return Information 26

230.11.4.2. What is Not Federal Tax Information 27

230.11.4.3. Safeguarding Federal Tax Information 27

230.11.4.4. Emailing Federal Tax Information 27

Data Center General-Procedural-Physical Access - Proximity Cards 27

230.58.4.1. Proximity Card for Non-BIT Employee Access 28

230.58.4.2. Physical Access to BIT Offices 28

Data Center General-Data Center Security-Accounts Access Control and Authorization 29

230.67.4.1. Individual Access Authorization 29

230.67.4.2. Least Privilege 29

230.67.4.3. Password Requirements 30

230.67.4.4. Individual Access Termination 30

230.67.4.5. Non-State Accounts 30

Data Center General-Payment Card Industry Data Security-Payment Card Industry Data Security Standard 31

230.72.4.1. Payment Card Industry Data Security Standard Requirements 31

Data Center General-Secure Information Technology Acquisition Policy-Secure Information Technology Acquisition Policy 31

230.73.4.1. Acquisition of Services Involving HIPAA Data 32

230.73.4.2. Security Scanning Requirements 32

230.73.4.3. Hardware Maintenance Agreements 32

Data Center General-Use of Production Data-Use of Production Data in a Non-Production Environment. 33

230.74.4.1. Use of Production Data in a Non-Production Environment 34

230.74.4.2. Purging of Data 35

230.74.4.3. Compliance 35

Data Center General-Security Impacts-Data Classification 35

230.75.4.1. Data Classification System 36

230.75.4.2. Classification of Data Produced under Contract 37

230.75.4.3. Data Classification Responsibilities 37

Data Center General-Remote Access to State Information System-Multi-Factor Authentication 38

230.76.4.1. Usage of Multi-Factor Authentication (MFA) 38

230.76.4.2. MFA Tokens 38

Data Center General-Approved Disposal of State Data-Media Sanitization 39

230.77.4.1. Sanitization of Media in a Contractor's Control 39

Data Center General-Transfer of Data-Secure Transfer of Data 40

230.78.4.1. Use of Secure File Transfer Protocol 41

Development-Application Security-Federal Tax Information 41

401.1.4.1. Allocation of Resources and Life Cycle Support 42
401.1.4.2. Information System Security Documentation 42
401.1.4.3. Software Usage Restrictions and User Installed Software 42
401.1.4.4. Developer Configuration Management 42
Development-Application Security-Security Assessments 43
401.3.4.1. Security Assessments 43
401.3.4.2. APM Assessment of Risk 43
401.3.4.3. Security Assessment Report 44
401.3.4.4. Annual Review 44
Development-Application Security-Data Encryption 44
401.5.4.1. Data Encryption 44
401.5.4.2. Hashing Values 45
401.5.4.3. Tools 45
401.5.4.4. Compliance Measurements 45
401.5.4.5. Exceptions 45
401.5.4.6. Non-Compliance 45
Development-Application Security-Authentication and Authorization 45
401.7.4.1. User Authentication and Authorization 46
401.7.4.2. Password Requirements 46
401.7.4.3. Invalid Login Attempts for projects using Federal Tax Information 47
401.7.4.4. reCAPTCHA 47
401.7.4.5. Public Key Infrastructure Certificates 47
401.7.4.6. Tools 47
401.7.4.7. Compliance Measurements 47
401.7.4.8. Exceptions 47
401.7.4.9. Non-Compliance 47
Development-Application Security-Software Development Life Cycle 47
401.9.4.1. Software Development Life Cycle 48
401.9.4.2. Change Management 48
Network-Service-Access Control 48
610.1.4.1. System Access Expectations 49
610.1.4.2. Contractor Access 49
610.1.4.3. Modems 50
610.1.4.4. Remote Access 50
610.1.4.5. Inspection and Review 50
610.1.4.6. Department of Social Services 50
Network-Concept-Security Domain Zones 51
610.3.4.1. Intranet 51
610.3.4.2. DMZ 52

610.3.4.3. Extranet ... 52

Network-Concept-Network Integrity ... 52

610.9.4.1. Responsibilities ... 53

610.9.4.2. Management ... 53

610.9.4.3. Disabling Critical Components of Network Security Infrastructure ... 53

610.9.4.4. Technical Asset or Contractor Connections ... 53

610.9.4.5. Local Area Network ... 53

610.9.4.6. Wide Area Network ... 53

610.9.4.7. Physical Controls ... 53

Network-Communication-Internet ... 54

610.11.4.1. Multiple Connections ... 54

610.11.4.2. Interfaces ... 54

610.11.4.3. Security ... 55

610.11.4.4. Responsibilities ... 55

610.11.4.5. IPv4/IPv6 and Device Names ... 55

Security-Network Discovery-Probing-Exploiting ... 55

620.1.4.1. Limiting Tool Functionality ... 56

620.1.4.2. Exploiting Security Controls of Information Systems ... 56

620.1.4.3. Cracking Application or Passwords ... 56

620.1.4.4. Exemptions ... 56

Security-Content Control-Internet Filtering ... 57

620.5.4.1. Exemptions ... 57

620.5.4.2. Appropriate Use of Administrator Access ... 57

620.5.4.3. DDN Content Filtering ... 58

620.5.4.4. DDN Intranet Content Filtering ... 58

620.5.4.5. Filter Exemption Requests ... 58

ITSP Change Log

Policy Number	Policy Title	New	Revised	Deleted
1.1.4.2	Chief Information Security Officer		03/01/2020	
10.1	Background Checks		03/01/2020	
10.11	Governance of Regulated Data within Information Systems	03/01/2020		
230.10.4.1	Hardware Maintenance Agreements			03/01/2020
230.11	Federal Tax Information and Federal Parent Locator Service Information		03/01/2020	
230.58.4.2	Physical Access to BIT Offices	03/01/2020		
230.67.4.5	Non-State Accounts	03/01/2020		
230.70.4.1	Authentication for Remote Access to the Data Center			03/01/2020
230.73.4.10	Banned Hardware	03/01/2020		
401.1.4.4	Developer Configuration Management		03/01/2020	
401.3.4.2	APM Assessment of Risk	03/01/2020		
401.3.4.3	Security Assessment Report		03/01/2020	
401.3.4.4	Annual Review		03/01/2020	
401.9	Software Development Life Cycle	03/01/2020		
410.1	Azure DevOps Server		03/01/2020	

Staff Augmentation Contractors must follow the BIT Version of the ITSP.

General-Information Technology Security Policy-Introduction

1.1.1. Overview

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

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

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

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

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

Information Technology Security is based on three principles:

- Confidentiality
- Integrity
- Availability

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

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

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

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

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

BIT Mission Statement

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

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

Goals:

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

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

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

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

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

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

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

Information Technology Security Model
The different technology layers of the Information Technology Security Model create opportunities for implementing security:

- User Education involves the training of employees to ensure that proper awareness is brought to the topic of security including steps to take when incidents occur that are outside of the scope of the daily work routine.
- Physical Access is taking appropriate steps to physically safeguard technical equipment such as outlining procedures to prevent workstations from being stolen which can include limiting access to a particular room or locking up the device in a cabinet.
- Network Access includes protecting the State Network from unauthorized access via internal methods and from outside our physical offices. Because technology can be manipulated by individuals or workstations to create a detrimental outcome, safeguards must be implemented to prevent, thwart, and repel workstation attacks from inside State Government and the Internet; access protection is not limited to workstations, it includes smartphones, Internet of Thing devices, environmental controls, and network - network connectivity.

