STATE OF SOUTH DAKOTA
DEPARTMENT OF LABOR AND REGULATION
123 WEST MISSOURI AVE.
PIERRE, SOUTH DAKOTA 57501

WORKFORCE INNOVATION AND OPPORTUNITY ACT - YOUTH OUTREACH
PROPOSALS ARE DUE NO LATER THAN OCTOBER 6TH, 2017; 5:00PM CST

RFP #: 1089   BUYER: SDDLR   EMAIL: felicia.alspach@state.sd.us

READ CAREFULLY

FIRM NAME: _____   AUTHORIZED SIGNATURE: _____

ADDRESS: _____   TYPE OR PRINT NAME: _____

CITY/STATE: _____   TELEPHONE NO: _____

ZIP (9 DIGIT): _____   FAX NO: _____

FEDERAL TAX ID#: _____   E-MAIL: _____

PRIMARY CONTACT INFORMATION

CONTACT NAME: _____   TELEPHONE NO: _____

FAX NO: _____   E-MAIL: _____

1

1.0 GENERAL INFORMATION

1.1 BIT STANDARD CONTRACT TERMS AND CONDITIONS

Any contract or agreement resulting from this RFP that includes an Information Technology solution will include the State's standard I/T contract terms listed in Appendix A, along with any additional contract terms as negotiated by the parties. If there are no Information Technology solutions or components proposed then Appendices A, B, and C do not apply. As part of the negotiation process the contract terms listed in Appendix A may be altered or deleted. The Offeror should indicate in their response any issues they have 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

1.2 PURPOSE OF REQUEST FOR PROPOSAL (RFP)

The South Dakota Department of Labor and Regulation (SDDLR) is requesting proposals for the purpose of providing outreach services for our Workforce Innovation and Opportunity Act (WIOA) Youth program. SDDLR reserves the right to seek alternative contractors for some of the services outlined in this document at the discretion of SDDLR.

The Workforce Innovation and Opportunity Act Youth program is designed to help youth and young adults with career exploration and guidance, continued support for education attainment, opportunities for skills training in in-demand industries and occupations, and exploring career pathways that lead to job obtainment.

The goal of SDDLR is to increase awareness of WIOA Youth program and to increase the number of Youth participants, who are between the ages of 16 and 24 years old within the State of South Dakota. Outreach will assist in promoting the Workforce Innovation and Opportunity Act Youth Program. Outreach efforts will not only allow recruitment of potential WIOA Youth participants, but also to locate, engage, and communicate with the youth influencers; i.e. educators, parents, counselors.

1.3 ISSUING OFFICE AND RFP REFERENCE NUMBER

The Department of Labor and Regulation for the State of South Dakota is the issuing office for this document. The reference number for the transaction is RFP #1089. This number shall be referred to on all proposals, correspondence, and documentation relating to the RFP.

1.4 SCHEDULE OF ACTIVITIES (SUBJECT TO CHANGE)

RFP Publication	1089
Deadline for Submission of Written Inquiries	September 29, 2017; 5:00PM CST
Proposal Submission	October 6, 2017; 5:00PM CST
Interviews	October 17, 2017
Anticipated Award Decision/Contract Negotiation	October 20, 2017

1.5 SUBMITTING YOUR PROPOSAL

All proposals shall be completed and received by Department of Labor and Regulation 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 and five (5) identical copies of the proposal shall be submitted.

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

> **REQUEST FOR PROPOSAL: #1089**
> **PROPOSAL DUE: OCTOBER 6, 2017**
> **SOUTH DAKOTA DEPARTMENT OF LABOR AND REGULATION**
> **C/O Felicia Alspach**
> **123 West Missouri Ave. Pierre, South Dakota 57501**

All capital letters and no punctuation are used in the address. The South Dakota Department of Labor and Regulation address as displayed should be the only information in the address field.

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 bidder shall attach an explanation to their offer.

1.7   NON-DISCRIMINATION STATEMENT

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

1.8   MODIFICATION OR WITHDRAWAL OF PROPOSALS

Proposals may be modified or withdrawn by the offeror prior to the established due date and time.

No oral, telephonic, telegraphic or facsimile responses or modifications to informal, formal bids, or Request for Proposals will be considered.

1.9   OFFEROR INQUIRIES

Offerors may make written or 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. Email inquiries shall be sent to Felicia Alspach at felicia.alspach@state.sd.us with the

subject line "RFP #1089. Inquiries may also be faxed to 605.773.6184. If inquiries are submitted by mail the envelope should be addressed to:

> SOUTH DAKOTA DEPARTMENT OF LABOR AND REGULATION
> C/O Felicia Alspach
> 123 West Missouri Ave. Pierre, South Dakota 57501

Be sure to reference the RFP number in your letter.

The South Dakota Department of Labor and Regulation prefers to respond to offeror's inquiries (if required) via e-mail. If an offeror does not indicate an email address, the State's response will be sent via fax. If no fax number is provided, the State will mail the response to the offeror. Offerors will be informed of any inquiries and the State's response. Offerors may not rely on any other statements, either of a written or oral nature, that alter any specification or other term or condition of this RFP. Offerors will be notified in the same manner as indicated above regarding any modifications to this RFP.

1.10   PROPRIETARY INFORMATION

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

1.11   LENGTH OF CONTRACT

November 1, 2017 to October 31, 2020

1.12   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.

1.13   DISCUSSIONS WITH OFFERORS (ORAL PRESENTATION/NEGOTIATIONS)

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

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

2.0 STANDARD 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 Work Plan, which will be attached to the contract as Exhibit A and incorporated by reference. The Contractor's response to this RFP shall be considered part of the Work Plan.

2.2 The services to be provided under the contract shall commence on November 1, 2017 and terminate on October 31, 2020.

2.3 The terms of the agreement shall state whether or not the Contractor will use State equipment, supplies or facilities. If the Contractor will use State equipment, supplies or facilities, the scope and conditions of such use will be clearly indicated in the 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 $200,000. $100,000.00 for the first year, and up to but not exceeding $50,000.00 for the two subsequent years. 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 the Prompt Payment Act, SDCL 5-26 for services provided under the contract.

2.5 The agreement shall indicate whether or not the State shall have the option to renew the agreement. If a renewal option is specified, the State shall have the option to renew the agreement (unless otherwise modified by a special contract term, condition, or specification), under the same terms and conditions, for one (1) year intervals. Notice of intent to renew shall be given by the State to the Contractor as mutually agreed upon prior to the end of the current contract term. If the notice of intent to renew is given, the Agreement shall renew unless terminated by either party pursuant to the Termination Provision of the Agreement.

2.6 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 and employees.

2.7 The Contractor, at all times during the term of the 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 $1,000,000.00 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. Worker's Compensation Insurance:

The Contractor shall procure and maintain workers' compensation and employers' liability insurance as required by South Dakota law.

