North Dakota
Information Technology Department

SOC3-Service Organization Control Report

ITD

For the Period of July 1st, 2017 through June 30th, 2018

Uriah Burchinal
Author
Sean Wiese
CISO

4201 Normandy Street
Bismarck, ND 58503
(701) 328-3190

Table of Contents

---

[1] North Dakota Century Code (N.D.C.C. 44-04-18) *Access to public records – Electronically stored information* is the primary legislative statute in North Dakota law that directs public accessibility to public records.

[2] The North Dakota Constitution Article XI Section 6 expresses a demand that all records of public or governmental entities shall be accessible to the public unless otherwise prohibited by lawful statute.

[3] North Dakota Century Code (N.D.C.C. 44-04-27) *Computer passwords and security information – Confidential* provides for confidentiality and restricts public access to security related content of computer systems.

[4] North Dakota Century Code (N.D.C.C. 12.1-13-01) *Disclosure of confidential information provided to government* describes the penalty as a class C felony, "if in knowing violation of a statutory duty imposed on him as a public servant, he discloses any confidential information which he has acquired as a public servant."

Independent Auditor's Report

STATE AUDITOR
Joshua C. Gallion

Phone: 701-328-2241
www.nd.gov/auditor

STATE OF NORTH DAKOTA
OFFICE OF THE STATE AUDITOR
STATE CAPITOL
600 E. BOULEVARD AVENUE – DEPT 117
BISMARCK, NORTH DAKOTA 58505

Independent Service Auditor's Report

The Honorable Doug Burgum, Governor
Members of the North Dakota Legislative Assembly
Shawn Riley, Chief Information Officer

Scope

We have examined the Information Technology Department's (ITD) Description of Service Organization's System 2018 for the period July 1, 2017 to June 30, 2018, based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (AICPA, Description of Controls)*, and the suitability of the design and operating effectiveness of controls stated in the description, to provide reasonable assurance that ITD's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.*

The ITD uses Multi-State Information Sharing & Analysis Center (MS-ISAC) for intrusion detection services. The controls related to this are identified in ITD's Description of System and Controls-2018 as SCA102, SCA106 and SCA108. Our examination did not include the services provided by the subservice organization, and we have not evaluated the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at ITD, to achieve ITD's service commitments and system requirements based on the applicable trust services criteria. The description presents ITD's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of ITD's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

The ITD is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the ITD's service commitments and system requirements were achieved. The ITD has provided the accompanying assertion titled "Assertion of ITD Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls state therein. The ITD is also responsible preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and the assertion; providing the services covered by the description, selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls state therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls state in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of our tests are presented in the section of our report titled "Description of Tests of Controls and Results Thereof."

Opinion

In our opinion, in all material respects,

a) The description fairly presents the ITD's Description of Service Organization's System 2018 was designed and implemented throughout the period July 1, 2017 to June 30, 2018, in accordance with the description criteria.

b) the controls stated in the description were suitably designed throughout the period July 1, 2017 to June 30, 2018, to provide reasonable assurance that the ITD's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of ITD's controls throughout that period.

c) The controls stated in the description operated effectively throughout the period July 1, 2017 to June 30, 2018, to provide reasonable assurance that ITD's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of ITD's controls operated effectively throughout that period.

Restricted Use

This report including the description of tests of controls and results thereof is intended solely for the information and use of the ITD; user entities of the ITD during some or all of the period July 1, 2017 to June 30, 2018, business partners of ITD subject to risks arising from interactions with ITD, practitioners providing services to such user entities and business partners, prospective user

entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the services provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organizations' s services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

/S/

Joshua C. Gallion
State Auditor

Bismarck, North Dakota

October 5, 2018

ITD Management Assertion

Assertion by Management regarding State of North Dakota Information Technology Dept. (ITD) service organization operations throughout the period July 1, 2017 to June 30, 2018

We have prepared the enclosed description of ITD's operation as a service organization. This service organization system description provides an explanation of the controls relevant to Security, Availability, Processing Integrity, and Confidentiality during some or all the period July 1, 2017 to June 30, 2018.

We confirm, to the best of our knowledge and belief, that

a. the description fairly presents ITD's service organization system made available to state entities as stipulated under North Dakota Century Code (NDCC) 54-59. The criteria we used in making this assertion were that the description presents our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of state entity users of ITD systems. Additionally, this system description does not omit or distort information relevant to the scope of ITD's operation as a service organization and it is prepared to meet the common needs of a broad range of state entity users of the system and the independent auditors of those entities.
b. the controls stated in the description were suitably designed throughout the period July 1, 2017 to June 30, 2018, to provide reasonable assurance that ITD's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.
c. the controls stated in the description operated effectively throughout the period July 1, 2017 to June 30, 2018, to provide reasonable assurance that ITD's service commitments and system requirements were achieved based on the applicable trusted services criteria.