- Workstation Platform means taking advantage of the inherent feature sets of workstation platforms. For example, user id and password capabilities must be used as intended within the workstation platform.
- Cyber Strength Evaluation of business software must apply across in-house developed and third party built or supplied software applications. New applications must be tested before being placed into service and existing applications must be re-evaluated on a regular basis.
- Cyber security language is incorporated within all information technology (I/T) requests for proposals and I/T contracts.
- Information System security entails designing the necessary security features and permissions to ensure that only legitimized staff have proper resource access. The design must consider areas such as viewers of departmental data to individuals that can add data or update records.
- Data security is the protection of the asset; often referred to as the "money in the vault". Ensuring that data is only accessible by permitted applications and personnel is the core of the security model. The data could be credit card numbers, social security numbers, health records, or financial information.

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

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

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

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

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

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

BIT Commissioner:

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

- Reasonable security measures are taken to protect sensitive files and information.
- Enforceable security rules are created and disseminated.

- System resources are managed and monitored to ensure prudent and legitimate usage.
- Alleged security violations are addressed and problems are investigated.
- Designated individuals are responsible for design, configuration, and support of technology resources.
- Employees and Contractors are responsible for:
- Taking the time to read, understand, and ask questions if necessary to clarify the policies defined herein.
- Fully adhering to these policies defined herein.
- Agreeing that use of State technologies which includes equipment, applications, and resources are for work-related purposes.
- Applying recommended password policies.
- Safeguarding sensitive information whether employee / contractor is in the office or traveling for the State.
- Reporting any unusual requests for information or obvious security incidents to the BIT Service Desk.
- Immediately reporting loss of any State technology devices or data.
- Understanding that everyone is a potential target of nefarious individuals seeking 'social engineering' information to be used for illegally accessing State of South Dakota systems and technologies; Hence, be aware that any information provided to outside entities can be dangerous.
- Protecting information technology assets by following policies and procedures.
- Ensuring each individual is authorized to use a given technical asset.
- Understanding and complying with the policies, procedures, and laws related to conditions of use authorizing access to BIT systems and data.
- Not subverting or attempting to subvert security measures.
- Department, Office, Division, or Group Managers are responsible for:
- Creating, disseminating, and enforcing conditions of use for technology and applications in areas of responsibility.
- Responding to concerns regarding alleged or real violations of this policy.
- Ensuring that their employees understand security responsibilities.
- Monitoring the use of South Dakota technology resources by observing usage.
- Determining the access requirements of staff, and ensuring completion of the appropriate forms, including all required authorizations for the application(s) requested by insuring only legitimate staff have access to the set of functions needed to perform defined tasks.
- Communicating terminations and status changes of individuals immediately to the Bureau of Human Resources (BHR) through BHR-defined procedures so that BIT is notified to ensure proper deletion or revision of user access is performed.
- Ensuring a secure physical environment for the staff use of State equipment, information systems, and data.
- Bureau of Information & Telecommunications (BIT) is responsible for:
- Taking reasonable action to assure the authorized use and security of data, networks, applications, and communications amongst these technologies.
- Promptly responding to client questions on details relating to appropriate use of technical resources.
- Providing advice regarding the development of conditions of use or authorized use and procedures through work order requests.
- Ensuring that investigations into any alleged personal workstation or network security compromises, incidents, or problems are conducted.
- Ensuring that appropriate security controls are enabled and are being followed in coordination with BIT staff that are responsible for security administration.
- Verifying and authorizing individuals for an appropriate level of access to only the resources required to perform one's responsibilities.
- Overseeing that an individual has the necessary security authorizations in order for the person to perform assigned duties or tasks.
- Cooperating with appropriate departments, branches, agencies, and law enforcement officials in the course of investigation of alleged violations of policy or law.
- Overseeing the administration of BIT employee and contractor access to BIT facilities.
- Coordinating disaster recovery and testing exercises.

Data Owners

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

- Tracking the data owned/managed by the agency and agency staff.
- Providing BIT notification within 24 hours of any notices regarding federal/state/or industry audits related to any aspects of an agency data, electronic communications, or data processing.
- Working with BIT to ensure access to the data and application(s) is limited to individuals with a legitimate need for the resource access.
- Ensuring that security measures and standards are implemented and enforced in a method consistent with BIT security policies and procedures.
- Establishing measures to ensure the integrity of the data and applications found within the owner's area of responsibility.
- Authorizing individual's appropriate security access rights for accessing the data and applications that are assigned to the data owner for administration.
- Periodically reviewing access rights to determine that the level is still appropriate for authorized users or the level needs to be changed.
- Assuring a process is in place to retain or purge information according to record retention schedules as set by the Records Management office of the Bureau of Administration or other entities.
- Determining the sensitivity and criticality of the data and application based on established Federal, State, and organizational definitions.
- Compliance with system security and integrity; noncompliance and enforcement; reservation of authority and rights is expected of all employees and contractors.
- All State and contractor personnel utilizing information technology resources shall cooperate fully with the cyber security policies of the State.
- The State reserves the right to take all necessary actions to prevent the State network and computing infrastructure from being used to attack, damage, harm, or improperly exploit any internal or external systems or networks.
- The State reserves the right to take all necessary actions to protect the integrity of the State network, the systems attached to the State network, and the data contained therein.
- Violations of federal, State regulations, or any laws respecting information technology will be considered serious matters that may warrant loss of applicable privileges, fines, or more serious action as necessary, to include but not limited, appropriate disciplinary action.

Individuals with questions concerning the policies described herein should be directed to either an immediate State supervisor or the BIT Service 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 regarding policies listed herein. Contractors are expected to follow all policies designated as an employee would follow them. Third party hosting companies also have a set of policies applicable to them. This set of policies is normally a subset of the entire BIT catalog of policies.

1.1.4. Policy

1.1.4.1. General

The policy of BIT is that information is considered a valuable asset and must be appropriately evaluated and protected against all forms of unauthorized access, use, disclosure, modification, or destruction. Security controls must be sufficient to ensure the confidentiality, integrity, availability, and accountability of sensitive and critical information processed and stored on BIT resources and other hosting parties. In addition to implementing the necessary safeguards, each State department, office, and agency is required to determine that the proper levels of protection for the information for that entity exists to include information that is under the control of the department, office, or agency. The security controls that must be applied will be consistent with the classification or value of the information and associated processes that the security controls are designed to protect. Information that is considered by management to be sensitive, critical, or sensitive and critical requires more stringent controls.

1.1.4.2. Chief Information Security Officer

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

- Enforcing the provisions of the Information Technology Security Policy.
- Providing for and implementing, in cooperation with the Data Center, Development, and Telecommunications Divisions of BIT, a written process to investigate any violations or potential violations of this policy or any policy regarding system security and integrity, individually or in cooperation with any appropriate State law enforcement or investigative official.
- Implementing training and education programs to ensure government employees are aware of the risks and expected behaviors towards cyber security.
- Keeping a record of system integrity problems and incidents.
- Maintaining and updating the Information Technology Security Policies.
- Taking such emergency action as is reasonably necessary to provide system control where security is deemed to have been lost or jeopardized.
- Performing periodic security surveys.
- Providing for network security by seeking to preclude misuse of the network of the State to gain or attempt to gain unauthorized access to any system.

- Performing checks of information systems to assess system security and integrity, as well as to determine the use or placement of illegal or improper software or equipment.
- Coordinating the cyber security activities across BIT to ensure technology services and IT policies are effective in balancing security requirements vs. client needs.
- Ensuring processes are in place to remove all data before equipment is disposed or redeployed.
- Coordinating and consulting with the BIT Security Infrastructure Team (SIT), Executive Working Group on Cyber Security, other State departments, Board of Regents, K-12 community, federal Department of Homeland Security, and Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Implementing decisions of the State concerning information technology security.
- Providing reports directly to the Office of the Governor where any serious security violation or potential challenge to security occurs.
- Leading the BIT Security Infrastructure Team.
- Leading the Executive Working Group on Cyber Security.
- Coordinating and entering into agreements with organizations on data-sharing.