Before beginning work under the Agreement, the Contractor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and which provide that such insurance may not be canceled, except on 30 days' prior written notice to the State. The Contractor shall furnish copies of insurance policies if requested by the State.

2.8 While performing services under agreement with the State, the Contractor is an independent contractor and not an officer, agent, or employee of the State of South Dakota.

2.9 Contractor agrees to report to the State any event encountered in the course of performance of this Agreement which results in injury, or death, 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.

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 requirement of any applicable law.

2.10 **Termination Provision:** The Agreement may be terminated by either party by providing written notice as mutually agreed and specified in the Agreement. In the event the Contractor breaches any of the terms or conditions of the Agreement, the Agreement may be terminated by the State at any time with or without notice. If termination for such a default is effected 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 the Agreement. If after the State termination 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 The Agreement depends upon the continued availability of appropriated funds and expenditure authority from the Legislature for the intended 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, the 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 The 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 thereof, and be signed by an authorized representative of each of the parties thereto.

2.13 The Agreement shall be governed by and construed in accordance with the laws of the State of South Dakota. Any lawsuit pertaining to or affecting the 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 the Agreement, and will be solely responsible for obtaining current information on such requirements.

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

2.16 All other prior discussions, communications and representations concerning the subject matter of the Agreement are superseded by the terms of the Agreement, and except as specifically provided therein, the Agreement constitutes the entire agreement with respect to the subject matter thereof.

2.17 Any notice or other communication required under the Agreement shall be in writing and sent to the appropriate address and individuals indicated in the Agreement, 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.

2.18 The Contractor may not use subcontractors to perform the services described in the Agreement 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 the Agreement, to indemnify the State, and to provide insurance coverage for the benefit of the State in a manner consistent with the 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.

3.0 SCOPE OF WORK

The selected media contractor may be responsible for market research, strategy, development, production, and associated new media components for the South Dakota Department of Labor and Regulation at an estimated budget up to but not exceeding $100,000.00 for the first year, and up to but not exceeding $50,000.00 for each subsequent year. SDDLR will look to the selected agency to provide recommendations for new media components and new creative ideas to reach our targeted groups. With prior approval from SDDLR, sub-contractors may be permissible.

DETAILS

STRATEGY: The contractor will identify and recommend appropriate media and tactics to align with the WIOA – Youth program goal of increasing awareness and participation throughout the State.

CREATIVE SERVICES: The Contractor will work collaboratively with SDDLR as needed on campaign development in the categories listed below including, but not limited to, advertising concepts, messages, themes, slogans, as well as, associated new media components.

The Contractor will provide either the originals or reproducible copies in quantities and formats satisfactory to the State of all material developed within 30 days of the final State approval. The Contractor will consider all reports, recommendations, documents, drawings, plans, specifications, technical data and information, copyrights patents, licenses or other products produced as a result of the services rendered under this Agreement the sole property of the State.

MEDIA PLACEMENT SERVICES: The Contractor may be required to purchase advertising. The Contractor may be required to obtain and place previously produced advertising.

The Contractor will process all invoices from media outlets and provide SDDLR with an itemized monthly bill as directed by the State. The Contractor must provide written documentation of bonus value summaries for media placement as directed by the State.

EVALUATION: The Contractor will include an evaluation component, with measurable goals. Success in regards to the goals will be measured periodically and at the conclusion of the campaign.

4.0 PROPOSAL REQUIREMENTS AND COMPANY QUALIFICATIONS

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

4.2 **Offeror's Contacts**: Offerors and their agents (including subcontractors, employees, consultants, or anyone else acting on their behalf) shall direct all of their questions or comments regarding the RFP, the evaluation, etc. 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/or exclusion from specific procurements. Offerors and their agents who have questions regarding this matter should contact the buyer of record.

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

4.4 Provide the following information related to at least three previous and current service/contracts, performed by the offeror's organization, which are similar to the requirements of this RFP. Provide this information for any service/contract that has been terminated, expired or not renewed in the past three years.

    a. Name, address and telephone number of client/contracting agency and a representative of that agency who may be contacted for verification of all information submitted;

    b. Dates of the service/contract; and

    c. A brief, written description of the specific prior services performed and requirements thereof.

5.0 PROPOSAL RESPONSE FORMAT

5.1 An original and five (5) copies shall be submitted.

    5.1.1 In addition, the offeror should provide one (1) copy of their entire proposal, including all attachments, in Microsoft Word or PDF electronic format.
Due to security concerns the State will not accept electronic proposals via email or on portable media so Offerors must provide a secure location where the State can electronically download the Offeror's proposal(s). This secure location can be a SFTP site, an encrypted FTP site or a webpage using SSL if files are only downloaded and nothing has to be uploaded. Offeror's shall reference their secure web location in the paper copy of their proposal.

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

5.2 All proposals shall be organized and tabbed with labels for the following headings:

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

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

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

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

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

5.2.3.3 A clear description of any options or alternatives proposed.

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

The cost proposal shall be submitted in a separate sealed envelope labeled "Cost Proposal" as outlined in section 1.5 of this RFP.

If an Offeror's technical proposal is not accepted by the State, the cost proposal will be returned to the Offeror unopened.

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

6.0 PROPOSAL EVALUATION AND AWARD PROCESS

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

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

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

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

6.1.4   Availability to the project locale;

6.1.5   Familiarity with the project locale;

6.1.6 Proposed project management techniques; and

6.1.7 Ability and proven history in handling special project constraints.

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

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

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

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

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

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

7.0 COST PROPOSAL

At the time of requested projects, the offeror must provide a breakdown of proposed costs based on the duties outlined under the Scope of Work services. The services include, but are not limited to strategic planning, creative services, media purchasing and evaluation activities. The costs should be broken down, to the extent possible, to reflect the cost associated with each service or component contained in the proposal.

The costs must include, but are not limited to, the commission percent and hourly rates to complete the scope of services. The costs must include a breakdown of how the total $200,000.00 will be utilized. Please submit a separate cost proposal for each year.

7.1 STAFFING

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

7.2 TRAVEL AND EXPENDITURE TABLE

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

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

NOTE: The state asks that consultants accept state per diem. Lodging per diem is $55/night and is readily achievable in South Dakota. Food per diem is $32/day.

7.3 OTHER COSTS

Show any other costs such as: software, hardware, ongoing costs, etc.

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

Appendix A

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

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

SECURITY INCIDENT NOTIFICATION
The Consultant will implement, maintain and update Security Incident procedures that comply with all State standards and Federal requirements. A Security Incident is a violation of any BIT security or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The BIT security policies can be found in the Information Technology Security Policies attached as Appendix B. The State requires notification of a Security Incident involving any of the State's sensitive data in the Contractor's possession. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Agreement constitutes notice by Consultant of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Consultant's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Consultant shall only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the Consultant. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Consultant will be distributing, broadcasting to or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent and the State must approve the content of any information on the Security Incident before it may be distributed, broadcast or otherwise released. The Consultant must reimburse the State for any costs associated with the notification, distributing, broadcasting or otherwise releasing information on the Security Incident.

