



Information Technology Security Policy

Contractor Version 5.0

March 1, 2020

General-Information Technology Security Policy-Introduction.....	4
1.1.4.1. General.....	9
1.1.4.2. Chief Information Security Officer.....	9
1.1.4.3. Security Infrastructure Team (SIT).....	10
1.1.4.4. Security Operations Team (SOT)	10
1.1.4.5. BIT Executive Working Group on Cyber Security.....	11
Administrative-I/T Asset Protection-Background Checks	11
10.1.4.1. Background Checks	11
10.1.4.2. Disqualifying Criteria	12
10.1.4.3. Noncriminal Agency Coordinator (NAC).....	12
10.1.4.4. Local Agency Security Officer (LASO)	13
10.1.4.5. Background Check Interpretation	13
10.1.4.6. Not Guilty Presumption	13
10.1.4.7. Background Check Information Challenge	13
10.1.4.8. Corrective Action.....	13
10.1.4.9. Training.....	13
10.1.4.10. Emailing Background Check Information	13
Administrative-I/T Asset Protection-Confidentiality.....	14
10.3.4.1. Confidentiality Agreement	14
10.3.4.2. Security Acknowledgement and Access	15
Server-Server Security-Server Maintenance and Administration.....	15
220.1.4.1. Visibility of Server and Framework Patching Status	16
Data Center General-Data Center Security-Accounts Access Control and Authorization	16
230.67.4.1. Individual Access Authorization	17
230.67.4.2. Least Privilege	17
230.67.4.3. Password Requirements	17
230.67.4.4. Individual Access Termination	17
230.67.4.5. Non-State Accounts	18
Data Center General-Use of Production Data-Use of Production Data in a Non-Production Environment. 18	
230.74.4.1. Use of Production Data in a Non-Production Environment	19
230.74.4.2. Purging of Data	20
230.74.4.3. Compliance	20
Data Center General-Security Impacts-Data Classification	21
230.75.4.1. Data Classification System.....	21
230.75.4.2. Classification of Data Produced under Contract.....	22
230.75.4.3. Data Classification Responsibilities	22
Data Center General-Remote Access to State Information System-Multi-Factor Authentication	23
230.76.4.1. Usage of Multi-Factor Authentication (MFA)	24
230.76.4.2. MFA Tokens	24

Data Center General-Approved Disposal of State Data-Media Sanitization	24
230.77.4.1. Sanitization of Media in a Contractor's Control.....	25
Development-Application Security-Security Assessments	26
401.3.4.1. Security Assessments	26
TERMS.....	27
ACRONYMS.....	35

ITSP Change Log

Policy Number	Policy Title	New	Revised	Deleted
1.1.4.2	Chief Information Security Officer		03/01/2020	
10.1	Background Checks		03/01/2020	
230.67.4.5	Non-State Accounts	03/01/2020		

General-Information Technology Security Policy-Introduction

1.1.1. Overview

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

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

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

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

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

Information Technology Security is based on three principles:

- Confidentiality
- Integrity
- Availability

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

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

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

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

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

BIT Mission Statement

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

Vision

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

Goals:

Provide a Reliable, Secure and Modern Infrastructure.

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

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

Deliver Valuable Services at Economical Costs.

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

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

Build and Retain a Highly Skilled Workforce.

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

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

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

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

Information Technology Security Model

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

- User Education involves the training of employees to ensure that proper awareness is brought to the topic of security including steps to take when incidents occur that are outside of the scope of the daily work routine.
- Physical Access is taking appropriate steps to physically safeguard technical equipment such as outlining procedures to prevent workstations from being stolen which can include limiting access to a particular room or locking up the device in a cabinet.
- Network Access includes protecting the State Network from unauthorized access via internal methods and from outside our physical offices. Because technology can be manipulated by individuals or workstations to create a detrimental outcome, safeguards must be implemented to prevent, thwart, and repel workstation

attacks from inside State Government and the Internet; access protection is not limited to workstations, it includes smartphones, Internet of Thing devices, environmental controls, and network - network connectivity.