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 five 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 five 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."

1. 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.
2. 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.
3. The determination required by Paragraph B will be made by the BIT Chief Information Security Officer (CISO) in consultation with the applicable Division Director.
4. Under no circumstances may an employee or contractor have access to confidential data if the individual is disqualified by this policy.
5. 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.
6. 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.
7. 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.

Administrative-I/T Asset Protection-Governance of Regulated Data within Information Systems

10.11.1. Overview

Standards for the governance of regulated data within information systems.

10.11.2. Purpose

This policy states the requirements for acquisitions and contracts with third parties as the contracts include information systems containing regulated data.

10.11.3. Scope

The scope of the policy includes all software or hardware processing, transferring or housing regulated data within BIT.

10.11.3.1. Scope Assumptions

The State of South Dakota hereby recognizes the status of the State as a carrier of regulated data under the definitions contained in State and federal regulations; "The State of South Dakota must comply with State and federal regulations pertaining to the establishment and management of an appropriate cyber security program in accordance with the regulatory requirements;" Compliance with regulations is mandatory and failure to comply can bring severe sanctions and penalties. BIT recognizes that data stored in BIT data centers is subject to this policy. Contracts and third-party agreements that store regulated data in any non-BIT managed data center must contain language outlined in this policy.

10.11.3.2. Scope Constraints

Business associate agreements referenced herein are the responsibility of the agency. BIT is not a party to those agreements.

10.11.4. Policy

10.11.4.1. Acquisitions

Whenever the information systems contain regulated data, the agencies must:

- Include the following requirements and specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, executive orders, directives, policies, regulations, and standards:
  - Security functional requirements and specifications
  - Security-related documentation requirements
  - Developmental and evaluation-related assurance requirements.
- Ensure third party providers of information systems used to process, store, or transmit the information are secure by designing and implementing the information system using security engineering principles.
- Perform configuration management during information system design, development, implementation, and operation; manage and control changes to the information system. The agency shall implement only organization-approved changes, document approved changes to the information system, and track security flaws and flaw resolution.
- Obtain, protect as required, and make available to authorized personnel adequate documentation for the information system;
- Comply with software usage restrictions enforcing explicit rules governing the installation of software by users.
- Ensure the information system developers create a security test and evaluation plan, implement the plan, and document the results.
- Manage the information system using a system development life cycle methodology that includes information security considerations.

10.11.4.2. Contracts with Third Parties

- For every Business Associate or third party identified, a contract or other written agreement must be in place.
- The agreement must document satisfactory assurances that the business associate or third party meets the applicable requirement set forth in the HIPAA Security Rule, the IRS 1075 for which the protected information is regulated, and any other federal laws or regulations. It must provide that all appropriate cyber safeguards will be implemented including administrative, physical, and technical; that all safeguards reasonable and appropriate that protect the confidentiality, integrity, and availability of regulated information are implemented by the business associate or third party.
- The agreement must identify roles and responsibilities of each party. The definitions must provide that the agents of both the business associates or third parties also comply with the agreement.
- The agreement must allow for the contract to be updated by the covered entity as appropriate by regulatory law.
- The agreement must provide that all business associates or third parties will report any and all security incidents to the covered entity which the business associate or third party suffers.
- The agreement must establish a process for measuring contract performance and terminating the contract if security requirements are not being met by the business associate or third party.
- The agreement must provide that the business associate or third party will authorize termination of the agreement if the contract is materially breached.
- An arrangement other than a business associates' contract is permissible if reasonable and appropriate in a situation when both entities are government entities or if the business associate or third party is required by law to perform a function or activity on behalf of a covered entity. A memorandum of understanding or reliance on law or regulation that requires equivalent actions on the part of the business associate or third party is acceptable only in these situations. The law, regulation, or memorandum that

assures the governmental entities will implement all required safeguards in transactions between the entities must be documented in the agreement.

10.11.4.3. Third Party Management Requirements (HIPAA, IRS) - DSS

All entities that are Business Associates under the HIPAA Security Rule and all third-party services that have been acquired for IRS information systems purposed must be identified.

Mainframe-Mainframe Security-Mainframe Accounts

210.3.1. Overview

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

210.3.2. Purpose

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

210.3.3. Scope

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

210.3.3.1. Scope Assumptions

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

210.3.3.2. Scope Constraints

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

210.3.4. Policy

210.3.4.1. Unique Account Requirement

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

210.3.4.2. Requests for Mainframe User IDs

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

210.3.4.3. Responsibility for Mainframe 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.

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 Service Desk.

Mainframe-Mainframe Security-Mainframe Access

210.25.1. Overview

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

210.25.2. Purpose

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

210.25.3. Scope

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

210.25.3.1. Scope Assumptions

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

210.25.3.2. Scope Constraints

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

210.25.4. Policy

210.25.4.1. Mainframe Access

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

Server-Server Security-Server Maintenance and Administration

220.1.1. Overview

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

220.1.2. Purpose

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

220.1.3. Scope

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

220.1.3.1. Scope Assumptions

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

220.1.3.2. Scope Constraints

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

220.1.4. Policy

220.1.4.1. Visibility of Server and Framework Patching Status

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

Server-Server Security-File Transfer Protocol

220.7.1. Overview

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

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

220.7.2. Purpose

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

220.7.3. Scope

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

220.7.3.1. Scope Assumptions

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

220.7.3.2. Scope Constraints

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

220.7.4. Policy

220.7.4.1. Use of File Transfer Protocol Server

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

Server-Server Security-Assurance HIPAA Regulations are Met

220.10.1. Overview

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

220.10.2. Purpose

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

220.10.3. Scope

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

220.10.3.1. Scope Assumptions

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

220.10.3.2. Scope Constraints

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

220.10.4. Policy

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

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

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-Data Center Security-Federal Tax Information and Federal Parent Locator Service Information

230.11.1. Overview

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

230.11.2. Purpose

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

230.11.3. Scope

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

230.11.3.1. Scope Assumptions

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

230.11.3.2. Scope Constraints

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

230.11.4. Policy

230.11.4.1. Federal Tax Information Returns and Return Information

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

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

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

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

230.11.4.2. What is Not Federal Tax Information

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

230.11.4.3. Safeguarding Federal Tax Information

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

230.11.4.4. Emailing Federal Tax Information

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

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 contractors, or other State personnel that have equipment located in BIT facilities. The general public is not allowed in secure BIT facilities unless approved by the CIO, CISO, or BIT Division level manager, have a government issued means of identification, wear a visitor's badge, and are escorted by authorized BIT personnel.

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 Access
When contractor or agency personnel need temporary access to a secure BIT room, they must provide their escort a photo ID and they and their escort must jointly sign-in using the sign-in sheets inside the door of each room. The contractor or agency personnel must be monitored at all times by an authorized employee of BIT. The individuals cannot be left alone in a secure room without supervision. Only BIT employees with access privileges to the room being accessed are authorized to escort visitors.

Access by Non-BIT Employees
Contractors and other agency personnel that have been issued a proximity card 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.

230.58.4.2. Physical Access to BIT Offices

Access to BIT office spaces, is limited to:

- BIT staff with an identification badge.
- Agency employees with a State or Federal government issued means of identification and visitor's badge, and who are escorted by BIT staff.
- Contractors who have passed a background check, company or government issued means of identification, and have a visitor's badge, and are escorted by BIT staff.
- Vendor representatives with a government issued and a vendor issued means of identification and a visitor's badge and who are escorted by BIT staff.