A. The Consultant shall notify the State Contact within twelve (12) hours of the Consultant becoming aware that a Security Incident has occurred.

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

B. Notification of a Security Incident at a minimum is to consist of the nature of the data exposed, the time the incident occurred and a general description of the circumstances of the incident. If not all of the information is available for the notification within the specified time period Consultant shall provide the State with all of the available information along with the reason for the incomplete notification. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

For the purposes of this Agreement the Security Incident definition in the State's Information Technology Security Policy does not apply.

HANDLING OF SECURITY INCIDENT

At the State's discretion the Consultant will preserve all evidence including but not limited to communications, documents, and logs. The Consultant will also (i) fully investigate the incident, (ii) cooperate fully with the State's investigation of, analysis of, and response to the incident, (iii.) make a best effort to implement necessary remedial measures as soon as it is possible and (iv) document responsive actions taken related to the Security Incident, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement. At the State's discretion and at the Consultant's expense the Consultant will use a credit monitoring service, call center, forensics company, advisors, or public relations firm services that are acceptable to the State. At the State's discretion the Consultant shall offer 5 year's credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State can require a risk assessment of the Consultant, 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 Consultant's expense.

If the Consultant is required by federal law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be reported to the State within twelve (12) hours of the investigation report being completed. If the Consultant is required by federal law or regulation to notify the affected parties, the State must also be notified, unless otherwise required by legal requirements.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to the State under law or equity, the Consultant will reimburse the State in full for all costs incurred by the State in investigation and remediation of the Security Incident including, but not limited, to providing notification to regulatory agencies or other entities as required by law or contract. The Consultant shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

BROWSER

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

SECURITY ACKNOWLEDGEMENT FORM

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

BACKGROUND CHECKS

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

INFORMATION TECHNOLOGY STANDARDS

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

SECURITY

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

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

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

LICENSE AGREEMENTS

Consultant warrants that it has provided to the State and incorporated into this agreement all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software before execution of this agreement. Failure to provide all such license agreements, End User License Agreements, and terms of use shall be a breach of this agreement at the option of the State. The parties agree that neither the State nor its end users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Consultant agrees that it shall indemnify and hold the State harmless from

any and all damages or other detriment, actions, lawsuits or other proceedings that arise from failure to provide all such license agreements, End User License Agreements, and terms of use or that arise from any failure to give the State notice of all such license agreements, End User License Agreements, and terms of use. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

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

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

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

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

Information, Federal Tax Information or any information defined under state statute as confidential Information or fragment thereof.

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

THE STATE OF SOUTH DAKOTA TECHNOLOGY OVERSIGHT
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.

APPLICATION OF CONTRACT TERMS
All of the following terms and provisions are applicable to each and every entity that hosts State data. If the Consultant is proposing to subcontract any hosting of State data to another entity, the relationship between Consultant and any such subcontracting entity must be that of Principal and Agent. No such Agent may act as an independent contractor for Consultant. Consultant must include in its contract with any such Agent explicit terms providing for this Principal and Agent relationship, and Consultant must further supervise such Agent so as to insure that such Agent complies with all of the following terms.

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

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

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

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

performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or that the consultant has with a third-party.

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

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

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

In Witness Whereof, the parties signify their agreement effective the date below first written by the signatures affixed below. By signing this agreement, the Bureau of Information and Telecommunications (BIT) is representing that as the State's technology governing organization it has reviewed only the technical provisions of this agreement.
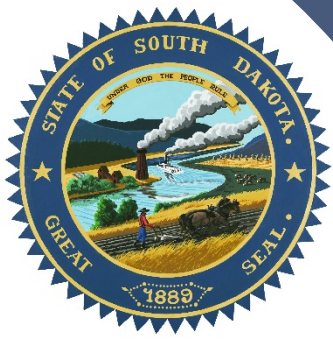
Information Technology Security Policy

CONTRACTOR
v 2.0

Last Updated: 03/13/2017

General-Information Technology Security Policy-Introduction

1.1.1. Overview

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

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

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

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

Information Technology Security is based on three principles:

- Confidentiality;
- Integrity;
- Availability.

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

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

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

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

Information Technology security requires on-going vigilance, and employees should understand the importance of cyber security in the protection of State data and technology resources along with the personal/home computing/data assets of every individual. Guardianship of State data, infrastructure and

applications is a critical priority for BIT. The effort is complicated by the balance needed between usability/service and meaningful protection.

BIT Mission Statement

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

VISION

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

Goals:

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

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

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

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

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

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

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

Instead of relying on one person or a firewall or anti-virus software or some other single piece of hardware or software, a series of assets and entities together build a safe computing environment. Technically, a layered approach is taken to accomplish security within the State which is called the Information Technology (IT)

Security Model. A foundation is established; additional layers may build on the previous layer or may also act independently to provide separate security measures. Each point of accessibility into the wired and wireless network creates security concerns. Security is not limited to technology. A critical portion of cyber security is the human aspect.

Information Technology Security Model

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

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

Partners

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

- State government of South Dakota branches, departments & constitutional offices;
- Internet Service Providers;

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

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

Roles and Responsibilities

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

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

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

BIT Commissioner

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

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

Employees and Contractors are responsible for:

- Taking the time to read, understand and ask questions if necessary to clarify the policies defined herein;
- Fully adhering to these policies defined herein;

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

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

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

Bureau of Information & Telecommunications

BIT is responsible for:

- Taking reasonable action to assure the authorized use and security of data, networks, applications, and communications amongst these technologies;
- Promptly responding to client questions on details relating to appropriate use of technical resources;
- Providing advice regarding the development of conditions of use or authorized use and procedures through work order requests;
- Ensuring that investigations into any alleged personal workstation or network security compromises, incidents or problems are conducted;
- Ensuring that appropriate security controls are enabled and are being followed in coordination with BIT staff that are responsible for security administration;

Information Technology Security Policy - Contractor

SOUTH DAKOTA
CYBER SECURITY

- Verifying and authorizing individuals for an appropriate level of access to only the resources required to perform one's responsibilities;
- Overseeing that an individual has the necessary security authorizations in order for the person to perform assigned duties or tasks;
- Cooperating with appropriate departments, branches, agencies, and law enforcement officials in the course of investigation of alleged violations of policy or law;
- Overseeing the administration of BIT employee and contractor access to BIT facilities;
- Coordinating disaster recovery and testing exercises.

Data Owners

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

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

Compliance with system security and integrity; noncompliance and enforcement; reservation of authority and rights is expected of all employees and contractors.