Description of Service Organization's System

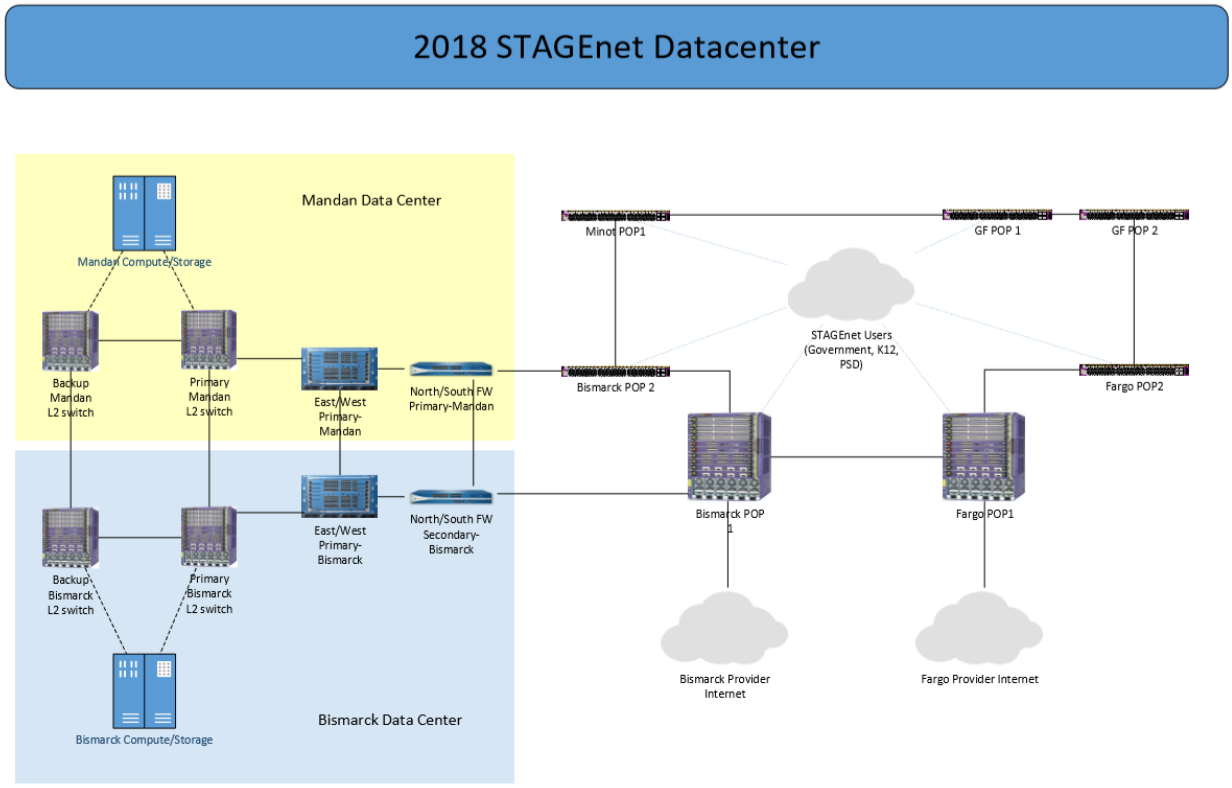
Scope and Purpose

The Information Technology Department (ITD) is located in Bismarck, North Dakota. Pursuant to North Dakota Century Code (NDCC) chapter 54-59, ITD is managed by the Chief Information Officer (CIO) who reports directly to the Governor. This document describes the control structure of ITD as it pertains to hosted services. The system is defined as the network, hardware, operating systems and middleware used by ITD in order to provide services to state agencies, including institutions under the control of the State Board of Higher Education, counties, cities, and school districts hereafter referred to as user organizations. Professional services work done by ITD on the behalf of an agency such as application development and desktop support are not a hosted service and therefore excluded. ITD entities such as the Center for Distance Education and EdTech do not function as part of the service organization and are therefore excluded.

Overview of Services Provided

ITD is responsible for providing and maintaining the underlying IT infrastructure that provides the base or foundation for the state's information technology systems. Infrastructure includes (1) hosting computer systems or hosting middleware; and (2) network services that accommodate the data, voice, video, and multimedia traffic over a statewide backbone to support the missions of government and education.

1. **Hosting**



Databases

ITD operates dedicated equipment necessary to host user organization database applications. ITD's database hosting catalog includes the following:

Full Database Hosting and Support

- Oracle
  A relational database management system from Oracle Corporation. ITD hosts both the Enterprise and Standard Editions. The enterprise version is built on the Oracle Real Application Cluster (RAC).

- Microsoft SQL Server
  A relational database management system from Microsoft. ITD's Microsoft SQL environment is in a highly available cluster design.
- IBM DB2
  A relational database management system from IBM.
- SoftwareAG Adabas
  A non-relational database management system from Software AG Inc. Adabas is a partner product to the NATURAL programming language.
- IBM VSAM
  An older database technology from IBM.

Limited Database Support

- MySQL
  An open source relational database management system that relies on SQL for processing data

Datacenter Space Rental

Datacenter Space Rental provides a managed facility for customers to locate servers and related computer equipment over which they retain ownership and operational authority.

Despite the remarkable transformation of the state IT enterprise over the past decade, states can be even more responsive and more capable of delivering services and protecting the states' data systems and information. That capacity rests critically on the task of re-engineering business processes and eliminating redundancies whenever possible. State CIOs have seized on the potential for galvanizing the state IT enterprise to produce better results and reduce costs by engaging in the consolidation of state data centers for optimizing the physical infrastructure and to streamline business functions

Disk Storage & Backup

ITD offers several levels of storage services, including automated backup services.

Tiered Solutions

- Basic Storage
  Designed for non-critical data that does not require high performance or high availability.
- File Share Storage
  Designed for critical documents, images, other non-transactional data that requires high performance and high availability.
- Premium Storage
  Designed for critical database and transactional data that requires high performance and high availability.

Backup/Recovery

Tapeless backup (disk-based) and tape storage is provided for all disk storage services.

Replication

Replication creates a real-time copy of data in both the primary and secondary datacenters and significantly improves recovery time in the event of a disaster.

File & Print

File and Print services allow people to store, secure, share, and print files over the network.

A file server's primary purpose is to provide a location for shared file access, i.e. shared storage of computer files (such as documents, sound files, photographs, movies, images, databases, etc.) that

can be accessed by workstations attached to the network. It is designed primarily to enable the rapid storage and retrieval of data and share this information with others.

A print server's primary purpose is to provide print job management to shared printers.

Hosting Platforms

ITD provides hosting services for a number of hardware platforms. ITD's hardware hosting catalog includes the following:

Intel Servers

ITD hosts a variety of application servers in a stand-alone, clustered and virtualized environment. All of these operate in our secure and environmentally controlled data center facility.

ITD uses a blade infrastructure that helps to lower cooling and electrical costs and reduces space requirements. We support both Linux and Windows operating systems with over 94% of servers running in a virtualized system.

Midrange (IBM iSeries) AS/400

ITD provides hosting services (including computer processing and electronic storage of data) for the IBM iSeries platform. The IBM iSeries, formerly known as the AS/400, is a mid-range server designed for small businesses and departments in large enterprises.

IBM Enterprise Server (Mainframe)

A mainframe is a high-performance computer used for large-scale computing purposes that require greater availability and security than a smaller-scale machine can offer. ITD uses the IBM Z10 system.

The mainframe is the classic centralized computing system. Even though the mainframe platform is not strategic to new application design, it remains a fully-supported modern platform for legacy applications.

Web Server & Middleware Platforms

ITD has several hosted solutions for both websites and web applications. ITD's web service hosting catalog includes the following:

Websphere

IBM's Web Application server. ITD provides the equipment necessary to host agencies WebSphere applications. The cost is tiered based on the size and complexity of the application

.NET

Microsoft's web application server; runs on the Windows Server platform.

IIS (Internet Information Services)

Microsoft's older web server; runs on the Windows Server platform.

Apache

An open source alternative for web servers; uses ITD's Linux infrastructure

2. Network Services

Local Area Network

ITD provides managed Local Area Network (LAN) service for a building or campus environment enabling data communication among local computing and printing resources within a user organization.

This service is typically only available to customers within the state government user space. Solutions may vary depending on location, however, they typically include service to the endpoint "jack in the wall" with connection capacities ranging from 10mb, 100mb, and 1g.

Wide Area Network

The statewide WAN provides gateway services to the public internet and functions as a private fault-tolerant network allowing for interconnectivity within STAGEnet. ITD manages the statewide WAN for all user organizations. Connection to the statewide WAN can be achieved by a variety of methods to meet the technical and financial requirements of a facility.

Major Metro Area Network presently exists in Bismarck and Fargo. These solutions provide for a resilient fault tolerant core network that provides dual redundant fiber paths to key locations. The MAN provided redundant connections to the WAN allow for sites to connect to the network with single or dual fiber solutions.

Fiber connections are available in most locations. Fees vary depending on location and construction costs may be required. The fiber connections can be connected to a variety of aggregation points including the WAN, MAN, or other aggregation points in a community.

Ethernet Transport Service (ETS) solutions exist in most locations across the state. This service starts and 5Mb and can scale to 1g and beyond.

Broadband solutions exist in many communities across the state. The solutions can be DSL or cable solutions with capabilities that vary in each community. Broadband solutions are connected to aggregation points on the statewide WAN and secured via a site-to-site VPN.

Custom Solutions are available in a variety of options to any location.

Wireless Network

ITD provides a managed and monitored 802.11abgn wireless network solution that can be installed in user organization locations.

This service is customized depending on customer requirements, and it can include public access and/or authenticated secured connections. Wireless service is typically deployed with both public access and secure authenticated access to STAGEnet.

STAGEnet-Guest; unencrypted access to the Internet using a real external IP address. Service is available authentication to any customer with a compatible wireless device.

STAGEnet-Member; authenticated and encrypted access to the internal network without the use of a Virtual Private Network (VPN).