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

Partners

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

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

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

Roles and Responsibilities

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

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

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

BIT Commissioner:

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

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

- Overseeing the administration of BIT employee and contractor access to BIT facilities.
- Coordinating disaster recovery and testing exercises.

Data Owners

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

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

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

Compliance and Enforcement:

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

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

1.1.2. Purpose

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

1.1.3. Scope

The **Information Technology Security Policy** is intended to address the range of cyber security related topics. Detailed policies are listed and explained throughout the document. Security topics included are workstation, server, network, applications development, mobile, administrative, operational, and other IT areas. The clientele served by BIT is very diverse. Including the Executive and Judicial branches of State government, local - municipal - county governments, K-12 schools, technical schools, and colleges and universities. Different policies will have a different set of impacted clienteles.

1.1.3.1. Scope Assumptions

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

1.1.3.2. Scope Constraints

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

1.1.4. Policy

1.1.4.1. General

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

1.1.4.2. Chief Information Security Officer

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

- Enforcing the provisions of the Information Technology Security Policy.
- Providing for and implementing, in cooperation with the Data Center, Development, and Telecommunications Divisions of BIT, a written process to investigate any violations or potential violations of this policy or any policy regarding system security and integrity, individually or in cooperation with any appropriate State law enforcement or investigative official.
- Implementing training and education programs to ensure government employees are aware of the risks and expected behaviors towards cyber security.
- Keeping a record of system integrity problems and incidents.
- Maintaining and updating the Information Technology Security Policies.

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

1.1.4.3. Security Infrastructure Team (SIT)

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

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

1.1.4.4. Security Operations Team (SOT)

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

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

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

1.1.4.5. BIT Executive Working Group on Cyber Security

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

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

The Group shall meet quarterly at a minimum.

Administrative-I/T Asset Protection-Background Checks

10.1.1. Overview

As a condition of employment, all current and prospective Bureau of Information and Telecommunications (BIT) employees and Information Technology contractors desiring to work for the State shall be screened thoroughly including verification of qualifications. Prospective employees and contractors will be notified that a background check will be done as part of the recruiting and selection process. These verifications must be performed at least once every five years.

10.1.2. Purpose

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

10.1.3. Scope

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

10.1.3.1. Scope Assumptions

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

10.1.3.2. Scope Constraints

Background checks are not performed for financial or credit information.

10.1.4. Policy

10.1.4.1. Background Checks

BIT requires all current and prospective BIT employees, State Technology contractors, and the South Dakota Public Broadcasting Engineering group who write or modify State of South Dakota-owned software, alter hardware, configure software of State-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo

Federal fingerprint-based background checks and to have these background checks repeated at least once every five years. Failure to comply with a federal background investigation may result in disciplinary action up to and including termination of employment or the rescinding of a conditional offer of employment. These background checks must be fingerprint-based and performed by the State with support from the State's law enforcement resources. Under provisions set forth in Title 28, Code of Federal Regulations (CFR), Section 50.12, the prospective employees and contractors will be provided written notification that their fingerprints will be used to check the criminal history records of the State and the Federal Bureau of Investigation (FBI). Identification records obtained from the FBI may be used solely for the purpose requested and may not be disseminated outside the receiving department, related agency, or other authorized entity. BIT will supply the fingerprint cards and the procedure that is to be used to process the fingerprint cards. Individuals should plan on the background check taking two to four weeks. The steps to process the background checks are found in procedures document ITSP 1010.1 Background Checks Procedures.