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

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

Compliance and Enforcement:

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

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

1.1.2. Purpose

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

1.1.3. Scope

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

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

1.1.3.1.   Scope Assumptions

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

1.1.3.2.   Scope Constraints

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

1.1.4. Policy

1.1.4.1.   General

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

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

1.1.4.2. Chief Information Security Officer

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

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

1.1.4.3. Policies

Information is considered a valuable asset and must be appropriately evaluated and protected against all forms of unauthorized access, use, disclosure, modification or destruction. Security controls must be sufficient

to ensure the confidentiality, integrity, availability, and accountability of sensitive and critical information processed and stored on BIT resources.

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

1.1.4.4.   Security Infrastructure Team (SIT)

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

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

1.1.4.5.   Security Operations Team (SOT)

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

- 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, 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.

1.1.4.6.   BIT Executive Working Group on Cyber Security

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

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

The Group shall meet quarterly at a minimum.

Administrative-I/T Asset Protection-Background Checks

10.1.1. Overview

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

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

These verifications must be performed at least every ten years.

10.1.2. Purpose

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

10.1.3. Scope

Background checks shall be limited to criminal history available through State and federal resources. Credit checking and financial history is not subject to this policy.

10.1.3.1. Scope Assumptions

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

10.1.3.2. Scope Constraints

Background checks are not performed for financial or credit information.

10.1.4. Policy

10.1.4.1. Background Checks

The State requires all contractors who write code for or modify State owned software, alter hardware, configure software of State-owned technology resources, have access to source code and/or protected-personally

identifiable or confidential information or have access to secure areas to have background checks and to have these background checks repeated at least every ten years.

These background checks must be fingerprint-based and performed by the State with support from our law enforcement resources. The State will supply the fingerprint cards and the procedure that is to be used to process the fingerprint cards.

It is prohibited to mail 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.

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

The steps involved include:

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

  - Approve;
  - Disapprove hire.

- The manager informs the Executive Assistant to the CISO of the final disposition;
- Fingerprint cards are destroyed;
- Disposition of application is filed.

Administrative-I/T Asset Protection-Confidentiality

10.3.1. Overview

All BIT employees and contracted technology professionals shall be granted appropriate access to information, agency documents, records, programs, files, diagrams, and pertinent data resources needed to

fulfill the job responsibilities of an individual or a contractual agreement. In return, it is expected that such data is treated as a trade secret and individuals will not modify data or disclose data to others without proper authorization. Products resulting from employment or custom built solutions for government agencies are the property of the State.

10.3.2. Purpose

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

10.3.3. Scope

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

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

10.3.3.1.   Scope Assumptions

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

10.3.3.2.   Scope Constraints

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

10.3.4. Policy

10.3.4.1.   Confidentiality Agreement

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

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

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

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

Complying with Legal Obligations

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

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

10.3.4.2. Security Acknowledgement and Access

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

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

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

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

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

Mainframe-Mainframe Security-Overview

210.1.1. Overview

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

210.1.2. Purpose

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

210.1.3. Scope

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

210.1.3.1. Scope Assumptions

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

210.1.3.2. Scope Constraints

This policy applies to mainframe users only.

210.1.4. Policy

210.1.4.1. Security of Mainframe Resources

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

210.1.4.2. Mainframe Access Granted by Business Need

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

210.1.4.3. Requesting Mainframe System Access

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

210.1.4.4. Mainframe Resource Examples

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

Mainframe-Mainframe Security-Mainframe Accounts

210.3.1.   Overview

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

210.3.2.   Purpose

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

210.3.3.   Scope

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

210.3.3.1.   Scope Assumptions

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

210.3.3.2.   Scope Constraints

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

210.3.4.   Policy

210.3.4.1.   Unique Account Requirement

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

210.3.4.2.   Requests for Mainframe User IDs

Access to mainframe systems and data is granted only when a specific business need is proven, as defined by BIT client departments and BIT Mainframe Security Administration. All access for department personnel

must be requested in writing to the BIT Help Desk using the *Employee Request Form (New/Move)* at the BIT Intranet http://intranet.bit.sd.gov/forms. All requests must be made by department personnel authorized to make such requests and access will be assigned based on the principle of least privilege, which requires that a user be given no more privilege than necessary to perform a job.

210.3.4.3.   Responsibility Mainframe User IDs and Passwords

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

210.3.4.4.   Department Security Officers

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

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

Mainframe-Mainframe Security-Mainframe Accounts

210.4.1.   Overview

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

210.4.2.   Purpose

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

210.4.3.   Scope

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

210.4.3.1.   Scope Assumptions

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

210.4.3.2.   Scope Constraints

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

210.4.4.   Policy

210.4.4.1.   Mainframe User ID Revocation

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

Mainframe-Mainframe Security-Disposition of Mainframe Output and Documentation

210.20.1.   Overview

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

210.20.2.   Purpose

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

210.20.3.   Scope

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

210.20.3.1.   Scope Assumptions

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

210.20.3.2.   Scope Constraints

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

210.20.4.   Policy

210.20.4.1.   Agency Defined Access to Output

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

210.20.4.2. Mainframe Documentation

Unless properly checked out by authorized agency representatives, user source documents including, but not limited to, source code, batch job instructions, and scheduling information may not be removed from BIT. Authorized agency representatives who wish to check out documents of this nature must present a valid photo ID and sign for the documents before removing them from BIT. During normal business hours, resources can be checked out in Production Control. After normal business hours, check-out of resources may be conducted at the computer operations door.

Mainframe-Mainframe Security-Mainframe Access

210.25.1.   Overview

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

210.25.2.   Purpose

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

210.25.3.   Scope

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

210.25.3.1. Scope Assumptions

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

210.25.3.2. Scope Constraints

This policy applies to only 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

This policy defines BIT's role regarding enterprise servers.

220.1.2.   Purpose

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

220.1.3.   Scope

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

220.1.3.1.   Scope Assumptions

This applies to the State's distributed system.

220.1.3.2.   Scope Constraints

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

220.1.4.   Policy

220.1.4.1.   Scope of Server Platforms

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

Server-Server Security-File Transfer Protocol

220.7.1.   Overview

The State supported FTP server is meant for short term storage only, and is not meant as a permanent data store. The FTP service should be used for applications uploading or downloading files that have a limited lifespan, transfer of files of large size, and temporary placement for files to be downloaded outside the technology infrastructure of the State. The FTP server is not backed up and all files placed on the server have a lifespan of seven days. If the files are not removed after seven days, the data will be automatically deleted. The FTP server is secured to the Internet; in order for outside entities to get into the FTP server, a FTP username and password is required. In addition, the FTP server is secured from internal clients of the State though the

configuration of the permissions for the device. By default, all State users have Read, Write and Delete access while internet users have no access.