Addressing Organizational Risk

Relevant Aspects of the Overall Control Environment

1. **Control Environment**

   ITD's control environment is developed around the ITD Cybersecurity Framework. This framework is based on the NIST Framework Core and addresses protecting systems by using the functions to identify, protect, detect, respond, and recover. Following the ITD Cybersecurity framework, ITD uses the NIST 800-53 r4 control set to achieve the framework outcomes as well as adhering to regulatory mandates.

2. **Control Activities**

   ITD's organizational structure provides an overall base for planning, directing and controlling operations and is the responsibility of executive management. The CISO is ultimately responsible for the security controls with the assistance of the executive management team.

3. **Risk Assessment**

   As part of ITD's Risk Management Plan, a formal process has been implemented to assess the threats and vulnerabilities that give rise to an inherent risk of the overall organization. Risks Identified by assessments are reviewed and addressed in order to close any control gaps and reach a residual risk profile that is acceptable.

4. **Monitoring**

   Monitoring of controls occurs through ongoing audits and periodically required federal responses to identified weakness. ITD also performs annual security assessments that includes a controls gap analysis.

5. **Information and Communications**

   The hosted services provided by ITD utilizes a network of hardware, systems software, and telecommunications systems. Facilitated through two (2) data centers in Bismarck, North Dakota and Mandan, North Dakota. Communications between user organizations and these data centers occur over a statewide communications network referred to as STAGEnet.

   Corporate-wide controls are communicated through the ITD Cybersecurity Framework and ITD policies that accompany them as well as statewide standards developed by the Enterprise Architecture Team.

Control Objectives and Description of controls

The following is a description of the internal controls that are generally considered to be part of ITD's control environment. The overall control structure of ITD consists of specific control activities that can be related to twelve (12) major areas. These areas are defined by the Trust Services Criteria.

- Organization and Management
  Criteria are relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units

- Communication and Information
  How the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

- Risk Assessment
  How the organization identifies potential risks that would affect the entity's ability to achieve its objectives.

- Monitoring of controls
  Criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

- Control Activities
  Addresses activities help ensure that risk responses that address and mitigate risks are carried out.

- Logical and physical access controls
  Defines how ITD restricts logical and physical access to systems, provides and removes that access, and prevents unauthorized access.

- System operations
  Addresses how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations.

- Change management
  The criteria relevant to how the organization identifies the need for changes to the system make the changes following a controlled change management process and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement

- Risk Mitigation
  Addresses the how the organization analyzes identified risks and develops responses to those risks including the design and implementation of controls and other risk-mitigating actions and conducts ongoing monitoring of risks and the risk management process.

- Confidentiality
  Confidentiality is ensuring that information is accessible only to those authorized to have access, regardless of where the information is stored or how it is accessed.

- Availability
  Availability is ensuring that authorized users have access to information and associated assets when required.

- Integrity
- Data Integrity is defined as safeguarding the accuracy and completeness of information and processing methods from intentional, unauthorized, or accidental changes.

The primary objective of the control structure is the establishment of an appropriately controlled environment to develop and implement policies and procedures to achieve internal control objectives that are aligned with the ITD Cybersecurity Framework.

1. Organization and Management

ITD has adopted the following six guiding principles that provide the foundation for the organization and set standards for how employees and managers are expected to act and interact:

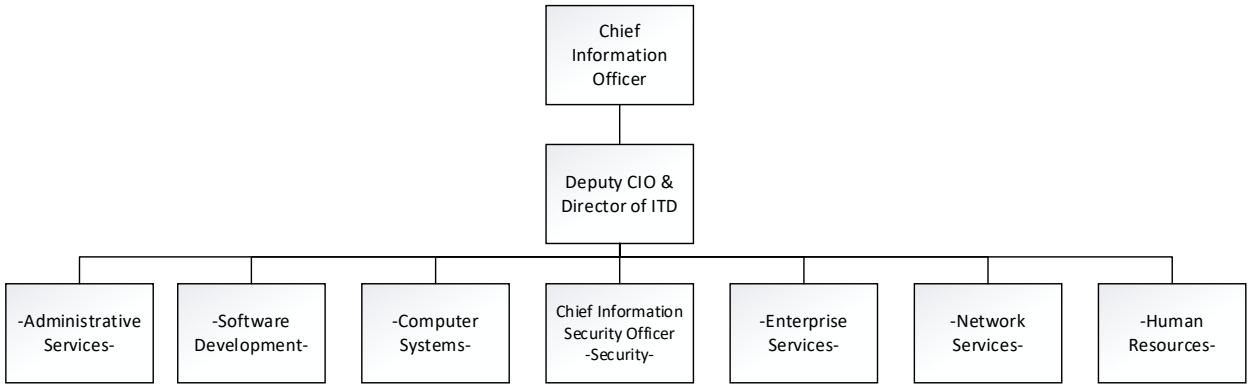
1. Respect - we treat everyone with dignity and respect.
2. Teamwork - we recognize ITD's success depends on partnerships and collaboration.
3. Achievement - we develop quality solutions that best address the needs of our state. We are committed to delivering results on time and on budget.
4. Integrity - we build long-term, lasting relationships through mutual trust. We value open, honest, two-way communication.
5. Leadership - we encourage initiative and creativity. We are committed to investing in knowledge and expertise.
6. Service - we hold ourselves accountable for a positive customer experience.

The ITD exists for the purpose of leading user organizations in discovering, assessing, and implementing information technologies. ITD is committed to better understanding user organization needs and in assisting in the implementation of the proper technical solution to accomplish those needs. ITD is organized to provide a broad range of technologies including mainframe and desktop computing, local

and wide area networks, voice and data technologies, web, client-server and mainframe software development, video conferencing, and emerging technologies. This is accomplished by investing in the development of highly skilled employees along with contracting outside vendors who maintain a level of expertise that is not available in-house or is limited due to the demands for a particular service.

ITD's mission is to provide leadership and knowledge to assist our customers in achieving their mission through the innovative use of information technology.

ITD has defined a hierarchical organizational structure with each division responsible for the security, availability, processing integrity, confidentiality, etc. of their respective areas. ITD has also implemented a Chief Information Security Officer, which has the authority over the Security Division and subsequent security program, as well as the responsibility to collaborate across organizational lines to ensure security, integrity, etc. of the State's computing resources.



The seven divisions outlined above include over 300 employees providing the following services to ITD's customers:

Administrative Services - Provide accounting functions, assist customers with billing and oversee strategic initiatives related to budgeting and records management.

Software Development – Develop and maintain computerized applications and provide related consulting services. Responsibilities include design, development, and support of customized software applications that operate on a variety of computer platforms and database management systems. Staff is on-call to support production applications 24 hours per day. This division also has a staff of project managers available for assisting agencies on large IT projects.

Computer Systems - Provide technical computing infrastructure and the expert skills required to host the state's applications, including clustered servers, redundant storage, multi-path networks, environmentally controlled data centers with generator backup and uninterpretable power supply systems. Provide round-the-clock job processing and routine system procedures required during the non-business hours.

Enterprise Services – Coordinate ITD's people, process, and technology in a way that promotes customer-centric services. Foster customer relations and align ITD's services with customer expectations. The Service Desk is the heart of this division. This division also contains enterprise program administrators that assist user organizations with setting direction and maximizing the value of technology investments.