10.1.4.2. Disqualifying Criteria

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

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

10.1.4.3. Noncriminal Agency Coordinator (NAC)

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

10.1.4.4. Local Agency Security Officer (LASO)

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

10.1.4.5. Background Check Interpretation

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

10.1.4.6. Not Guilty Presumption

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

10.1.4.7. Background Check Information Challenge

An opportunity to challenge and discuss the disqualification due to information found in the criminal history records of the FBI will be provided to the applicant for five days, if requested. Due to the confidential nature of the criminal history records of the FBI and the restrictions on disclosure of the records, it may be discussed that the applicant was disqualified because of criminal history information; however, the specific FBI results may not be disclosed to the applicant, neither in writing nor verbally. Under provisions set forth in Title 28, CFR, Section 50.12, if the information on the record is used to disqualify an applicant, the official making the determination of suitability for licensing or employment shall provide the applicant the opportunity to complete, or challenge the accuracy of, the information contained in the FBI Identification record. The deciding official should not deny the license or employment based on the information in the record until the applicant has been afforded a reasonable time to correct or complete the information or has declined to do so.

10.1.4.8. Corrective Action

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

10.1.4.9. Training

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

10.1.4.10. Emailing Background Check Information

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

Administrative-I/T Asset Protection-Confidentiality

10.3.1. Overview

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

10.3.2. Purpose

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

10.3.3. Scope

This policy applies to BIT and technology contractors of the State. It includes the protection of sensitive data in addition to the work products built under State guidance. Individuals shall maintain confidentiality and data integrity of documents, records, configurations, programs, and files and understand that work products resulting from such efforts are the property of the State.

10.3.3.1. Scope Assumptions

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

10.3.3.2. Scope Constraints

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

10.3.4. Policy

10.3.4.1. Confidentiality Agreement

The individual must not, at any time, use or disclose any trade secrets or confidential information of the State to anyone, include agencies or contractors that have business with the State, without written permission from the BIT Commissioner, except as required to perform duties for the State. The individual agrees to adhere to all data processing and technology policies governing the use of the technology infrastructure of the State. The individual agrees that all developments made and works created by the individual in connection with the contractual agreement of the State shall be the sole and complete property of the State, and all copyrights and other proprietary interest, therein, shall belong to the State. Upon the request of the State to include the termination of the employment of the person, the individual will leave all reports, messages, programs, diagrams,

documentation, code, memoranda, notes, records, drawings, manuals, flow charts, and any other documents whether manual or electronic pertaining to the State, including all copies thereof, with BIT to include all data resources whether manual or electronic involving any trade secrets or confidential information of the State to include agencies or contractors that have business with the State.

Complying with Legal Obligations

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

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

10.3.4.2. Security Acknowledgement and Access

Once chosen, contractors must identify all individual contractors that will be participating in work for the State and begin participating after the work has begun. Contractors working with the State shall be required to sign the *Security Acknowledgement form* (<http://intranet.bit.sd.gov/forms/>). All BIT employees and contractors need to have a copy signed and filed. Contractor access to the technology infrastructure of the State is closely managed and limited. Contractors do not have the same degree of access nor privileges given to State employees. At the sole discretion of BIT, access for a contractor to the technology infrastructure of the State can be amended or terminated.

Server-Server Security-Server Maintenance and Administration

220.1.1. Overview

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

220.1.2. Purpose

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

220.1.3. Scope

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

220.1.3.1. Scope Assumptions

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

220.1.3.2. Scope Constraints

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

220.1.4. Policy

220.1.4.1. Visibility of Server and Framework Patching Status

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

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

230.67.1. Overview

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

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

230.67.2. Purpose

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

230.67.3. Scope

This policy covers all State IT resources managed by BIT.