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

220.7.2. Purpose

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

220.7.3. Scope

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

220.7.3.1. Scope Assumptions

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

220.7.3.2. Scope Constraints

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

220.7.4. Policy

220.7.4.1. Use of File Transfer Protocol Server

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

Server-Server Security-Assurance HIPAA Regulations are Met

220.10.1. Overview

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

220.10.2. Purpose

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

220.10.3. Scope

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

220.10.3.1. Scope Assumptions

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

220.10.3.2. Scope Constraints

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

220.10.4. Policy

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

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

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

Server-Server Security-Technical Asset Connections

220.11.1. Overview

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

220.11.2. Purpose

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

220.11.3. Scope

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

Information Technology Security Policy - Contractor

south dakota
bureau of
information &
telecommunications

SOUTH DAKOTA
CYBER SECURITY

220.11.3.1.   Scope Assumptions

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

220.11.3.2.   Scope Constraints

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

220.11.4.   Policy

220.11.4.1.   Requirements for State Connected Devices

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

220.11.4.2.   Exemptions

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

Network-Service-Domain Naming System

220.13.1.   Overview

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

220.13.2.   Purpose

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

220.13.3.   Scope

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

220.13.3.1.   Scope Assumptions

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

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

220.13.3.2. Scope Constraints

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

220.13.4. Policy

220.13.4.1. South Dakota Agency Website Naming

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

220.13.4.2. Registering a Domain

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

The State assumes ownership of all domain names, and BIT manages the registration and renewal of all domains for the State. BIT will maintain a domain name longer than a client agency uses it in many cases to assure the state does not become associated with inappropriate content. BIT will terminate registration of legacy domain names after a period of time, normally 1-2 years after the name is found to be no longer advertised and no longer found within search engines.

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

BIT will automatically renew all active BIT managed domains.

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

230.9.1. Overview

Cloud-based technology providers rely on a wide range of technologies and business models to offer and maintain their services. The security, reliability, portability, resilience, and long-term viability of any given

Information Technology Security Policy - Contractor

south dakota

bureau of
information &
telecommunications

SOUTH DAKOTA
CYBER SECURITY

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

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:

  - o The name of a person with respect to whom a return is filed;
  - o Mailing address;
  - o Taxpayer identification number;
  - o Email addresses;
  - o Telephone numbers;
  - o Social Security Numbers;
  - o Bank account numbers;
  - o Date and place of birth;
  - o Mother's maiden name;
  - o Biometric data (e.g., height, weight, eye color, fingerprints);
  - o 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-Technical Asset Connections-Domain

230.52.1. Overview

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

network site. The individual or organization responsible for the non-compliant technical device or network may also receive a service charge.

230.52.2.   Purpose

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

230.52.3.   Scope

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

230.52.3.1.   Scope Assumptions

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

230.52.3.2.   Scope Constraints

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

230.52.4.   Policy

230.52.4.1.   Protection of External Devices

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

Data Center General-Operational-Change Control Process

230.53.1.   Overview

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

230.53.2.   Purpose

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

230.53.3.   Scope

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

230.53.3.1.   Scope Assumptions

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

230.53.3.2.   Scope Constraints

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

230.53.4.   Policy

230.53.4.1.   Assessment, Alerts and Procedures

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

230.53.4.2.   Routine and Scheduled Changes

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

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

BIT has two regular maintenance periods:

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

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

230.53.4.3. Emergency Changes

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

Data Center General-Procedural-Physical Access - Proximity Cards

230.58.1. Overview

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

230.58.2. Purpose

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

230.58.3. Scope

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

230.58.3.1. Scope Assumptions

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

230.58.3.2. Scope Constraints

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

230.58.4. Policy

230.58.4.1. Proximity Card for Non-BIT Employee Access

Temporary Guest Access

On occasion, situations may exist where a contractor needs to have temporary access to a secured environment. Authorized visitors must provide their escort with a photo ID and the guest and escort must jointly sign in using the sign in sheets located inside the door of each equipment facility. The

individuals are guests of the State, and must be monitored at all times by an authorized employee of BIT. The individuals cannot be left alone in a secured location without supervision. Only BIT employees with access privileges to the secured facility being accessed are authorized to be an escort for visitors.

Permanent Access Procedures for Non-BIT Employees

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

Access to the state campus tunnel system

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

Data Center General-Accountability-Authorization

230.65.1.   Overview

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

230.65.2.   Purpose

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

230.65.3.   Scope

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

230.65.3.1. Scope Assumptions

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

230.65.3.2. Scope Constraints

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

230.65.4.   Policy

230.65.4.1. Administrative Capabilities on Servers

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

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

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

230.67.1.   Overview

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

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

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

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

230.67.2.   Purpose

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

230.67.3.   Scope

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

230.67.3.1. Scope Assumptions

All devices authorized to the DDN or managed by BIT must be protected. Employees and contractors requesting or requiring individual accounts must be aware of the security policies and expectations applied to them and commit to follow them. Privileges will be assigned to individuals only by their immediate supervisor or higher level manager. Security administrators will conduct periodic reviews to verify that only access rights corresponding to an individual's job duties have been assigned. Managers of employees and contractors must notify BIT via defined processes when those managers determine access is no long required or justified to accounts and/or DDN computing data or network resources.

230.67.3.2. Scope Constraints

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

230.67.4.   Policy

230.67.4.1. Individual Access Authorization

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

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

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

230.67.4.2. User Privilege Capabilities

All users with access to the DDN will be granted user level access rights for their BIT managed workstation. Individuals who wish to have Administrative privileges on their BIT managed workstation must contact the BIT Help Desk. Written business justification must be provided with the request by an agency manager for the request to be considered.

Local privileges will be granted if:

- BIT developer needs to test applications and the software they use requires administrator privileges;
- Client software requires administrator privileges in order to run;
- Technical staff needs to install software for testing.

230.67.4.3. Least Privilege

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

230.67.4.4. Password Requirements

- Must be changed every ninety days;
- Must be at least eight characters;

- Must contain at least three of the following four character groups:

  - English uppercase characters (A through Z);
  - English lowercase characters (a through z);
  - Numerals (0 through 9);
  - Non-alphabetic characters (such as !, $, #, %).

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

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

230.67.4.5. Agency Specific Policy DOR, DSS and DLR Resets

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

230.67.4.6. Individual Access Termination

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

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

For situations involving immediate termination, the BIT Help Desk must be notified immediately so that access and authorization assigned to the individual can be disabled.

In all departing employee situations, managers must take reasonable steps to ensure no assets of the State including data, software or hardware are taken, shared, inappropriately modified or destroyed by the individual.

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

230.72.1.   Overview

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

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

230.72.2.   Purpose

To ensure the State is in compliance with PCI security standards

230.72.3.   Scope

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

230.72.3.1.   Scope Assumptions

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

230.72.3.2.   Scope Constraints

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

230.72.4.   Policy

230.72.4.1.   Payment Card Industry Data Security Standard Requirements

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

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

230.73.1.   Overview

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

230.73.2.   Purpose

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

230.73.3.   Scope

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

230.73.3.1.   Scope Assumptions

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

230.73.3.2.   Scope Constraints

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

230.73.4.   Policy

230.73.4.1.   Requests for Proposals

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

230.73.4.2.   Contracts

Contracts including information technology components of any manner must go through the BIT contract process. The BIT Security and Vendor Questions must be included as part of the contracts process. If the RFP process was not utilized, the Security and Vendor questions must be evaluated and reviewed before contract

negotiations can precede. Exceptions to this require the BIT Commissioner's or Chief Security Officer's approval. It may also require a signed release from the agency recognizing the risks involved. This step is determined by the BIT CISO.