Network Services – Oversee the statewide network providing broadband connectivity, internet access, video conferencing and other networking services to user organizations, local government, higher education, and K-12 schools. Ensure the reliability and security of the statewide network from the threats

of viruses, worms, and hackers. The division is on-call 24/7 to ensure information flows freely to the right people, at the right place, at the right time.

Human Resources - Provide a variety of services to ITD, including the following: recruitment, selection, and retention of highly qualified employees; strategic planning assistance; policy implementation; job classifications maintenance; employee/manager relations; benefits; compensation; legal compliance; training and development; and risk management & workplace safety.

Security - Is tasked with designing, developing, and monitoring controls. The implementation, operation, and maintenance of controls is the responsibility of the respective divisions that oversee the systems and processes the controls apply to. Approval of system controls is done is performed by the executive management team and is coordinated by the CISO.

ITD has established workforce conduct standards, background screening procedures, and enforcement measures by way of information policy and procedures.

The Cybersecurity Framework includes a Statement of Management Commitment and provides an overview of the roles and responsibilities for various officials and organizational offices involved in cybersecurity.

2. Communications and Information

The design and the operation of systems and its boundaries are documented. Detailed architectural documents are maintained in an internal Wiki. Access to the Wiki is limited to ITD Architects and Executive management. High-level design documents provided to internal and external users of the system are available and provided as needed. Ongoing operational documentation is maintained by system administrators responsible for system operation.

Security commitments are communicated to internal users through policy and annual awareness training. Service level agreements, business level agreements, and contracts all communicate levels of responsibility for all parties whose role affect system operations. Information needed for a user to carry out their responsibilities are provided.

Failures, incidents, concerns, and other complaints are submitted through a call or email to the ITD service desk. These items have a ticket opened and are documented and resolved within timeframes designated in the service level agreement

System changes are communicated through the change management process.

ITD provides services to a variety of customers and ensures open and timely communication through the following methods:

- An intranet site that summarizes significant IT events and changes occurring during the month.
- E-Mail messages to communicate time-sensitive messages and information.
- Quarterly agency newsletter titled “Information Link”.
- Quarterly IT Directional meetings to inform entities on current initiatives and issues.
- Meetings with key customers on a recurring basis to gather information about current and future projects.

ITD also publishes an annual report which includes: major accomplishments, future initiatives, ITD's performance measures, and ITD's service rates which are compared with costs charged by similar organizations. ITD distributes the report to the Legislative Information Technology Committee, Legislative Audit and Fiscal Review Committee, and the Statewide Information Technology Advisory Committee. The report is also available on ITD's website under "Publications".

Procedures have been implemented for sharing information with third-parties, which is accomplished through Information Exchange Agreements (IEA).

3. Risk Assessment

ITD has placed into operation a risk assessment process to identify and manage risks that could affect the ability to provide reliable transaction processing for user organizations. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks. The agenda for each quarterly management meeting includes a discussion of these matters. This process has identified risks resulting from the nature of the services ITD provides, and management has implemented various measures to manage those risks.

ITD identifies potential threats through a yearly security assessment of the control structure through the use of the Cyber Security Evaluation Tool provided by the Department of Homeland Security. The security assessment is run against NIST 800-53 moderate controls to identify potential risk. ITD also commissions a penetration test every two (2) years. The outcome of the security evaluation and penetration test is analyzed, and mitigation and remediation strategies are put in place. Policies, standards, and procedures are evaluated based on the risk mitigation plan to implement achieve the risk mitigation strategy.

4. Monitoring of Controls

The effectiveness of controls is evaluated against requirements on an ongoing basis. The controls in place are audited against federally on average every three years. A Service Organization Controls audit is performed by the State Auditor's Office every two (2) Years to assess the controls in place. Federally required audits for specific agencies include ITD controls for hosted systems. These audits occur approximately every three years. ITD is required along with the agency to submit quarterly responses in the form of Corrective Action Plans and POA&Ms.

5. Control Activities

ITD's CISO along with the executive management team is responsible for the overall control environment at ITD and for formulating, implementing, and monitoring the controls in place in the various divisions of ITD. The management team consists of the CIO, Deputy CIO, CISO, and Division Directors.

6. Logical and Physical Access Controls

ITD has implemented Active Directory as the mechanism for logical access to provide an identification, authentication and authorization mechanism. Active Directory is used to restrict access to both the system and components thereby preventing unauthorized access. All users are both identified and authenticated when accessing the system. In addition, ITD utilizes the following identity management repositories:

- Tivoli Directory Server (LDAP for external users and FTP users)
- RACF (mainframe users)
- AS/400
- Oracle
- SQL (for applications that cannot use AD Groups)

ITD has established a single forest architecture for its Active Directory. All user organizations networks using Active Directory coordinate their installation and maintenance activities with ITD to ensure that all networked Active Directory computers are members of the State forest, NDGOV. Organizational Units (OU) are used to create grouping of computers, users, and groups to provide for the delegation of administrative control of the agency network. Each agency has an OU within the Active Directory to allow

for the administration of the agency network. The agency OU contains all user accounts for the agency, all Group definitions, and memberships for the agency and all computer accounts for the agency.

The Enterprise and Domain Administrator role/responsibilities reside with ITD. The Domain Administrator initially establishes each agency's OU, along with the first user, computer, and group. This first group, called [agency name]-ou-admins, is delegated full control over the OU. From that point on the administration of the OU is the responsibility of the agency and ownership of the OU and its Group Policy is given to the Agency Administrator group. ITD will only grant access to information based upon authorization requests from Agency IT Coordinators.

By default, the Enterprise and Domain Administrators have full administrative rights to all computers within the Active Directory Forest. The OU administrators can limit the rights of the Enterprise and Domain Administrators to the domain controllers within the active directory forest. However, the Enterprise Administrator does retain the right to remove these restrictions. This is a fail-safe feature to allow the Enterprise Administrator the ability to repair any damage to the Active Directory. While this is a necessary enterprise feature and requires modification to the OU security, all such access by the Enterprise Administrator is monitored and logged.

New users are registered and authorized based on the role they will be filling with ITD. Human Resource process ensures proper authorization of users as well as the removal of such authorizations when the users are terminated or transferred.

Access to all system components and functions are authorized based on the roles and responsibilities of the system users. Physical access to sites is restricted to only personnel that needs access to the site in order to fulfill job duties and customer commitments. Transmission, movement, and removal of information is protected and restricted as required by both requirements and policy.

All servers and workstations administered by ITD require users to login prior to being granted access to system resources. To ensure security and confidentiality, all Active Directory login credentials are encrypted during transmission. Local guest and anonymous accounts have been deactivated or deleted. All workstations located in an area of public access are configured to provide only the services needed. All workstations have automatic screen locking active with a maximum of a 15-minute activation time. Servers and workstations are required to be either manually logged off or locked prior to leaving them unattended.

Unique user IDs and passwords are assigned to each user, and initial passwords and passwords reset by administrators are one-time passwords that are required to be changed at next use. A web application has been created to allow authorized individuals to unlock Active Directory accounts. ITD has a centrally managed password management system in an encrypted database. Master "break-glass" passwords are stored at the secondary datacenter in a sealed envelope. Where acceptable to the network/host operating systems, ITD enforces the following password as defined in ITD's Identification and authentication standard.

Guest and system-supplied user IDs not required by applications or systems are required to be removed, renamed, or disabled during system setup. For guest and system-supplied user IDs that cannot be removed or disabled, the default password is changed. For network infrastructure devices, all default authentication credentials are required to be changed during setup.