230.67.3.1. Scope Assumptions

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

230.67.3.2. Scope Constraints

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

230.67.4. Policy

230.67.4.1. Individual Access Authorization

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

230.67.4.2. Least Privilege

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

230.67.4.3. Password Requirements

Must:

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

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

230.67.4.4. Individual Access Termination

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

230.67.4.5. Non-State Accounts

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

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

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

230.74.1. Overview

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

230.74.2. Purpose

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

230.74.3. Scope

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

Approval is obtained by using the [BIT Moving Live Data Request Form](#). Any data protected under Federal or State regulation or statute or industry standard is considered protected data. Protected data includes but is not limited to Personally Identifiable Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), Family Educational Rights and Privacy Act (FERPA), Criminal Justice Information System data (CJIS), The Federal Parent Locator Service (FPLS), and Payment Card Industry data (PCI). Protected production data that is

masked, deidentified or aggregated is no longer considered to be protected data. Information on what is legally protected data that is Personally Identifiable Information (PII) is found [here](#).

230.74.3.1. Scope Assumptions

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

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

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

230.74.3.2. Scope Constraints

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

230.74.4. Policy

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

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

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

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

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

The infrastructure scan report must include at least:

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

- Technical findings, including the exact details of what was found and their severity.

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

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

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

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

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

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

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

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

230.74.4.2. Purging of Data

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

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

230.74.4.3. Compliance

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

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

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

Data Center General-Security Impacts-Data Classification

230.75.1. Overview

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

230.75.2. Purpose

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

230.75.3. Scope

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

230.75.3.1. Scope Assumptions

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

230.75.3.2. Scope Constraints

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

230.75.4. Policy

230.75.4.1. Data Classification System

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

Data classification is based on three objectives:

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

There are four risks associated with each objective:

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

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

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

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

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

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

230.75.4.2. Classification of Data Produced under Contract

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

230.75.4.3. Data Classification Responsibilities

It is the data owner's responsibility to:

- Choose a systematic decision process to classify the data.
- Document the classification.

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

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

It is BIT's responsibility to:

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

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

230.76.1. Overview

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

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

230.76.2. Purpose

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

230.76.3. Scope

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

230.76.3.1. Scope Assumptions

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

230.76.3.2. Scope Constraints

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

230.76.4. Policy

230.76.4.1. Usage of Multi-Factor Authentication (MFA)

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

230.76.4.2. MFA Tokens

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

Mobile device authentication is the preferred method of secondary authentication.

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

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

230.77.1. Overview

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

230.77.2. Purpose

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

230.77.3. Scope

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

230.77.3.1. Scope Assumptions

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

230.77.3.2. Scope Constraints

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

230.77.4. Policy

230.77.4.1. Sanitization of Media in a Contractor's Control

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

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

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

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

These are the media sanitization requirements:

Low confidentiality status:

Purge

Moderate confidentiality status:

Media is not reused- Destroy

Media is reused- Purge

High confidentiality status:

Destroy

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

Following sanitization, a Certificate of Media Sanitization should be completed for each piece of media that has

been sanitized, the certificate can be found on this [webpage](#). This certificate must be sent to the State Contact who will pass it on to Data Center Director.

Development-Application Security-Security Assessments

401.3.1. Overview

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

401.3.2. Purpose

The purpose of this policy is to ensure applications, systems, or websites developed by BIT, contractors, or by any third-party must pass a security assessment prior to being accepted into production.

401.3.3. Scope

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

401.3.3.1. Scope Assumptions

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

401.3.3.2. Scope Constraints

This policy does not apply to mainframe or desktop applications.

401.3.4. Policy

401.3.4.1. Security Assessments

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

TERMS

Abstraction Technologies

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

Access Attempts

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

Accreditation (also referred to as Vulnerability Assessment)

Scanning of a system looking for security vulnerabilities.

Accreditation Boundary

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

ADABAS

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

Ad hoc Networking (WANET or MANET)

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

Adverse Event

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

Agency

An association, authority, board, commission, committee, council, department, division, task force or office within the

Executive Branch of State government. Includes the staff of that individual department.