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

230.67.1. Overview

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

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

230.67.2. Purpose

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

230.67.3. Scope

This policy covers all State IT resources managed by BIT.

230.67.3.1. Scope Assumptions

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

230.67.3.2. Scope Constraints

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

230.67.4. Policy

230.67.4.1. Individual Access Authorization

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

230.67.4.2. Least Privilege

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

230.67.4.3. Password Requirements

Must:

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

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

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

230.67.4.4. Individual Access Termination

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

230.67.4.5. Non-State Accounts

Non-State accounts (NS) are used by persons not directly employed by the State to access the State's domain. An NS account must be requested by an agency by submitting the Non-State Account Request information to the BIT Service Desk (773-4357). The request must be approved by the BIT LAN Services Manager. Any access to resources must follow the principle of least privilege. The requesting agency must specify those State resources to which the NS account needs access.

If an NS account is not logged in for six consecutive months, it will expire. If the account is not logged in for twelve consecutive months, it will be deleted. The agencies are responsible for reviewing their NS Accounts for accounts that are about to be expired or deleted.

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

230.72.1. Overview

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

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

230.72.2. Purpose

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

230.72.3. Scope

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

230.72.3.1. Scope Assumptions

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

230.72.3.2. Scope Constraints

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

230.72.4. Policy

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

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

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 technological unsound and discover all cost associated with the acquisition. These processes must work in conjunction to accomplish those ends. This must be accomplished while recognizing the sometimes-unique needs of BIT's clients and encouraging their full participation in the process. BIT acquisition resources can be found on the BIT Technology Review webpage.

230.73.2. Purpose

The purpose is the acquisition of I/T goods and services as securely as possible.

230.73.3. Scope

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

230.73.3.1. Scope Assumptions

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

230.73.3.2. Scope Constraints

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

230.73.4. Policy

230.73.4.1. Acquisition of Services Involving HIPAA Data

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

230.73.4.2. Security Scanning Requirements

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

230.73.4.3. Hardware Maintenance Agreements

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

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

230.74.1. Overview

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

230.74.2. Purpose

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

230.74.3. Scope

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

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

230.74.3.1. Scope Assumptions

This policy does not apply to Mainframe systems provided both the source and destination environments are the State Mainframe.

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

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

230.74.3.2. Scope Constraints

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

230.74.4. Policy

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

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

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

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

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

The infrastructure scan report must include at least:

- What software, platform and framework were used to perform the scan;
- What general categories were evaluated, host discovery, vulnerability scan, external vulnerability scan or compliance checks;
- Explain the exact details of the test run with those categories;
- General findings or summary report;
- Technical findings, including the exact details of what was found and their severity.

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

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

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

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

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

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

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

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

230.74.4.2. Purging of Data

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

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

230.74.4.3. Compliance

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

1. Notify her or his manager.
2. The manager must notify the Development Director and CISO.
3. The data must be purged.
4. The Development Director and CISO will be notified when it is purged.

If unapproved, unmasked, protected production data is found in a non-production environment, the CISO will decide if it is a security incident. The individual(s) responsible for unapproved unmasked protected production data in a non-production environment may be subject to disciplinary action up to and including dismissal. The placing of unapproved unmasked FTI, HIPAA, or FPLS data on a non-production environment may subject the responsible individual to legal action as stated in IRS 1075 or The American Recovery and Reinvestment Act of 2009.

Data Center General-Security Impacts-Data Classification

230.75.1. Overview

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

230.75.2. Purpose

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

230.75.3. Scope

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

230.75.3.1. Scope Assumptions

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

230.75.3.2. Scope Constraints

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

230.75.4. Policy

230.75.4.1. Data Classification System

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

Data classification is based on three objectives:

- **Confidentiality**
- **Integrity**
- **Availability**

There are four risks associated with each objective:

- **High Risk**
- **Medium Risk**
- **Low Risk**
- **No Risk**

Starting March 31, 2019, all State hosted data must to be classified using *Application Portfolio Management* (APM). Starting June 30, 2019, all Contractor hosted data will be classified using APM. Starting March 1, 2019 all contracts must use the Data Classification Table to assess the contracts risks. This information will be entered on the Contract MOU Review Checklist and Summary. Both the Data Classification Table and the checklist can be found on the *Templates: Technology Contracts* webpage.

Any data that is Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI), Health Information

Portability and Accountability Act (HIPAA), or any information defined under State or Federal statute as confidential is automatically considered to be highly confidential. Examples risk assessments are:

- Public Assistance Records- **High Risk**.
- Pistol Permits Records- **Medium Risk**.
- Inventory of Emergency Vehicles- **Low Risk**.

Further information on protected information can be found in the ITSP Terms and Acronyms Directory and http://intranetbit.sd.gov/standards/PII.aspx.

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

230.75.4.2. Classification of Data Produced under Contract

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

230.75.4.3. Data Classification Responsibilities

It is the data owner's responsibility to:

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

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

It is BIT's responsibility to:

- Assure that proper access controls are implemented, monitored and audited for building, floor and/or cage access in accordance with the data classification labels assigned by the data owner.
- Submit audit results to the data owners as required by law or regulation.
- Perform regular backups of state data.
- Validate data integrity.
- Restore data from backup media.
- Fulfill the data requirements specified in agency security policies, standards and guidelines pertaining to information security and data protection.

- Retain records of data activity that include information on who accessed the data and what data was accessed as considered appropriate by the federal regulatory agency responsible for establishing security controls for the data.
- Provide appropriate security controls for contractor hosted services according to the data classification labels assigned by the data owners.

Data Center General-Remote Access to State Information System-Multi-Factor Authentication

230.76.1. Overview

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

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

230.76.2. Purpose

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

230.76.3. Scope

This policy applies to remote access to the State's network.

230.76.3.1. Scope Assumptions

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

230.76.3.2. Scope Constraints

This policy applies to remote access of State data, equipment, and applications.

230.76.4. Policy

230.76.4.1. Usage of Multi-Factor Authentication (MFA)

Remote access is any access to a State information system by a user communicating through an external network, for example, the Internet. MFA will be required for remote access of State data, equipment and applications. Assurance Level 3 as given in NIST 800-63 must be used.

230.76.4.2. MFA Tokens

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

Mobile device authentication is the preferred method of secondary authentication.

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

Data Center General-Approved Disposal of State Data-Media Sanitization

230.77.1. Overview

There can be a significant risk when sensitive data is collected and kept on media. This media must be appropriately sanitized when no longer needed. Media sanitization methodology is dependent on the confidentiality of the data. Effective sanitization requires knowing where the data is, what the data is, and how the data needs to be protected. Any sanitation must also be checked and documented.

230.77.2. Purpose

The purpose of this policy is to ensure State data is properly sanitized when it is out of the State's control.

230.77.3. Scope

Any media containing State data in a Contractor's control. Media is any material on which data is on or may be recorded on, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical disks. This includes both portable media and media that is installed on devices like workstations, servers, laptops, tablets, and phones.

230.77.3.1. Scope Assumptions

Electronic media with State data must be securely sanitized. The methods used are dependent on the confidentiality of the data.

230.77.3.2. Scope Constraints

Mainframe electronic media is out of scope, it has its own IRS policy requirements. Any media that is in BIT's control is also out of scope. Only media in a Contractor's control is in scope.

230.77.4. Policy

230.77.4.1. Sanitization of Media in a Contractor's Control

The required sanitization method is dependent on the data's classification, see ITSP 230.75.4.1. The data owner is responsible for classifying their data. Contractors are responsible for either sanitizing media in their care or returning it to the State as agreed to in their contract. There are two approved sanitation methods, purge or destroy see NIST 800-88:

Purge- A method of sanitization by applying physical or logical techniques that renders target data recovery infeasible using state of the art laboratory techniques.