ITD issues general credentials for ITD staff that allows them access to basic e-mail, file, and print services. These credentials are not granted Administrator level access. The staff that requires Administrator access are issued a separate set of credentials to administer IT systems. The Administrator access granted is the least privilege necessary to perform the job function effectively

Wherever possible, individual credentials are used to administer ITD resources. When shared credentials are necessary, they are changed every 60 days and immediately when a staff member with security privileges terminates their employment with ITD. Additionally, ITD automatically disables accounts after 60 days of inactivity.

Unauthorized malicious software is prevented and detected through both network protections and endpoint protections. ITD, in conjunction with the Enterprise Architecture Security Domain Team, has implemented policies and procedures to address the prevention and detection of computer viruses and the installation of virus prevention software and critical updates. ITD uses virus and spyware detection programs on all workstations and servers. In addition, ITD deploys additional appliances at key locations on the network to monitor virus activity.
Anti-Malware software has been installed and active on all devices that can effectively run an anti-malware or anti-virus client. Auto-distribution of current anti-virus signature files has been configured. All incoming files, including email, are scanned in real-time for malware. In addition, all files are scanned for malware on a weekly basis. Files containing malware which cannot be cleaned are deleted.

ITD resides within a locked facility and utilizes identification badges to grant access to restricted areas and to ensure that only authorized personnel is in restricted areas. ITD employees and contractors are required to wear their badges while on ITD premises. Contractors who have had security background checks are allowed unescorted access to ITD premises specific to the project they are working on.

Visitors to ITD datacenters are required to sign-in at one of ITD's reception areas and wear Visitor badges. Visitors are not permitted unescorted access at ITD datacenters. Visitor logs serve as audit records for physical visit reconstruction.

ITD maintains a video surveillance system for critical ITD entry points. The video logs are maintained for approximately three weeks and are used to investigate security or personel incidents. ITD receives usage reports from the Highway Patrol who manages the door access system. These reports are reviewed by security and data center staff for inappropriate access attempts.

Physical security to facilities housing ITD equipment and personnel is also controlled via multiple physical barriers. Media-storage areas (key-locked cabinets, tape vaults, etc.) are doubly secured via badge-reader and traditional key-lock countermeasures.

7. System Operations

Vulnerability scans are run on a regular basis on base infrastructure components. Specific vulnerability scans are run at user organization's request at a frequency determined ate their request. Vulnerabilities are evaluated and sent to the responsible administrators for resolution.

Networking equipment monitors for signatures including know vulnerabilities. A managed security appliance is provided and monitored by MS-ISAC for alerting and reporting of threats in real time.

A security incidents plan has been developed as well as policy and procedures for the handling of security incidents. This includes the definition of security incidents, handling evidence, investigative practices, roles, responsibilities and lines of communication. This plan includes communication requirements set forth by the user organization.

Incident Response is coordinated by the ITD Security Division and is responsible for ensuring that ITD responds to security incidents in a timely and effective manner. An individual has been designated to coordinate the incident prevention/response/notification process throughout ITD. Incident response

contacts are designated by each user organization. The ITD coordinator communicates incidents or vulnerabilities to user organization contacts. The user organization contact communicates any incidents or vulnerabilities to appropriate personnel.

ITD maintains a Security Information Event Management (SIEM) system to store centralized log information. This system is used to identify and prioritize potential security events for investigation. ITD currently maintains system and operations logs for the following environments:

- Active Directory
- Tivoli Directory Server
- AS/400
- RACF
- Oracle
- SQL Server
- PeopleSoft
- VPN – Juniper and NetMotion
- Syslog – firewall logs

ITD, in conjunction with the Enterprise Architecture Security Domain Team, has implemented policies and procedures to address firewall management, intrusion prevention and detection, and remote access. ITD adheres to the concept of least privilege necessary when configuring and administering the State's IT infrastructure. Accordingly, network and system administrators only enable the services or ports that are necessary for the equipment or application to perform its necessary business function. This principle includes but is not limited to the following infrastructure components: Servers, Switches, Firewalls, and Applications. Where applicable, ITD deploys Secure Socket Layer (SSL) encryption. Remote Desktop Protocol (RDP) is allowed inside the state network when configured at the strongest security settings. Third-party solutions such as LogMe In or GoToMyPC are expressly prohibited and, where possible, are blocked. ITD utilizes a content filtering appliance to filter access to Internet sites and materials it deems inappropriate for business use.

Firewalls have been implemented to protect the State's network and computing resources from untrusted sources. The ITD Network Firewall Group administers firewalls based upon authorized service requests passed through the Work Management System after review by the ITD Security division. ITD's policy over firewall control is to lock down all access and open only authorized ports and hosts that require access. ITD's Security team reviews firewall activity logs each following business day for reported failed connection attempts. The review looks for repeated attempts to break one or multiple firewalls within the network. If found, the Security Officer reports the incident(s) to the Network Firewall Group to lock the offender from accessing the outermost state network firewall.

ITD has implemented Intrusion Detection Systems and performs regular vulnerability assessments on its computing and network infrastructure to proactively identify systems with high-risk profiles. Where possible, ITD utilizes automated procedures to respond to event anomalies. Current automated processes include:

- Automated user account locking after 3 unsuccessful attempts
- Automated distribution of sensitive attempt violations to information owners
- Blocking all traffic from nation states that present sustained and systemic risk to the health of STAGEnet

ITD utilizes the state Virtual Private Network (VPN) for all remote access connections other than those that are externally available outside the state firewall. ITD system and network administrators only use state-owned computers and state-owned mobile devices that adhere to ITD's mobile device access standards for access to systems when using their Administrator credentials

8. Change Management

ITD evaluates and addresses the requirements of systems throughout the system lifecycle. ITD works in conjunction with the user organization to ensure all requirements are in place. All system components are updated as defined by rudiments as they change. Identified deficiencies are addressed if discovered.

Changes to system components are implemented through the change management process. Changes to the system can be initiated by either ITD or at the request of the user organization. Testing is carried out on all changes as appropriate. Users and stakeholders review and approve results of testing prior to implementation. A request for the change is put in through a formal process and then reviewed by the change advisory board. Once approved all affected entities are notified of the change. Once the change is implemented another notice is sent.

Emergency maintenance may be done outside of the standard Change Windows and without 48-hour notice. Emergency changes must be logged. Divisional staff may expedite the voting process, and assume full responsibility, by changing the status to "Approved" at any time. If possible, it is helpful to use a status of "Accepted Divisionally" for a short period of time to allow internal discussion.

Changes that could affect a system's internal control are evaluated by the presence of a security division representative on the Change Advisory Board. Mitigation strategies are reassessed if required due to a change.

9. Risk Mitigation

ITD is primarily funded by Special Funds. Government and educational entities pay ITD for technology services with money allocated in their budgets by the legislature. ITD itself is an internal service fund operating from a revolving cash fund. Federal regulations prohibit ITD's Total Net Assets from exceeding two times its average monthly expenditures.
ITD generates monthly billing at the beginning of each month for services provided during the previous month. The services are divided into Data Processing and Telecommunications billing statements. ITD maintains about 120 service rates.
Effective October 1, 1998, the allowable portion agencies may apply towards the ITD billings when charging federal programs is 100% for all bill codes. In July 1998 ITD met with a representative from the Cost Allocation Division of the US Department of Health and Human Services. It was determined that the rates ITD charges do not include any unallowable costs and that ITD's retained earnings fall within the acceptable limits found in the Cost Principles for State and Local Governments (Circular A-87).
ITD tracks and monitors the expense and revenue of each service in cost centers to ensure that one service is not subsidizing another. The federal government does not allow state central service agencies to accumulate an excess fund balance. Regulations establish specific standards for determining allowable costs for services in federally funded projects. ITD monitors the cost centers and adjusts rates accordingly.