Application

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

Application Scans

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

Application Server

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

Authorized Developer

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

Authorized Persons

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

Back Door

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

Blocked mail

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

Bluetooth

The wireless communication technology that conforms to the Bluetooth computing and telecommunications industry specification. This specification describes how mobile phone, landline phones, computers, and mobile devices

can easily exchange information by using a short-range wireless connection.

Browser

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

Brute Force Attack

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

Bureau of Information and Telecommunications

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

Business Associate (BA)

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

Business Associate Agreement (BAA)

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

Chief Information Security Officer (CISO)

BIT senior executive charged with implementing the information technology security programs for the State.

Circuit

A theoretical structure simulating electrical and data paths.

Closed Source

Proprietary software where the state does not hold the copyright.

Cloud Service

Services made available to users on demand via the internet from a cloud computing provider's servers as

opposed to being provided by the State's on-premise servers. See also Infrastructure as a Service and Platform as a Service.

Code

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

Commercial off the Shelf Software

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

Communication Protocols

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

Connectivity

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

Content Filtering

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

Contractor

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

Covered Entity

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

Cracking passwords

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

Credentials

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

- RACF
- NATURAL

Data and Information Types

Data is measured, collected, reported, and analyzed. Data

as a general concept refers to the fact that some existing information or knowledge is represented or coded in some form suitable for better usage or processing. Pieces of data are individual pieces of information.

Data and Information Types: Confidential

Any data or information, other than trade secrets, that is materially sensitive in nature, whether manual or electronic, which is valuable and not generally known to the public. Identified here, are few examples, this list is not inclusive. Personally identifiable information which is not in the public domain, and if improperly disclosed could be used to steal the identity of an individual, violate the right of an individual to privacy or otherwise harm the individual or business to include, but is not limited to social security numbers, tax payer identification numbers, and any other department determined data that is not in the public domain or intended for release to the public domain and if improperly disclosed might:

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

Data and Information Types: Return Information

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

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

- Telephone numbers
- Social Security Numbers
- Bank account numbers
- Date and place of birth
- Mother's maiden name
- Biometric data (e.g., height, weight, eye color, fingerprints)
- Any combination of the preceding.

Returns are forms submitted on paper or electronically with return information to the IRS by, or on behalf of, or with respect to any person or entity. Examples can include Forms 1040, 941, 1120 and other informational forms, such as 1099 or W-2.

Data and Information Types: Sensitive

Any information and data not available to the public via the [Freedom of Information Act](#) or the [State Open Records Laws SDCL 1-27](#).

Data and Information Types: Trade Secret

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

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

See [SDCL 1-27-30](#)

Database

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

Data Breach

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

Data Mining

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

Dataset

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

DDN Intranet

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

De-Militarized Zone (DMZ)

A perimeter network that contains external network facing services. Applications needing access from the public Internet are located in the DMZ.

Digital Dakota Network (DDN)

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

Directory

The service that identifies all resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, computers, and peripheral devices such as printers. The directory service allows a user on a network to access any resource without knowing where or how it is physically connected.

Distributed Denial of Service (DDOS)

A botnet is a series of computers compromised. A DDOS attack utilizes 1 or more botnets to target a single computer or website. The massive amount of botnet traffic overloads the recipient with more data than it can handle, resulting in service delays or outages. The counts indicate the number of attacks targeting the Board of Regents, K12 public schools and State government.

Domain Name

A name owned by a person or organization and consisting of an alphabetical or alphanumeric sequence followed by a suffix: used as an Internet address to identify the location of particular Web pages.

Dynamic Naming System (DNS)

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

Easter Egg

A secret message buried in an application.

Employee

Anyone employed directly by the State of South Dakota or employed by any third-party company (contractor or

subcontractor) that has a contract to provide work for a State government agency. Contractors and Employees are treated identically throughout the Information Technology Security Policy.

End User Data

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

External Network

Any network that resides outside of the established security perimeter.