230.73.4.3.   Acquisition of Internet of Things Devices

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

230.73.4.4.   Acquisition of Services Involving HIPAA Data

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

230.73.4.5.   Security Scanning Requirements

Applications going onto the State's system or service(s) hosted by a contractor, SaaS, PaaS, IaaS, must be scanned. The policy will require that if a contract has not been signed for any application going on the state's infrastructure that needs to be scanned, authorization to scan must be signed by the contractor first. If the state will have an application or service hosted by a contractor, SaaS, PaaS, IaaS, and the contract has not been signed, a scanning authorization must be signed by the contractor before scanning can be done. Any exceptions to these policies must be approved by the BIT Chief Information Security Officer and may require a signed release by the agency recognizing the risks involved.

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

400.3.1.   Overview

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

400.3.2.   Purpose

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

400.3.3. Scope

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

400.3.3.1. Scope Assumptions

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

400.3.3.2. Scope Constraints

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

400.3.4. Policy

400.3.4.1. Security Assessment

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

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

- It is the responsibility of the application owner, website owner or the party requesting that the application or website be moved into production, to verify that a security assessment is performed;

    o The security assessment process is initiated by sending a request to provision a production environment, to the BIT Help Desk.

- Prior to any hosted application or website being moved into production, written verification from the BIT Security team (BIT.ENTNETWORKSEC@state.sd.us) must exist, verifying that the application or website has passed a security assessment:

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

Information Technology Security Policy - Contractor

SOUTH DAKOTA
CYBER SECURITY

south dakota
bit
bureau of
information &
telecommunications

- If an application has significant changes, a scan will need to be re-initiated:

    o Significant changes include:

        ▪ .Net Version upgrades;
        ▪ Database upgrades;
        ▪ Changes outside of the application.

        ▪ IIS upgrade;
        ▪ Server moves.

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

Security Assessment Task Responsibility List -

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

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

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

Failure to provide such verification may result in the application or website not being placed in production until the security assessment passes and received certification of completion. The application or website will remain unavailable until which time the security assessment certification and testing has been completed and verified in writing, as required. A detailed report that includes remediation requirements is sent to the appropriate parties responsible for the application. This process will repeat itself as many times as needed until the application is deemed secured.

BIT Assessment Team

BIT will form an annual assessment team comprised of BIT individuals who have been identified as having the knowledge and skills to properly assess the requirements for effective security controls, assessing risk, and

Information Technology Security Policy - Contractor

south dakota
bit
bureau of
information &
telecommunications

SOUTH DAKOTA
CYBER SECURITY

understanding the various user needs of the system. These individuals shall also understand the consequences of non-adherence to security controls and processes. The BIT assessment team will conduct an annual assessment of security controls for applications and systems. This assessment will be performed concurrently with the BIT level annual security discussions and will verify:

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

BIT Security Policy

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

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

Assessment Report

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

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

Network-Service-Access Control

610.1.1.   Overview

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

610.1.2.   Purpose

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

610.1.3.   Scope

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

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

610.1.3.1.   Scope Assumptions

BIT has standardized access control methods and technologies. Only users, workstations, accounts and services compliant with or outlined in this policy are permitted within the DDN.

An Agency specific clause is documented in the policy section. The policy applies to the Department of Social Services systems and applications referenced. The policy assumes that Department of Social Services systems and applications referenced are supported or maintained by developers and support staff who have access to remote connections.

610.1.3.2.   Scope Constraints

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

610.1.4.   Policy

610.1.4.1.   System Access Expectations

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

- Unique identification or UID for each user;
- System level identification for each system (e.g. Active Directory accounts);

- Capability to restrict access to specific nodes or network applications;
- Access control software or hardware that protects stored data and the security system from tampering; Audit trails of successful and unsuccessful log-in/access attempts;
- Account credentials must not be stored in unencrypted fashion on any workstation or storage platform.

If a system requires access control methods that fall outside of the listed requirements, the agency sponsoring or requesting that system must work with their BIT Point of Contact to engage BIT in a review of this system. If an exemption would be required, the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms) must be submitted to the BIT HELP Desk (773-4357) for exemption considerations.

Unrestricted access into or out of the DDN Intranet and/or DMZ is prohibited. Systems or applications that must call out to a remote system or "call home" for any reason must be vetted and approved by BIT prior to their installation within State infrastructure.

610.1.4.2.   Contractor Access

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

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

610.1.4.3.   Modems

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

610.1.4.4.   Remote Access

Remote access to the DDN Intranet and DMZ, to include all data files and applications, must be BIT managed, secured and encrypted. Supported forms for remote access are:

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

SSL VPNs are not permitted under any circumstances.

610.1.4.5.   Inspection and Review

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

610.1.4.6.   Department of Social Services

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

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

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

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

Network-Concept-Security Domain Zones

610.3.1.   Overview

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

610.3.2.   Purpose

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

610.3.3.   Scope

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

610.3.3.1.   Scope Assumptions

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

610.3.3.2.   Scope Constraints

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

610.3.4.   Policy

610.3.4.1.   Intranet

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

610.3.4.2.   DMZ

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

610.3.4.3.   Extranet

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

Network-Concept-Network Integrity

610.9.1.   Overview

The DDN is a complex network containing a multitude of inter-dependent systems, connections, and roles. Adequate security measures must be in place to protect the technical assets of the State - physically and

logically - from damage, theft, vandalism, and other forms of threats in order to maintain the integrity of the network.

610.9.2.   Purpose

This policy is to establish the baselines of how network integrity is maintained through technology standards and personnel practices. Adequate security measures must be in place through these standards to protect the technical assets of the State.

610.9.3.   Scope

Technologies, contracts, and practices, to include hardware, software or circuits, must be physically and logically protected against theft, damage, and misuse.

610.9.3.1.   Scope Assumptions

By maintaining accurate accountability of property and instituting appropriate countermeasures to safeguard property, the opportunity for loss, theft or pilferage of valuable technical resources can be greatly diminished. Clients that request the construction of a local or wide area network will work with BIT for the design, implementation, and support matrix of the proposed network segment.

610.9.3.2.   Scope Constraints

While this policy applies to BIT managed equipment at BIT's higher education client locations, this policy does not include the private, internal networks of BIT's higher education clients.

610.9.4.   Policy

610.9.4.1.   Responsibilities

BIT is responsible for providing secure and reliable network connectivity through approved and managed platforms for agencies. This responsibility encompasses local networks, wide-area networks, wireless networks, cellular networks, secure remote access networks, and relevant security components.