ITD monitors budgetary spend with cashflow statements and budget reconciliation reports showing biennium to date spending trends. To allow the Budget Office to control the rate of expenditures as required in NDCC 54-44.1-03, Section 5, ITD may allot their appropriations by month. The state accounting system allows monthly expenditure estimates and will provide comparisons of monthly estimates to actual expenditures.

Physical assets are maintained within a fixed asset application that calculates depreciation on a monthly and annual basis. In accordance with NDCC 44-04-07, the director of each agency and institution is required to maintain a complete and current inventory record of all property of sufficient value and performance to render such inventory record practical. Each year, every agency and institution are to do a physical inventory (an actual verification of the inventory records via a physical observance of each item)

and certify said inventory. ITD has insured our state-owned assets in accordance with NDCC 26.1-22, the State Fire and Tornado Fund.

ITD has defined the practices in place to ensure that the control activities defined in the description on the system are in place and operating. These practices are laid out as part of the control matrix for each and every control activity.

10. Confidentiality

User organization information is protected throughout the system lifecycle. Information is accessible only to those who need such access to perform the functions of their roles. Information is protected against unauthorized access, use or disclosure. ITD works in conjunction with the user organizations to ensure that requirements are defined and met as needed.

Access to information outside of system boundaries is not allowed unless so directed by the user organization. ITD contracts with third-party organizations specifically address confidentiality. Contractor requirements set forth by the user organization are followed as designated by the user organization. Changes to confidentiality commitments and requirements are communicated to all applicable parties.

On an annual basis, ITD employees and contractors are required to sign an acknowledgment document that references North Dakota Century Code § 12.1-13-01. This document relates to the disclosure of confidential information provided to government and states, "A person is guilty of a class C felony if, in knowing a violation of a statutory duty imposed on him as a public servant, he discloses any confidential information which he has acquired as a public servant. 'Confidential information' means information made available to the government under a governmental assurance of confidence as provided by statute."

See the section above entitled Security Access and Management for an overview of controls related to logical and physical access, including data and resources considered confidential. Individual agencies must establish logical access control consistent with the EA Standard – ST006-04.6 –Access Control and EA Standard – ST004-04.1 – Active Directory.

The standards outlined in G002-99 – Information Technology Contract Guidelines provide specific guidelines for establishing a contract with third-party technology providers along with applicable confidentiality requirements.

Encryption is used when the electronic transmission of information involves sensitive data that passes over the public network. The sensitivity of data is determined by the government entity administering the data or the application. Where possible, ITD utilizes the following encryption methods:

- Full disk encryption on all portable devices.
- Secure Socket Layer (SSL) Encryption for all web applications that require authentication and/or process sensitive data.
- Encrypted e-mail solutions for staff and customers that require e-mail encryption.

In accordance with ST002-04.1 *Remote Access Standard*, all remote access requires encrypted communications, and all external connectivity to the internal state network utilizes a VPN. All VPN connectivity is authenticated and authorized by the enterprise authentication/authorization process. Authentication for remote access to servers is provided by the central authentication server and requires registered user ID's. Where data encryption is used, the government entity administering the data or the application is required to have a recovery plan for encryption keys.

11. Availability

Capacity is evaluated and planned for to ensure availability starting with architectural of the environment. The usage of system capacities such as disk space, processor, memory, and bandwidth are monitored and maintained through various tools that report and alert based on predefined criteria. This allows the system to be managed and provide for all capacity needs in a timely manner.

Recovery of the infrastructure is planned for and documented with prioritization of services defined and reviewed. Backup and replication systems are monitored and responsible parties are alerted in the event of a failure. ITD has established formal policies and procedures that outline requirements for agencies to review their data and identify backup requirements. These standards also indicate that backup procedures must adhere to the Continuum of Government guidelines. Requirements for backup of systems is primarily covered by the Enterprise Service Level Agreement and thereafter the Hosting Service Level Agreement.

Daily off-site backups are provided for all data hosted and source-code written by ITD. Databases have full weekly backups and nightly incremental backups, while other datasets only backup items that have changed during the day. The standard backup configuration allows for a maximum of five different versions of each file to be stored within a seventeen (17) day window. A single version of the file will be retained even if it was done outside the seventeen (17) day window. Upon deletion from a system, the most recent version of a file is retained for forty seven (47) days before being completely purged from backup. Large-scale storage of static data typically warrants an alternative custom backup configuration.

Service level objectives for backup reliability include:

- There will be less than two failed/ canceled full or incremental backups per month
- Successful backups are expected 99.00% of the time, with a minimum of 95.00%
- Successful recoveries are expected 99.00% of the time, with a minimum of 95.00

ITD's Computer Operations Manager and support staff receive an itemized list of tapes from backup administrators. These tapes are outputted at the secondary data center from the tape library system to be transported to the offsite backup location. These tapes are gathered and transported to the offsite location. Additionally, this process identifies tapes that are already in the offsite location for return to the tape library. These tapes are gathered and transported to the secondary data center for return to the tape library.

ITD supports near real-time failover. Systems are manually failed over, allowing ITD to assess the incident and make decisions based on all factors of the incident

Procedures supporting system recovery in accordance with recovery plans tested as defined and agreed upon with each induvial agency as directed by that agency.

ITD's Data Center environmental controls include fire suppression, raised floors, water detectors, smoke alarms, and air conditioning units. Semi-annual tests are done to verify correct alarm operation. The Facility Management Division provides a UPS for backup power and power regulation, and a generator for extended power loss. The UPS is tested semi-annually and the generator is tested weekly. The data center has a raised floor, smoke detectors, air conditioning, and security camera. Agency personnel is allowed access to the room through their key cards.

ITD maintains a disaster recovery hot site in Mandan, ND. The hot site facility provides replication of critical data and selected application servers. It houses full daily backup tapes for file recovery or complete system restore if needed. At this facility, ITD maintains a back-up of the current client-server and mainframe operating systems, start-up instructions, a copy of the disaster recovery plan, and a recovery priority list of mainframe and mid-tier applications. The off-site storage facility is physically

secured through a combination vault door and cement walls and ceiling. There is a fire extinguisher located inside the off-site vault. ITD updates the vault combination upon employee turnover, or annually at a minimum.

ITD performs regular testing its Disaster Recovery Plan at the hot site facility. Tests include restoring the IBM mainframe, AS/400, and other selected processing platforms. Test procedures and results are documented and reviewed by ITD's Contingency Planning Specialist, who coordinates any necessary changes to the Disaster Recovery Plan. External agency personnel also participate in the testing process to validate the recovery of their applications.

12. Integrity

ITD is responsible for maintaining the storage integrity of the information as submitted by user organizations. Information is backed up and stored as agreed upon with the user organization. These backups ensure that the information is in the same state as it was when submitted.

Backups to tape will alert on excessive CRC errors. Backup errors and issues are monitored and addressed by ITD storage administrators. Backups made to disk (virtual tape) are monitored for excessive I/O errors.

No data modifications are made by ITD staff unless directed to do so by the user organization through a support ticket. Modifications are documented and only performed by staff that is responsible for the system in questions and qualified to do so.