Destroy- A method of sanitization that renders target data recovery impossible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Using the data security classification table which can be found on this webpage, classify the confidentiality of the data. The data's status will be based on the risks associated with the data. Any data classified as no risk does not have to be sanitized. No risk data in a contractor's care is still subject to any adverse event notification requirements agreed to in their contract.

These are the media sanitization requirements:

Low confidentiality status:

Purge

Moderate confidentiality status:

Media is not reused- Destroy

Media is reused- Purge

High confidentiality status:

Destroy

In some cases, a Contractor is legally required to keep highly confidential State data intact or otherwise cannot sanitize the data. These circumstances are dealt with in the Contractor's contract with the State. The inability to sanitize data must be included in any response to a Request for Proposals and the data owner must be informed before any contract is signed.

Following sanitization, a Certificate of Media Sanitization should be completed for each piece of media that has been sanitized, the certificate can be found on this webpage. This certificate must be sent to the State Contact who will pass it on to Data Center Director.

Data Center General-Transfer of Data-Secure Transfer of Data

230.78.1. Overview

Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which allows data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. This term is also known as SSH File Transfer Protocol

The SFTP makes sure data is securely transferred using a private and safe data stream. The SFTP's main purpose is to transfer data but can also be used to access an FTP server. The SFTP protocol runs on a secure channel, the client user must be authenticated by the server and no clear text passwords or file data are transferred.

230.78.2. Purpose

The purpose of this policy is to ensure that State data is securely transferred.

230.78.3. Scope

The policy covers any transfer of State data.

230.78.3.1. Scope Assumptions

This policy assumes that State data needs to be sent to or from outside the State's network or between non-State networks.

230.78.3.2. Scope Constraints

The policy does not cover non-State data.

230.78.4. Policy

230.78.4.1. Use of Secure File Transfer Protocol

SFTP must be used when State data is being sent outside the State's network, from another network to the State or is being sent between non-State networks.

Development-Application Security-Federal Tax Information

401.1.1. Overview

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

401.1.2. Purpose

The purpose of this policy is to meet federal security requirements to safeguard FTI on any information system that is acquired 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 having a security assessment.

401.1.3.2. Scope Constraints

The policy only applies to information systems that receive, process, store, or transfer FTI. Security assessments are not conducted on mainframe or desktop applications. If BIT is unable to conduct a security assessment on a vendor hosted application, the vendor must still follow Federal requirements to protect FTI and must meet BIT security requirements specified in contact terms.

401.1.4. Policy

401.1.4.1. Allocation of Resources and Life Cycle Support

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

401.1.4.2. Information System Security Documentation

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

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

A report specifying each area reviewed and the deficiencies found during the assessment process will be stored 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 annually during information system SDLC and operation as well as manage and control changes to the information system to include:

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

Development-Application Security-Security Assessments

401.3.1. Overview

This policy ensures that 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 applications, systems, or websites developed by BIT, contractors, or by any third-party must pass a security assessment prior to being accepted into production.

401.3.3. Scope

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

401.3.3.1. Scope Assumptions

This policy assumes that if the application, website, or system hosts any type of State data can have a security assessment.

401.3.3.2. Scope Constraints

This policy does not apply to mainframe or desktop applications.

401.3.4. Policy

401.3.4.1. Security Assessments

Configurations and installation parameters on all State applications must comply with BIT security management policies, procedures, and standards. All BIT developed applications, third-party applications, internally hosted websites, and externally hosted websites must pass a security assessment before being accepted into production. The originator of the request to release to production has the responsibility of verifying that a security assessment has been performed. The requestor must obtain written verification from the BIT Security Operations Center (SOC) that the software, application, or website has passed the security assessment. Security assessments will be done as part of the Software Development Life Cycle (SDLC) process.

401.3.4.2. APM Assessment of Risk

BIT Development Managers and BIT Point of Contacts (POC) will complete an Assessment of Risk with the agencies that own the system, application, or website and enter the results in Application Portfolio Management (APM). Once the system, application, or website is in production, the frequency of security assessments will be determined by the BIT Security Operations Center (SOC), based on the Assessment of Risk.

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, at minimum.

401.3.4.3. Security Assessment Report

A report specifying each area reviewed or audited during the assessment process will be completed and stored with the system documentation.

401.3.4.4. Annual Review

The BIT Security Operations Center (SOC) will conduct an annual review of security controls for applications and systems. This review will occur concurrently with annual security discussions and will verify:

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

Development-Application Security-Data Encryption

401.5.1. Overview

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

401.5.2. Purpose

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

401.5.3. Scope

All data required to be encrypted must comply with this policy by June 30, 2024.

401.5.3.1. Scope Assumptions

This policy does not apply to Mainframe systems. Mainframe data is encrypted at rest which complies with IRS 1075.

401.5.3.2. Scope Constraints

This policy applies to applications and/or systems that have been developed or rewritten by BIT, contractors employed by BIT, and/or third-party vendors contracted by the State.

401.5.4. Policy

401.5.4.1. Data Encryption

All High Impact Personally Identifiable Information (PII) Data is required to be encrypted at both at rest and in transit. High Impact PII includes, but is not limited to, Social Security Numbers (SSNs), Federal Tax Information (FTI), and Protected Health Information (PHI). See BIT PII Storage Standards http://intranetbit.sd.gov/standards/PIIstorage.aspx. Other data may be recommended or required to be encrypted depending on the results of Software Development Life Cycle (SDLC) security reviews.

401.5.4.2. Hashing Values

Only values that are not going to be decrypted can use a hashing algorithm, all other values must use one of the encryption tools or algorithms listed above. Data that cannot be hashed includes, but is not limited to, Protected Health Information (PHI), Federal Tax Information (FTI), and Personally Identifiable Information (PII).

401.5.4.3. Tools

See BIT PII Storage Standards http://intranetbit.sd.gov/standards/PIIstorage.aspx for the acceptable Tools for encryption.

401.5.4.4. Compliance Measurements

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

401.5.4.5. Exceptions

Any exceptions to this policy must be approved in advance by the BIT Development Enterprise Team Manager.

401.5.4.6. Non-Compliance

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

Development-Application Security-Authentication and Authorization

401.7.1. Overview

This policy defines how authentication and authorization is implemented on websites, applications, and systems for the protection of State data.

401.7.2. Purpose

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

401.7.3. Scope

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

401.7.3.1. Scope Assumptions

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

401.7.3.2. Scope Constraints

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

401.7.4. Policy

401.7.4.1. User Authentication and Authorization

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

- Web applications for sd.gov services that require a logon screen for user authentication must use mySD single sign on (SSO) authentication.
- Desktop applications that require user authentication functionality must use Active Directory or SSO for logon and role management, if possible.
- Mainframe systems that require user authentication functionality must use Resource Access Control Facility (RACF).
- Shared use of User Accounts is not permitted. When user accounts are created, they must be created for an individual - not for a group.

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

401.7.4.2. Password Requirements

The following password requirements must be built into your project.

1. Enforce a minimum password complexity of:
    - Eight-character minimum and a maximum of 64 characters
    - At least one numeric and at least one special character
    - A mixture of at least one uppercase and at least one lowercase letter
    - Storing and transmitting only encrypted representations of passwords
2. Enforce password minimum lifetime restriction of one day
3. Prohibit Password reuse for 24 generations
4. Allow the use of a temporary password for system logon requiring an immediate change to a permanent password
5. Password-protect system initialization (boot) settings
6. Allow passwords to be copied and pasted into the login.
7. No passwords hint.
8. No knowledge-based authentication. (For example, what was the name of your first pet?).