610.9.4.2.   Management

BIT is responsible for providing secure and reliable network connectivity through approved and managed platforms for agencies. This responsibility encompasses local networks, wide-area networks, wireless networks, cellular networks, secure remote access networks, and relevant security components.

610.9.4.3.   Disabling Critical Components of Network Security Infrastructure

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

610.9.4.4.   Technical Asset or Contractor Connections

Connection of any contractor and/or their equipment to the DDN or any subsystem requires prior approval from the BIT Commissioner or their designee(s). To request any equipment to be installed or connected to the DDN, requestors should begin by submitting a request to the BIT HELP Desk (773-4357) and must provide two weeks' notice. The request must include the dates, times, duration of connection, and the reasons for the connectivity. The requestor must be ready to provide the technical device, any available documentation, and technical contacts to BIT.

610.9.4.5. Local Area Network

All LANs must follow the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard for wired Ethernet networks. State wireless networks operate only in accordance to the wireless policy. Devices and systems in use must meet the specifications laid out by IEEE, to include but not necessarily limited to: 802.1x, 802.3x full duplex, 802.3, 802.3z 1000BASE-LX, 802.3ab 1000BASE-T, 802.3z 1000BASE-X, 802.3ae 10GbE LAN-PHY, 802.1w RSTP, 802.1s, 802.3ad with LACP support, 802.1Q.

Wired network ports that are not individually identified as in use by a State employee, such as those in conference rooms or public areas, will remain disabled unless specifically requested via the BIT HELP Desk (773-4357). Requests must include the dates and times these ports will be used by State employees.

610.9.4.6. Wide Area Network

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

610.9.4.7. Physical Controls

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

Network-Communication-Internet

610.11.1. Overview

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

610.11.2. Purpose

south dakota
bit
bureau of
information &
telecommunications

Information Technology Security Policy - Contractor

SOUTH DAKOTA
CYBER SECURITY

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

610.11.3.   Scope

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

610.11.3.1.   Scope Assumptions

Devices or networks connected to the DDN are expected to be in compliance with this policy.

610.11.3.2.   Scope Constraints

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

610.11.4.   Policy

610.11.4.1.   Multiple Connections

Preserving control of all Internet or other connections to the DDN and its devices is paramount to maintaining a secure perimeter. Therefore, no entity or device that participates on the DDN may maintain or install an Internet connection on a network that is also connected to the DDN. Devices are not permitted to be dual-homed (connected to the DDN and the public Internet simultaneously). All traffic destined to the Internet from a DDN-connected entity or arriving from the Internet to the DDN must be through BIT managed solutions. K-12 schools or Post-Secondary Educational institutions that are connected to the DDN are not allowed to have a connection to a public ISP.

610.11.4.2.   Interfaces

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

610.11.4.3.   Security

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

permission from the BIT Chief Information Security Officer before such an activity is performed. Unauthorized behavior will be referred to the appropriate law enforcement agency.

610.11.4.4. Responsibilities

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

610.11.4.5. IPv4/IPv6 and Device Names

BIT is responsible for the management of the DDN public IPv4/IPv6 address space which has components used by the State to include the assignment of device names. Workstations and servers are required to use Dynamic Host Configuration Protocol (DHCP) for the assignment of IPv4/IPv6 addresses. Requests for an exemption from DHCP must be submitted to the BIT HELP Desk (773-4357) for review using the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms). For application access, applications are prohibited from using individual IPv4/IPv6 addresses. Domain names must be created for application reference instead of IPv4/IPv6 address. Requests for an exemption from references to domain names must be submitted to the BIT HELP Desk (773-4357) for review using the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms).

If an exemption is granted, the requestor assumes all liability for the support and the maintenance of the application when the host address is required to change due to infrastructure changes on the DDN. IPv4/IPv6 Addresses and device names are considered classified, private information of the State. Naming standards and IPv4/IPv6 addresses for workstations, servers, networking equipment, security devices, and any other technical device are classified as protected, nonpublic information that may not be distributed without express, written approval of the BIT Commissioner to an entity not associated with the State. Other internal network addresses, identifiers, configurations, and related system design information for the technology infrastructure of the State must be restricted. Technical devices and users outside the DDN must be unable to access classified information without explicit management approval. Exemptions to information access must be submitted to the BIT HELP Desk (773-4357) by the use of the *Security Exemption Request Form* at the BIT Intranet (http://intranet.bit.sd.gov/forms).

Security-Network Discovery-Probing-Exploiting

620.1.1.   Overview

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

620.1.2.   Purpose

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

620.1.3. Scope

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

620.1.3.1. Scope Assumptions

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

620.1.3.2. Scope Constraints

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

620.1.4. Policy

620.1.4.1. Exploiting Security Controls of Information Systems

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

620.1.4.2. Cracking Application or Passwords

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

620.1.4.3. Limiting Tool Functionality

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

620.1.4.4. Exemptions

Information Technology Security Policy - Contractor

south dakota
bureau of
information &
telecommunications

SOUTH DAKOTA
CYBER SECURITY

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

Security-Content Control-Internet Filtering

620.5.1. Overview

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

620.5.2. Purpose

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

620.5.3. Scope

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

620.5.3.1. Scope Assumptions

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

620.5.3.2. Scope Constraints

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

620.5.4. Policy

620.5.4.1. DDN Intranet Content Filtering

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

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

620.5.4.2.   Filter Exemption Requests

If access to a blocked Internet site is necessary for reasons related to work expectations or data is needed to understand the Internet surfing habits of an individual, the Department Secretary, Bureau Commissioner, or Executive Leadership must submit a request directly to the BIT Commissioner through the BIT HELP Desk (773-4357). Requests related to Internet Site Administration for the individual to meet work expectations or individual investigations are handled at the highest management level possible.

Requests for access to blocked sites and requests for information on surfing habits are documented in the work order system maintained by the BIT HELP Desk (773-4357). Additionally, the Content-filtering category database of the filtering solution is updated daily.

Requests must include:

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

620.5.4.3.   Exemptions

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

Exemption Details:

- All Internet filtering exemptions must be approved by the BIT Commissioner;
- All requests for the data of an individual pertaining to Internet practices must come from the Department Secretary or Bureau Commissioner of the agency directly to the BIT Commissioner as requests for data are handled at the highest level possible;

- A report on an individual should be completed within two weeks. All requests for data must be approved by the BIT Commissioner.

620.5.4.4. Appropriate Use of Administrator Access

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

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

620.5.4.5. DDN Content Filtering

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

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

➢ **Accreditation**: Scanning of a system looking for security vulnerabilities.

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

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

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

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

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

➢ **Business Associate (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 Business Associate 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.

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

➢ **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.

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

   o RACF;
   o NATURAL.