Extranet

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

Fail Over

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

Federal Tax Information (FTI)

FTI is any return or return information and data received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information and data. Even if identifiers are deleted the data is still considered FTI. Information and data provided directly by the taxpayer or third parties is not FTI. If FTI is replaced with the same data provided by the taxpayer or third party, it is no longer considered FTI. For additional information see **Data and Information Types: Return Information.**

File Transfer Protocol (FTP)

A standard network protocol used to transfer data files between one workstation network and another.

Firewall

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

Hackers

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

Hot Spot

A physical location where people may obtain Internet access. Hypervisor is a program that is running one or more virtual machines on a single physical server. See also virtualization.

Identity Theft

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

Inbound Traffic

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

Individually Identifiable Health Information (Also known as Personal or Personally Identifiable Health Information)

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

Information system

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

Infrastructure

The technology (hardware and software) that comprise the computer network, phone network, and connections to the Internet including the computer and storage environments.

Infrastructure-as-a-Service

The capability provided to the state to provision, process, and store networks and other fundamental deployments and run arbitrary software, which can include operating systems and applications. The state does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components, for example, host firewalls.

Internet of Things (IoT)

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

IP Address

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

Load Balancing

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

MAC Address

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

Malicious Phishing

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

Malicious Software

A program that gives a hacker control of your computer.

Malware

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

Metadata

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

Mobile Applications

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

Mobile Device

A portable, wireless computing device that is small enough to be used while held in the hand.

Mobile Wi-Fi

A wireless router that acts as a mobile wireless network outbound spot.

NATURAL

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

Network

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

Non-Public Data

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

Non-State Account (NS)

An account that provides access to State IT resources used by a non-State employee.

On Premise

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

Open Source

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

Operating System

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

Outbound Traffic

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

Payment Card Industry (PCI)

Credit card security specifications created by the credit card industry.

Peripherals

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

Personally Identifiable Information (PII)

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

Platform

The type of computer system the network is running on. The state has three; the Windows based platform, the mainframe system, and the AS 400 system.

Platform-as-a-Service (PaaS)

The capability provided to the state to deploy onto the cloud infrastructure state-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The state does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Portable Device

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

Portable storage device

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

Power over Ethernet (POE) switches

A network switch that has Power over Ethernet injection built in.

Presentation Layers

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

Processor

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

Production Environment

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

Program

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

Protected Data

Data protected by any law, regulation, industry standard,

or has been designated as sensitive by the State or Federal government.

Protected Health Information (PHI)

Individually identifiable health information that is:

- Transmitted by electronic media.
- Maintained in electronic media.
- Transmitted or maintained in any other form or medium.
- PHI excludes individually identifiable health information in:
 - Education records covered by the Family Educational Rights and Privacy Act.
 - Employment records held by a covered entity in its role as employer.

PHI includes but is not limited to the patient's name, address, doctor, clinic, diagnosis, and prescribed medication. See **Data and Information Types: Protected Health Information** for additional information.

Reaccreditation

The periodic rescanning of a system looking for security vulnerabilities.

Relative Pathing

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

Remote Access Device (RAD)

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

Resource Access Control Facility (RACF)

An IBM software product. It is a security system that provides access control and auditing functionality for the z/OS and z/VM operating systems.

Rogue Access Point

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

Router

A networking device that forwards data packets between computer networks.

Sanitization

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

Script

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

Security Activity

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

Security Incident

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

Security Infrastructure Team (SIT)

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

Security Operations Team (SOT)

The BIT SOT meets daily to review any cyber security findings or issues with the State Infrastructure within the previous day.

Server

A computer that contains a program that awaits and fulfills requests from other programs in the same or other computers. A given application in a computer may function as a source of requests for services from other programs and also as a server of requests from to other programs.

Service Level Agreement

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

SIM card

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

Social engineering

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

Software-as-a-Service (SaaS)

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

Software Development Life Cycle (SDLC)

A software development methodology used by BIT.