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

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

401.7.4.3. Invalid Login Attempts for projects using Federal Tax Information

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

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

401.7.4.4. reCAPTCHA

ReCAPTCHA will be required on all login pages and public facing form submissions unless they are protected by a login page that already uses reCAPTCHA. For more details on how to implement reCAPTCHA, see Procedure 1451.3.

401.7.4.5. Public Key Infrastructure Certificates

BIT will issue public key infrastructure certificates or obtain public key infrastructure certificates from an approved service provider.

401.7.4.6. Tools

For instructions on how to use mySD in your application, visit mySD.sd.gov and click **Developer Toolkits**.

401.7.4.7. Compliance Measurements

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

401.7.4.8. Exceptions

Any exceptions to this policy must first be approved in advance by the Development Enterprise Team Manager.

401.7.4.9. 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.

Development-Application Security-Software Development Life Cycle

401.9.1. Overview

A Software Development Life Cycle (SDLC) is a consistent and repeatable process for the planning, managing, development, design, testing, and implementation of IT projects.

401.9.2. Purpose

The purpose of this policy is to describe requirements for developing and implementing applications and systems developed by BIT and to ensure that development work is compliant with all regulatory, statutory, Federal, or State guidelines.

401.9.3. Scope

BIT Development is responsible for developing and maintaining in the BIT SDLC.

401.9.3.1. Scope Assumptions

BIT Development IT projects will follow the BIT SDLC.

401.9.3.2. Scope Constraints

BIT Development enhancements and maintenance work are out of scope for this policy.

401.9.4. Policy

401.9.4.1. Software Development Life Cycle

The BIT Software Development Life Cycle (SDLC) defines and documents security processes, roles, and responsibilities. BIT SDLC requires the Application Portfolio Management risk assessment to be completed in APM prior to releasing the application to production. BIT approved agile methodologies will be used to complete the SDLC.

401.9.4.2. Change Management

Change Management is a required process in the BIT SDLC, a Change Management form must be approved prior to releasing any code to production.

Network-Service-Access Control

610.1.1. Overview

Access to the technology infrastructure of the State is essential to maintaining a productive workforce. With this access comes the risk and responsibility of approving, monitoring, and securing the users, workstations, and systems being accessed to protect their confidentiality, integrity, and availability. Controlling access to State technology systems is paramount to avoid damages. Such damages include loss of sensitive or confidential data, destruction or theft of intellectual property, harm to public image, disruption of or damage to public safety activities, and fines or financial liabilities incurred as a result of the damage.

610.1.2. Purpose

The purpose of this policy is to establish rules, guidelines and expectations surrounding access to State technology resources.

610.1.3. Scope

BIT is responsible for designing, configuring and maintaining access to technology systems owned by or operated for the State and its citizens. To supply reliable and secure access, standards and policies for limiting and controlling technology access are established in this policy.

- All State employees and contractors with a State-owned or non-State-owned workstation used to connect to the State network or State infrastructure;
- Remote access connections, to include but not limited to the Internet, used to complete tasks on behalf of the State, including email access and viewing Intranet resources;
- All workstations and devices utilized, and the technical implementations of access used to connect to State networks;
- Communication - originating from and to - DDN Intranet and DMZ.

610.1.3.1. Scope Assumptions

BIT has standardized access control methods and technologies. Only users, workstations, accounts and services compliant with or outlined in this policy are permitted within the DDN. An Agency specific clause is documented in the policy section. The policy applies to the Department of Social Services systems and applications referenced. The policy assumes that Department of Social Services systems and applications referenced are supported or maintained by developers and support staff who have access to remote connections.

610.1.3.2. Scope Constraints

While this policy applies to BIT managed technology systems at our K-12 and Higher Education client locations, this policy does not apply to users and workstations managed and operated by those institutions on their local networks.

610.1.4. Policy

610.1.4.1. System Access Expectations

All access for user and/or system level rights must be granted, reviewed and approved by BIT for accuracy and adequacy to ensure that the appropriate level of access for the intended functions is granted. All access methods utilized to connect to State networks must be implemented through approved combinations of hardware and software security tools that have:

- Unique identification or UID for each user.
- System level identification for each system (e.g. Active Directory accounts).
- Capability to restrict access to specific nodes or network applications.
- Access control software or hardware that protects stored data and the security system from tampering. Audit trails of successful and unsuccessful log-in/access attempts.
- Account credentials must not be stored in unencrypted fashion on any workstation or storage platform.

If a system requires access control methods that fall outside of the listed requirements, the agency sponsoring or requesting that system must work with their BIT Point of Contact to engage BIT in a review of this system. If an exemption would be required, the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms) must be submitted to the BIT HELP Desk (773-4357) for exemption considerations. Unrestricted access into or out of the DDN Intranet and/or DMZ is prohibited. Systems or applications that must call out to a remote system or "call home" for any reason must be vetted and approved by BIT prior to their installation within State infrastructure.

610.1.4.2. Contractor Access

Access to the DDN Intranet and DMZ by contractors is rigorously controlled and managed. The following rules apply to any contractors connecting to State infrastructure:

- Requests for contractor access to technology infrastructure must be approved by BIT. A *Security Exemption Form*, located at the BIT Intranet (http://intranet.bit.sd.gov/forms), submitted to the BIT HELP Desk (773-4357) is required to gain any level of access to State technology systems.
- Contractor access will be limited to the bare-minimum number of systems necessary to accomplish BIT-approved tasks and procedures. This access will be controlled by any number of mechanisms, to include, but not limited to, user accounts, firewall policies, Group Policy, scheduled lockdown and maintenance windows, and/or Skype for Business remote access with BIT personnel monitoring and controlling the access.
- Contractors will not have any access to State workstations without explicit authorization from the BIT Commissioner or BIT Chief Information Security Officer. A *Security Exemption Form*, located at the BIT Intranet (http://intranet.bit.sd.gov/forms), submitted to the BIT HELP Desk (773-4357) is required to request access.
- Administrative accounts on State technology systems must be fully vetted by BIT, periodically reviewed for accuracy and necessity, and limited to the minimum level of systems and access necessary. Domain, enterprise, or similar administrative access levels are strictly prohibited for contractors.

610.1.4.3. Modems

Dial-in or dial-out telephony modems are not allowed to be connected to servers or any other technical assets of the State for any use. Digital Subscription Lines (DSL), cellular and cable modems managed by BIT are not considered telephony modems under this policy.

610.1.4.4. Remote Access

Remote access to the DDN Intranet and DMZ, to include all data files and applications, must be BIT managed, secured and encrypted. Any remote access where Federal Tax Information (FTI) and or Criminal Justice Information System (CJIS) data is accessed over the remote connection must be performed using multi-factor authentication. Supported forms for remote access are:

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

SSL VPNs are not permitted under any circumstances. There is no direct remote access using Remote Desktop Protocol (RDP) allowed from the Internet to the State network or to any cloud-based resource with access to the State network. Indirect RDP access from the Internet is only allowed if it goes through a BIT-approved remote access service.

610.1.4.5. Inspection and Review

BIT will verify compliance to this policy through a number of methods, including but not limited to: periodic walk-throughs, video monitoring, internal and external audits, automated systems processes, business tool reports, and inspections. Feedback will be provided to the required entities.

610.1.4.6. Department of Social Services

In November of each year, a review will be conducted of all personnel with remote access to a major system supporting the needs of the Medicaid Management Information System (MMIS).

- A document will be generated and filed containing the names of personnel with remote access and privileged functions.
- If a determination is made that an individual no longer requires remote access to MMIS, then the remote access will be terminated.

In November of each year, a review will be conducted of all personnel with remote access to a major system supporting the needs of the Division of Child Support.

- A document will be generated and filed containing the names of personnel with remote access and privileged functions.
- If a determination is made that an individual no longer requires remote access to the Division of Child Support System, then the remote access will be terminated.