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

   o **Confidential**: Any data or information other than trade secrets that is materially sensitive in nature, whether manual or electronic, which is valuable and not generally known to the public. Identified here, are few examples - this list is not inclusive - personally identifiable information which is not in the public domain, and if improperly disclosed could be used to steal the identity of an individual, violate the right of an individual to privacy or otherwise harm the individual or business to include, but is not limited to:

      ▪ Social security numbers;
      ▪ Tax payer identification numbers;
      ▪ Any other department determined data that is not in the public domain or intended for release to the public domain and if improperly disclosed might:

         • Cause a significant or severe degradation in mission capability;
         • Cause loss of organizational integrity or public confidence;
         • Result in significant or major damage to organizational assets;
         • Damage the integrity of the State;
         • Result in significant or major financial loss;
         • Result in significant, severe or catastrophic harm to individuals.

   o **Federal Taxpayer Identification (FTI)**: Consists of returns or return information and may contain personally identifiable information (PII). FTI is any return or return information and data received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information and data. FTI does not include information and data provided directly by the taxpayer or third parties. If the taxpayer or third party subsequently provides returns, return information and data or other PII independently, the information and data is not FTI as long as the IRS source information and data is replaced with the newly provided information and data.

   o **Personally Identifiable Information: (PII):** Any information about an individual maintained or collected by an agency, including:

      ▪ Any information that can be used to distinguish or trace an individual's

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

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

- *FERPA*: Education records are protected by FERPA (Family Educational Rights and Privacy Act). Examples: Tax records of parents and students; Class lists, grade rosters, records of advising sessions, grades, financial aid applications;
- *HIPAA*: Certain health information and data is protected by HIPAA (Health Information Portability and Accountability Act) if it is individually identifiable and held or transmitted by a covered entity. Examples: Health records, patient treatment information and data, health insurance billing information and data;
- *GLBA*: Financial records are protected by GLBA (Gramm-Leach-Bliley/Financial Services Modernization Act);
- *ITAR and EAR*: Export Controlled Research is protected by ITAR (International Traffic in Arms Regulations) and EAR (Export Administration Regulations). Example: dual-use technology used for scientific advancement as well as military applications.

o **Return Information:** In general, is any information and data collected or generated by the IRS with regard to any person's liability or possible liability under the Internal Revenue Code (IRC). Return information and data includes, but is not limited to:

- Information and data, including the return, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRC for any tax, penalty, interest, fine, forfeiture, or other imposition or offense;
- Information and data extracted from a return, including names of dependents or the location of business;
- The taxpayer's name, address, and identification number;
- Information and data collected by the IRS about any person's tax affairs, even if identifiers, such as name, address, and identification number are deleted;
- FTI may include PII. FTI may include the following PII elements:

  - The name of a person with respect to whom a return is filed;
  - His or her mailing address;
  - His or her taxpayer identification number;
  - Email addresses;
  - Telephone numbers;
  - Social Security Numbers;
  - Bank account numbers;
  - Date and place of birth;
  - Mother's maiden name;
  - Biometric data (e.g., height, weight, eye color, fingerprints)
  - Any combination of the preceding.

- Returns are forms submitted on paper or electronically with return information to the IRS by, or on behalf of, or with respect to any person or entity; examples

03/13/2017

can include Forms 1040, 941, 1120 and other informational forms, such as 1099 or W-2.

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

- o **Trade Secret**: Any scientific or technical information and data, design, process, procedure, formula, pattern, compilation, program, device, method, technique, process, strategic planning information or improvement whether manual or electronic that is:

  - ▪ Valuable and not generally known to the public, including, but not limited to, workstation software programs;
  - ▪ Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use;
  - ▪ Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

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

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

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

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

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

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

➢ **Federal Parent Locator System (FPLS)**: The FPLS is an assembly of systems operated by OCSE, to assist states in locating noncustodial parents, putative fathers, and custodial parties for the establishment of paternity and child support obligations, as well as the enforcement and modification of orders for child support, custody and visitation. It also identifies support orders or support cases involving the same parties in different states. The FPLS helps federal and state agencies identify over-payments and fraud, and assists with assessing benefits. Definition from: (http://www.acf.hhs.gov/programs/css/resource/federal-parent-locator-service-information-for-families).

03/13/2017

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

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

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

- **Health Insurance Portability and Accountability Act (HIPAA):** Provides a standard for privacy and security protections for an individual's health information. Initially enacted in 1996 it was followed by the Health Information Technology for Economic and Clinical Health (HITECH) act in 2009 and the HIPAA Omnibus Rule in 2013. See also entries for Regulated data, Business Associate and Covered Entity.

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

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

- **IRS**: Internal Revenue Service.

- **Malware**: short for malicious software, is any software used to disrupt workstation operations, gather various types of data and information, gain access to DDN Intranet or display unwanted popups or ads.

- **Metadata:** Metadata is data that describes other data. For example the "date modified" field in a listing of files is metadata.

- **MMIS:** Medicaid Management Information System.

- **Mobile Device:** A portable, wireless computing device that is small enough to be used while held in the hand.

- **Mobile Wi-Fi (MIFI)**: A wireless router that acts as a mobile wireless network hotspot.

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

- **NIST:** National Institute of Standards and Technology.

- **OWASP:** Open Web Application Security Project.

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

- **Peripherals**: Devices that are utilized to enter data and information into a workstation or

retrieve data and information from a workstation.

➢ **Portable Device:** Is 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.

➢ **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.

➢ **Reaccreditation**: The periodic rescanning of a system looking for security vulnerabilities.

➢ **Remote Access Device (RAD)**: RADs include smartphones like iPhones, Windows and Android phones; mobile computing devices like iPods, iPads, and notebooks; as well as other non-state workstations such as public access terminals located in libraries, schools and airports or any other internet capable computing device that is mobile or outside the management of BIT. This list is not inclusive.

➢ **Resource Access Control Facility (RACF):** An IBM software product. It is a security system that provides access control and auditing functionality for the z/OS and z/VM operating systems.

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

➢ **Security Incident**: Any cyber security event or threat of an event affecting the normal operation of a workstation, software application or the technology infrastructure of the State.

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

➢ **Security Operations Team (SOT)**: The BIT SOT meets daily to review any cyber security findings or issues with the State Infrastructure within the previous day.

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

➢ **State**: Refers to the government of the State of South Dakota when capitalized.

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

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

  o USERID;
  o A User ID;
  o SD Domain Account.

03/13/2017

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

Please return agreement to your BIT Manager or Designated BIT Contact

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

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

    Information Technology Security Policy – BIT: http://intranet.bit.sd.gov/policies/
    Information Technology Security Policy – CLIENT: http://intranet.bit.sd.gov/policies/
    Information Technology Security Policy – CONTRACTOR: http://bit.sd.gov/vendor/default.aspx

Acknowledgement: State of South Dakota Information Technology Security Policy

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

_____ _____   _____   _____
Employee or Contractor signature   Date   Employee's BIT Manager   Date

_____
Employee or Contractor name and Company name in block capital letters