Software patches

Changes made to applications to fix security vulnerabilities or impaired functionality.

Spoofing

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

State

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

State Contact

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

State Data

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

State Proprietary Information

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

Statement of Work

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

Structure Query Language

A computer language that is used to manage data, where

the data is presented as a set of related tables, and to make queries of a database.

System

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

Test Environment

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

Time Bomb

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

Trojan Horse

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

User Identification (UID)

A user, identifier, or account utilized for access control to specify which technical assets and resources an individual or entity can access. Examples are:

- USERID
- A User ID
- SD Domain Account

Virtual Private Network (VPN)

A method to encrypt data that is sent or received over the public Internet.

Virtualization

The creation of a virtual version of something, such as an operating system, a server, a storage device or network resources. By allowing multiple virtual versions of something on the same physical server more efficient use is made of network resources.

Web Probing

An intelligence gathering effort to gather background information and to identify configuration files and directories of servers providing web content.

Web Server

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

Web Server attacks

Attacks against the servers that connect the state network to the Internet as well as servers that host (store and run) websites. These attacks can be to access data that is not meant to be accessible through the websites via direct

probes and software injections from malicious hosts. They can also be meant to prevent users from accessing the websites or the servers. Incidents is the number of successful compromises and Hack Scans are the number of infiltration attempts.

Wi-Fi

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

Wireless Access Point (WAP)

A networking hardware device that allows a Wi-Fi device to connect to a wired network.

Wiring closet

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

Workstations

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

Worm

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

DDN

Digital Dakota Network

DDOS

Distributed Denial of Service

DHCP

Dynamic Host Configuration Protocol

DMZ

De-Militarized Zone

DNS

Dynamic Naming System

DOH

South Dakota Department of Health

DSN

Data Source Name

DSS

South Dakota Department of Social Services

EAR

Export Administration Regulations

FERPA

Family Educational Rights and Privacy Act

FPLS

Federal Parent Locator System

FTI

Federal Tax Information

FTP

File Transfer Protocol

GLBA

Gramm-Leach Bliley/ Financial Services Modernization Act

HIPAA

Health Information Portability and Accountability Act

IaaS

Infrastructure as a Service

IEEE

Institute of Electrical and Electronics Engineers

IoT

Internet of Things

IPv4

Internet Protocol version 4

IPv6

Internet Protocol version 6

ACRONYMS

ACL

Access Control List

ADABAS

Adaptable Data Base System

BA

Business Associate

BAA

Business Associate Agreement

BHR

South Dakota Bureau of Human Resources

BIT

Bureau of Information & Telecommunications

CISO

Chief Information Security Officer

COTS

Commercial off the Shelf Software

DBMS

Database Management System

IRS

Internal Revenue Service

ITAR

International Traffic in Arms Regulations

MANET

Mobile Ad Hoc Network

MIFI

Mobile Wi-Fi

MMIS

Medicaid Management Information System

MOU

Memorandum of Understanding

NIST

National Institute of Standards and Technology

NS

Non-State Account

OWASP

Open Web Application Security Project

PaaS

Platform-as-a-Service

PCI

Payment Card Industry

PII

Personally Identifiable Information

PHI

Protected Health Information

RACF

Resource Access Control Facility

RAD

Remote Access Device

RADIUS

Remote Authentication Dial-In User Service

SaaS

Software-as-a-Service

SDLC

Software Development Life Cycle

SLA

Service Level Agreement

SNMP

Simple Network Management Protocol

SOC

Security Operations Center

SOT

Security Operations Team

SOW

Statement of Work

SSID

Service Set Identifier

SQL

Structure Query Language

TACACS+

Terminal Access Controller Access-Control System Plus

UAT

User Assurance Testing

UID

User Identification

VOIP

Voice Over Internet Protocol

VPN

Virtual Private Network

WAN

Wide Area Network

WANET

Wireless Ad Hoc Network

WAP

Wireless Access Point