SQL integrity is a check performed weekly at ITD to ensure that the data written to disk maintains integrity. SQL server writes a checksum to each 8K data page. During an integrity check, SQL Server reads each data page in a database and calculates the checksum to compare against the stored value. If a mismatch is found the check shows up in a weekly email to DBAs. Most of the time a page can be repaired by using existing data using SQL commands built into the engine. As an alternative, it can be repaired by restoring a backup copy of the table, index, or other object affected.

SQL Backups run nightly and ITD DBA's use a policy checker tool to verify each database has a successful backup. Databases with missing backups can be added to the backup schedule according to the customer's needs. In addition, other policy checks validate security rights, database parameter settings, or other SQL server settings deemed necessary to monitor.

ITD's Enterprise and Hosting Service-Level Agreement (SLA) provides tailored solutions such as IBM WebSphere and its associated components, which generate security exceptions (alerts/events) in cases of abnormal server states, resource utilization, and/or transaction outcomes. Firewall logs of repeated failures and auto-blacklist actions are reported as security alerts to a Security Information and Event Management (SIEM). Additionally, service monitoring systems comprise ancillary error/exception alerting mechanisms (e.g., unsuccessful or unusually slow HTTP GET).

The tables below outline Enterprise Architecture (EA) standards that have been established related to the integrity of data handled by ITD systems.

Encryption Standards ST007-05.2 and ST002-04.2 ensure the integrity of the information by protecting it from alteration.

EA Standard ST007-05.2 – *Encryption*
Encryption shall be used when the electronic transmission of information involves sensitive data that passes over the public network.

EA Standard ST002-04.2 – *Remote Access*

1. All external connectivity to the internal state network must be by VPN.
2. All VPN solutions will be provided by ITD.
3. All VPN connectivity will be authenticated and authorized by the enterprise authentication/authorization process.
4. The enterprise Multi-Factor Authentication solution will be required in conjunction with VPN for remote access to sensitive data and/or information as defined by the agency.

The EA Standard DIT003-06.1 provides direction on how databases shall be secured including the principle of integrity.

EA Standard DIT003-06.1 – *Enterprise DIT Security*

1. Every database will have at least three distinct areas: development, acceptance testing, and production.
2. Administrative privileges on production and acceptance testing database areas:
    - Multi-agency shared infrastructure will be restricted to the agency hosting the database.
    - Single agency infrastructure will be restricted to either the agency hosting the database or the agency's DBA staff.
3. Migrating changes from acceptance test to production requires that the agency who owns the data have a formal acceptance testing and sign off process.
4. Agency assigned developers will have developer privileges to development database areas.
5. Create user privileges on all database areas will be restricted to the database or security administrators.
6. Access to system level views of database catalog information will be restricted.
7. Migrating changes from development to acceptance test is requested by the agency assigned developers.
8. Database scripts which modify database objects will be reviewed, approved, and run on production and acceptance test databases by the database administrators.
9. Installation and creation of production, acceptance test and development databases for new systems must be performed by the database administrators.
10. User authentication shall utilize the enterprise Microsoft Active Directory if supported by the Database.
11. Personnel administering vendor applications that control changes to database objects through the vendor's tool and not scripts will be allowed to apply upgrades to all database areas. Prior to deployment in production, the changes created by the tool must be reviewed to assure that all changes adhere to this standard. In addition, before any changes are made to any database area, backups must be taken for recovery purposes.

The EA Standard DIT003-06.1 provides a guideline on how databases should be secured including the principle of integrity

EA Standard DIT-BP001 – *Database Security Best Practices*

1. Grant privileges only to a user or application which requires the privilege to accomplish necessary work. Excessive granting of unnecessary privileges can compromise security.
2. No administrative functions are to be performed by an application. For example, create user, delete user, grant role, grant object privileges, etc.
3. Privileges for schema or database owner objects should be granted via a role and not explicitly. Do not use the "ALL" option when granting object privileges, instead specify the exact privilege needed, such as select, update, insert, delete.
4. Password protected roles may be implemented to allow an application to control access to its data. Thereby, end users may not access the application's data from outside the application.
5. Access to Administrative or System user accounts should be restricted to authorized DBAs.
6. Do not grant system supplied database roles. These roles may have administrative privileges and the role privileges may change with new releases of the database.
7. Database catalog access should be restricted. Example: Use "USER_VIEWS" instead of "DBA_VIEWS" for an Oracle database.
8. Privileges granted to PUBLIC are accessible to every user and should be granted only when necessary.

9. Any password stored by applications in the database should be encrypted.
10. Applications should not "DROP", "CREATE" or "ALTER" objects within the application.
11. Utilize the shared database infrastructure to share cost whenever possible.
12. Applications should not access the database with the same security as the owner of the database objects. For example, on SQL Server do not grant the "dbowner" role and on Oracle do not use the Schema userid to connect to the database. Setup another userid with the necessary privileges to run the application.

Subservice Organizations

Subservice Organization	Services Provided
Multi-State Information Sharing & Analysis Center	• Netflow Monitoring and Analysis (Albert) • Network & Computer Forensic Analysis • Log & Malware Analysis • Access to the Malicious Code Analysis Platform (MCAP) • Remediation Consulting

User Control Considerations

ITD's applications and processing procedures were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve certain control objectives included in this report. This section describes additional controls that should be in operation at user organizations to complement the controls at ITD. User auditors should consider whether the following controls have been placed in operation at user organizations.

- All data and systems in the custody of ITD have a defined owner. The defined owner is the agency responsible for the business use of the data. There is one and only one owner for each data and the owning agency appoints an agency security officer who is responsible for controlling access rights.
- ITD utilizes an online Work Management System where authorized users can request additions, changes or deletes to access rights for systems maintained by ITD.
- On an annual basis, ITD contacts the Security Officers at each agency to review the access rights granted to each agency. This is an addition to the daily and monthly access reports sent to each agency.
- ITD enforces Active Directory standards internally, over user authentication within their internal Windows and web-based applications. Agency security personnel are responsible for establishing and monitoring active directory parameters, in accordance with EA Security Domain Team recommendations, for user authentication and data access privileges within their own directories of the state network.
- ITD does not own most of the information residing inside ITD's information systems. The information owner for most data is the user organization.
- Controls to provide reasonable assurance that changes to processing options (parameters) are appropriately authorized, approved, and implemented
- Controls to provide reasonable assurance that transactions are appropriately authorized, complete, and accurate
- Controls to provide reasonable assurance that erroneous input data are corrected and resubmitted
- Controls to provide reasonable assurance that output reports are reviewed by appropriate individuals for completeness and accuracy
- Controls to provide reasonable assurance that output received from ITD is routinely reconciled to relevant user organization control totals