Network-Concept-Security Domain Zones

610.3.1. Overview

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

610.3.2. Purpose

Different areas or zones of the State network require different levels of protection and security. This policy will define the different zones and expectations for each zone.

610.3.3. Scope

Links to external networks, including but necessarily not limited to, the Internet, federal agencies, and third-party companies must be managed by BIT to ensure the security of the technology infrastructure of the State.

610.3.3.1. Scope Assumptions

All individuals that utilize the DDN must work with BIT to define business practices or align connectivity into one of the three security domain zones which are the Intranet Zone, De-Militarized Zone (DMZ), and Extranet Zone. BIT will not always be able to allow devices and assets to communicate amongst the Security Domain Zones for security reasons, which can include Federal requirements.

610.3.3.2. Scope Constraints

Networks outside of the control of BIT, such as the local university networks operated by Higher Education are outside of the scope of this policy.

610.3.4. Policy

610.3.4.1. Intranet

The Intranet zone is the private, internal network that contains traditional clients of the State and internal business systems. To access the Intranet from external locations, such as the Public Internet, a *Firewall Modification Request Form* must be completed at the BIT Intranet (http://intranet.bit.sd.gov/forms). Only approved methods and technologies can be used to traverse into the Intranet from other network zones.

610.3.4.2. DMZ

The DMZ is the portion of the DDN that provides limited security services and is designed to support services and systems that are utilized by external users. In most situations, the external users require access to resources in the DMZ from the Public Internet. All services and systems that need to be publicly accessible must be placed within the DMZ zone. Access to the DMZ from external locations will require an approved *Firewall Modification Request* Form completed at the BIT Intranet (http://intranet.bit.sd.gov/forms).

610.3.4.3. Extranet

The Extranet zone is segmented from the Intranet zone and the DMZ zone to support network connections for agencies that are not part of the infrastructure of the State Intranet due to business situations. Access to the Extranet from external locations will require an approved *Firewall Modification Request Form* completed at the BIT Intranet (http://intranet.bit.sd.gov/forms).

Network-Concept-Network Integrity

610.9.1. Overview

The DDN is a complex network containing a multitude of inter-dependent systems, connections, and roles. Adequate security measures must be in place to protect the technical assets of the State - physically and logically - from damage, theft, vandalism, and other forms of threats 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 (773-4357) and must provide two weeks' notice. The request must include the dates, times, duration of connection, and the reasons for the connectivity. The requestor must be ready to provide the technical device, any available documentation, and technical contacts to BIT.

610.9.4.5. Local Area Network

All LANs must follow the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard for wired Ethernet networks. State wireless networks operate only in accordance to the wireless policy. Devices and systems in use must meet the specifications laid out by IEEE, to include but not necessarily limited to: 802.1x, 802.3x full duplex, 802.3, 802.3z 1000BASE-LX, 802.3ab 1000BASE-T, 802.3z 1000BASE-X, 802.3ae 10GbE LAN-PHY, 802.1w RSTP, 802.1s, 802.3ad with LACP support, 802.1Q.Wired network ports that are not individually identified as in use by a State employee, such as those in conference rooms or public areas, will remain disabled unless specifically requested via the BIT HELP Desk (773-4357). Requests must include the dates and times these ports will be used by State employees.

610.9.4.6. Wide Area Network

To assure privacy through carrier networks, all carrier-based services utilize private virtual links in a fashion determined and maintained by BIT. This can include, but is not necessarily limited to, carrier managed Multiprotocol Label Switching (MPLS) networks, Metro Ethernet (MEF) networks, dark fiber networks, or IPSec secured virtual private networks (VPNs) over commercial Internet services. Secure socket layer (SSL) VPNs are not allowed in any location on the network.

610.9.4.7. Physical Controls

All line junction points to include cable and line facilities must be located in secure areas or an area that is locked with a key or similar allowed system. Devices to include but not limited to firewalls, servers, switches, hubs, routers, and wireless access points, must be protected from unauthorized physical access.

Network-Communication-Internet

610.11.1. Overview

All devices connected to any technology infrastructure of the State must be protected. BIT is responsible for defining and managing the method, services, and providers used to access the Internet. The Internet is a tremendous tool to be utilized by the State, but the open-system architecture of the Internet creates risks that must be mitigated; BIT does not control the Internet. All Internet access to or originating from the DDN must be approved through the BIT HELP Desk (773-4357).

610.11.2. Purpose

Access to and access from the Internet is approved, managed, and maintained by BIT.

610.11.3. Scope

This policy establishes acceptable expectations for connections from a State office or connected entity to the public Internet. It establishes rules and regulations for the types of, ownership of, and equipment involved in public Internet connections and the DDN.

610.11.3.1. Scope Assumptions

Devices or networks connected to the DDN are expected to comply with this policy.

610.11.3.2. Scope Constraints

Networks not fully under the management of BIT, such as the local county government networks in a courthouse, are out of scope for this policy.

610.11.4. Policy

610.11.4.1. Multiple Connections

No entity or device that participates on the DDN may maintain or install an Internet connection on a network that is also connected to the DDN. Devices are not permitted to be dual homed (connected to the DDN and the public Internet simultaneously). All traffic destined to the Internet from a DDN-connected entity or arriving from the Internet to the DDN must be through BIT managed solutions. K-12 schools or Post-Secondary Educational institutions that are connected to the DDN are not allowed to have a connection to a public ISP.

610.11.4.2. Interfaces

Establishing a direct, real-time connection between the DDN and external organizations networks, such as Federal Government, contractor support, or any other public or private network, must be approved by BIT. Additional tasks may be required from BIT to determine what additional suitable security measures can be implemented for the connection. All real-time, external connections to the technology infrastructure of the State must pass through a firewall or a similar technology entry point.

610.11.4.3. Security

Only services that are explicitly authorized by BIT will be permitted inbound and outbound between the DDN Intranet and the Internet. BIT is responsible for periodically reviewing the implemented security rules for devices that manage inbound and outbound connections. Depending on vulnerabilities and other security risks identified, access to the Internet and from the Internet to the DDN can be restricted and/or expanded without notice. Individuals may not probe security mechanisms at any DDN site, State facility or Internet location without specific, written permission that has been obtained from an authoritative person from each of the affected entities. Similarly, any scanning or security probing activity against a DDN site or State facility requires written permission from the BIT Chief Information Security Officer before such an activity is performed. Unauthorized behavior will be referred to the appropriate law enforcement agency.

610.11.4.4. Responsibilities

Devices connected to the DDN may not be used to make unauthorized connections, to break into, or adversely affect the performance of any asset on the DDN or the Internet. All equipment of the State, including but not limited to, workstations, email system, Internet access tools, and other information systems, are restricted to official State business use only.

610.11.4.5. IPv4/IPv6 and Device Names

BIT is responsible for the management of the DDN public IPv4/IPv6 address space which has components used by the State to include the assignment of device names. Workstations and servers are required to use Dynamic Host Configuration Protocol (DHCP) for the assignment of IPv4/IPv6 addresses. Requests for an exemption from DHCP must be submitted to the BIT HELP Desk (773-4357) for review using the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms). For application access, applications are prohibited from using individual IPv4/IPv6 addresses. Domain names must be created for application reference instead of IPv4/IPv6 address. Requests for an exemption from references to domain names must be submitted to the BIT HELP Desk (773-4357) for review using the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms). If an exemption is granted, the requestor assumes all liability for the support and the maintenance of the application when the host address is required to change due to infrastructure changes on the DDN. IPv4/IPv6 Addresses and device names are considered classified, private information of the State. Naming standards and IPv4/IPv6 addresses for workstations, servers, networking equipment, security devices, and any other technical device are classified as protected, nonpublic information that may not be distributed without express, written approval of the BIT Commissioner to an entity not associated with the State. Other internal network addresses, identifiers, configurations, and related system design information for the technology infrastructure of the State must be restricted. Technical devices and users outside the DDN must be unable to access classified information without explicit management approval. Exemptions to information access must be submitted to the BIT HELP Desk (773-4357) using the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms).

Security-Network Discovery-Probing-Exploiting

620.1.1. Overview

BIT establishes and maintains security controls to secure State devices and protect data; therefore, it is important to provide guidelines to strictly prohibit individuals from probing the DDN network, including network, service and port discovery, or trying to exploit these security controls that exist on the DDN.

620.1.2. Purpose

This policy is designed to provide clarification on Probing/Exploiting Security Controls.

620.1.3. Scope

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

620.1.3.1. Scope Assumptions

Security controls are tested frequently throughout the State infrastructure. This includes testing all BIT managed devices; external devices that require connectivity, including contractors and other unmanaged connections; workstations used by K-12 and Higher Education.

620.1.3.2. Scope Constraints

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

620.1.4. Policy

620.1.4.1. Limiting Tool Functionality

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

620.1.4.2. Exploiting Security Controls of Information Systems

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

620.1.4.3. Cracking Application or Passwords

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

620.1.4.4. Exemptions

Exemptions must be approved, in advance, and in writing, by the BIT Chief Information Security Officer. Activities that are prohibited include but are not limited to the use of scanning software and utilities, keylogging devices, vulnerability assessment tools, and denial-of-service utilities. Exemptions for probing and exploiting security controls must be submitted to the BIT HELP Desk (773-4357) by using the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms).

Security-Content Control-Internet Filtering

620.5.1. Overview

All content accessed from the DDN must be sufficiently protected and monitored to be consistent with BIT Information Technology Security policies. These policies are designed to prevent unauthorized use, modification, disclosure, destruction or denial of access to State assets. Therefore, Internet traffic is monitored for all users and workstations connected to the DDN Intranet. Domain administrative accounts are prohibited from browsing the Internet.

620.5.2. Purpose

Primary purpose is to protect and secure information and assets managed by the State. Secondary purpose is to inform and educate users of their responsibilities towards the use of information, products, and services obtained from the Internet.

620.5.3. Scope

This policy incorporates all users initiating communication between workstations connected to the DDN and the Internet, including web browsing, (IM) instant messaging, file transfer, file sharing and the Intranet.

620.5.3.1. Scope Assumptions

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

620.5.3.2. Scope Constraints

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

620.5.4. Policy

620.5.4.1. Exemptions

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

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

620.5.4.2. Appropriate Use of Administrator Access

Accounts that are members of the SD Domain Administrators group have administrator access to Active Directory services and systems. Use of those accounts specific to Internet access is strictly prohibited. These include Administrators, Domain Administrators, and other accounts with a level of access beyond that of a normal user account. Use of these privileged accounts is restricted to administrative responsibilities and must be prohibited from non-administrative activities. Web browsing or any access to/from the Internet under an Administrator role is strictly prohibited. A malicious website can be used to compromise a workstation or server while online. A compromised asset with elevated Administrative privileges can cause significant additional harm over that of a normal user account.

620.5.4.3. DDN Content Filtering

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

620.5.4.4. DDN Intranet Content Filtering

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

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

620.5.4.5. Filter Exemption Requests

If access to a blocked Internet site is necessary for reasons related to work expectations or data is needed to understand the Internet surfing habits of an individual, the Department Secretary, Bureau Commissioner, or Executive Leadership must submit a request directly to the BIT Commissioner through the BIT HELP Desk (773-4357). Requests related to Internet site administration for the individual to meet work expectations or individual investigations are handled at the highest management level possible. Requests for access to blocked sites and requests for information on surfing habits are documented in the work order system maintained by the BIT HELP Desk (773-4357). The content-filtering category database of the filtering solution is updated daily. Requests must include:

- The name(s) of the requestor.
- The phone number(s) of the requestor.
- The SD Domain UID(s) of the requestor;
- The site for which access is required or the scope of the data requested for an individual.
- The length of time required for access to the site or the time-period to be recorded in a report.

TERMS

Abstraction Technologies
The removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services. See also Directory, IP Address, and Relative Pathing.

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

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

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

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

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

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

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

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

Application Scans
Scans performed by BIT against business software applications to identify security vulnerabilities. This includes applications BIT writes and software that is procured from other software companies.

Application Server
A type of server designed to install, either on workstations or other servers, operate, host applications, and associated services for end users and I/T services. It facilitates the hosting and delivery of applications, which are used by multiple and simultaneously connected local or remote users.

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

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

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

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

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

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

Brute Force Attack
A hacker sets up an automated process against login pages to repeatedly test the user id and/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 servers 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: 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 1 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 alphanumeric sequence followed by a suffix: used as an Internet address to identify the location of particular 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)
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. Even if identifiers are deleted the data is still considered FTI. Information and data provided directly by the taxpayer or third parties is not FTI. If FTI is replaced with the same data provided by the taxpayer or third party, it is no longer considered FTI. For additional information see **Data and Information Types: Return Information.**

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 Is 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.

Non-State Account (NS)
An account that provides access to State IT resources used by a non-State employee.

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 that identifies a person by name or by government-issued identification numbers including Social Security, driver's license, and passport numbers. It also includes data that can be used to distinguish an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. PII also includes financial account information, including account number, credit or debit card numbers, or protected health information (PHI), educational, or employment data 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, industry standard, or has been designated as sensitive by the State or Federal government.

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, doctor, clinic, diagnosis, and prescribed medication. See **Data and Information Types: Protected Health Information** for additional information.

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.

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-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.

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.

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

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

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

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

Statement of Work
A written statement in a solicitation document or contract that describes the State's service requirements.

Structure Query Language
A computer language that is used to manage data, where the data is presented as a set of related tables, and to make queries of a database.

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

ACL
Access Control List

ADABAS
Adaptable Data Base System

BA
Business Associate

BAA

Business Associate Agreement

BHR
South Dakota Bureau of Human Resources

BIT
Bureau of Information & Telecommunications

CISO
Chief Information Security Officer

COTS
Commercial off the Shelf Software

DBMS
Database Management System

DDN
Digital Dakota Network

DDOS
Distributed Denial of Service

DHCP
Dynamic Host Configuration Protocol

DMZ
De-Militarized Zone

DNS
Dynamic Naming System

DOH
South Dakota Department of Health

DSN
Data Source Name

DSS
South Dakota Department of Social Services

EAR
Export Administration Regulations

FERPA
Family Educational Rights and Privacy Act

FPLS
Federal Parent Locator System

FTI
Federal Tax Information

FTP
File Transfer Protocol

GLBA
Gramm-Leach Bliley/ Financial Services Modernization Act

HIPAA
Health Information Portability and Accountability Act

IaaS
Infrastructure as a Service

IEEE
Institute of Electrical and Electronics Engineers

IoT
Internet of Things

IPv4
Internet Protocol version 4

IPv6
Internet Protocol version 6

IRS
Internal Revenue Service

ITAR
International Traffic in Arms Regulations

MANET
Mobile Ad Hoc Network

MIFI
Mobile Wi-Fi

MMIS
Medicaid Management Information System

MOU
Memorandum of Understanding

NIST
National Institute of Standards and Technology

NS
Non-State Account

OWASP
Open Web Application Security Project

PaaS
Platform-as-a-Service

PCI
Payment Card Industry

PII
Personally Identifiable Information

PHI
Protected Health Information

RACF
Resource Access Control Facility

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