User Entity Control	Associated Control Objectives
User organizations are responsible for establishing security access administration policies and procedures for the allocation of user IDs, passwords and access levels which are created by client system administrators.	Control Objective 1
User organizations are responsible for maintaining the confidentiality of system user IDs and passwords.	Control Objective 1
User organizations are responsible for timely written notification to ITD of changes to authorized security officers administrators, and persons authorized to approve access requests.	Control Objective 1
User organizations are responsible for the administration and tracking of Security awareness training within their organizations.	Control Objective 2
User organizations are responsible for sending authorized requests to ITD for updating access related to a change in an employee's job function, new employment, or termination.	Control Objective 6
User organizations should establish their end users in such a way that segregation of duties is achieved.	Control Objective 6
User organizations should configure workstations to enforce a session time-out after a period of activity.	Control Objective 6
User organizations are responsible for establishing and maintaining physical security of all user offices and computer equipment.	Control Objective 6
User organizations are responsible for limiting physical access to only those individuals that require such access to perform their jobs.	Control Objective 6
User organizations are responsible for approving and testing changes and updates.	Control Objective 8
User organizations should have procedures in place to require management authorization of requests for ITD to change or customize their environment.	Control Objective 8
User organizations are responsible for individualized Disaster Recover Plans and working with ITD to ensure proper requirements and agreements are in place.	Control Objective 10
User organizations are responsible for verification and validation of User organization information submitted.	Control Objective 12
User organizations are responsible for the development of an incident response plan at their sites in the event they are notified of an incident.	N/A
User organizations are responsible for reporting any issues encountered to ITD and for providing such assistance as is necessary to permit problem resolution.	N/A
User organizations are responsible for communicating compliance needs based on all applicable laws, requirements, and standards needed to operate.	N/A
User organizations are responsible for submitting waiver requests based on all applicable laws and standards on behalf of venders who cannot meet such requirements and standards.	N/A
User organizations are responsible for submitting waiver requests for any hosting services not maintained by ITD.	N/A

Recommendations

No documentation of destruction of backup tapes (Recommendation #1)

Condition:
Backup tapes to be destroyed were marked on ITD's inventory list but there was no actual documentation that they were destroyed.

Effect:
A security risk could occur if expired tapes aren't destroyed properly.

Cause:
ITD doesn't monitor expired backup tapes to ensure they are destroyed properly

Criteria:
“IRS Publication 1075 Media Sanitation Requirements Explained states that it is critical that an agency maintain a record of its sanitization to document what media were sanitized, when, how they were sanitized, and the final disposition of the media.

Recommendation:
We recommend ITD follow IRS guidelines for maintaining a record of documentation of when, how, and what media is destroyed.

ITD Response:
ITD agrees with this finding. While destruction of tape media was documented certificates of destruction were not maintained. ITD has adjusted the destruction process to maintain such records going forward.

ITD isn't monitoring their user groups within Active Directory (Recommendation #2)

Condition:
There were 4 employees that were not listed in the right Active Directory Group, so they didn't receive the sixty (60) day max password life settings

Effect:
The 4 Employee accounts are at an increased risk of being compromised.

Cause:
These are employees they neglected to put in.

Criteria:
ITD's Password Group Policy (7.2) states ITD follows a sixty (60) day window for the maximum life of a password.

Recommendation:
We recommend ITD ensure all employees receive the established standard for password expiration, length, complexity and history

ITD Response:
ITD agrees with this finding. ITD has implemented process to ensure that password complexity requirements are applied to all ITD employees.

Unnecessary Privileged Accounts *(Recommendation #3)*

Condition:
ITD has 48 employees with privileged accounts that have not been accessed and default passwords that have not been changed.

Effect:
Privileged accounts still have the default password and without being changed to a more secure and complex password, they create a security risk for ITD.

Cause:
ITD failed to ensure that the privileged accounts were needed and to ensure that once they were setup the user logged in at least once to change the password.

Criteria:
ITD's "Description of Service Organization's System" states staff that require Administrator access are issued a separate set of credentials to administer IT systems.

Recommendation:
We recommend ITD ensure employees need privileged accounts before setting them up and once setup ensure the account password is changed.

ITD Response:
ITD agrees with this finding. ITD has adjusted active directory scripts to disable privileged accounts that have not logged in.

Inactive Privilege Accounts Not Disabled *(Recommendation #4)*

Condition:
ITD has 48 employees with privileged accounts that have not been disabled after 90 days of inactivity.

Effect:
These accounts still have the default password and without being changed to a more secure and complex password, they create a security risk for ITD.

Cause:
ITD has not written a script that will disable privileged accounts that haven't been logged into.

Criteria:
ITD's "Description of Service Organization's System" states domain-level user accounts are automatically disabled after 90 days of inactivity.

Recommendation:
We recommend ITD ensure privileged accounts that are never used are disabled after 90 days.

ITD Response:
ITD agrees with this finding. ITD has adjusted active directory scripts to disable privileged accounts that have not logged in.

Non-Privileged Credentials Used for Admin Activities *(Recommendation #5)*

Condition:
There were 7 out of the prior 19 administrative groups in the last audit that contained both privileged and non-privileged accounts.

Effect:
Privileged accounts have greater security requirements, using non-privileged accounts for administrative activities increases the security risk.

Cause:
ITD failed to implement a prior recommendation.

Criteria:
ITD's "Description of Service Organization's System" states only privileged accounts are used for system administration activities.

Recommendation:
We recommend ITD ensure that only privileged accounts are used for administrative activities.

ITD Response:
ITD agrees with this finding. ITD does not allow for administrative work to be performed without a privileged account. However, because some groups exist that have both regular users and privileged accounts ITD cannot demonstrate this. ITD is working to clean up such groups and formally document the need and purpose for any group that contains both account types.

Veterans preference law not correctly applied *(Recommendation #6)*

Condition:
ITD did not appear to follow the veterans preference for a position filled on 6/4/2018. A veteran scored a tie for the top 5 candidates for this position and ITD only interviewed the top 4 candidates. They sent a letter to the veteran indicating ITD interviewed the top 5 and the veteran didn't make the cut even though they were tied for 5th.

Effect:
The veteran did not receive the preference state law requires.

Cause:
ITD HR said their standard is to interview the top five. In this case there wasn't a top five—due to the scoring, there would have been nine applicants to interview. Thus, it makes sense to start with the top four and then add the next five (that had the same score for 5th place) if a candidate wasn't found. They take a close look at the scoring and they work to meet their standard every time. In this case, the scores didn't allow for that. As far as the veteran's letter, a standard template was used—five is their predetermined number.

Criteria:
Violation of the Veterans Preference law (NDCC 37-19.1)

Recommendation:
We recommend that ITD correctly apply the Veterans Preference law as part of their competitive hiring process

ITD Response:
ITD disagrees with this finding. ITD always works to follow veteran's preference law. In the instance noted for this finding ITD has worked with the employment attorney who has given the opinion that in this case the law was followed. ITD will continue to work to follow veteran's preference going forward.

State Auditor's Concluding Remarks:
North Dakota Century Code 37-19.1-02(3)(c) states "The employing authority shall designate a prescribed number of eligible individuals to be considered from the top number of a group of eligible candidates in rank order." Best practice guidance provided by Human Resource Management Services states, "Before receiving and reviewing applications, a decision should be made as to how many applicants to forward on to the appointing authority for final consideration." In this case, the decision to interview four applicants instead of five was made after reviewing the applications and determining that five applicants were tied for the fifth position.

No Policy/Procedures for sensitive equipment not found during inventory *(Recommendation #7)*

Condition:
Policies/procedures haven't been established for follow-up on sensitive equipment not found during their annual physical inventory.

Effect:
Unaudited equipment could pose a security risk if it has sensitive information on it.

Cause:
ITD relies on encryption as a safety net for unaudited items that pose a security risk. ITD has not made a serious effort to identify and find their sensitive equipment

Criteria:
ITD's "Description of Service Organization's System" states they maintain an inventory of information assets. Procedures are established to review the inventory on an annual basis.

Recommendation:
We recommend ITD develop policies and procedures to follow-up on sensitive equipment not found during the annual physical inventory to ensure the equipment is found or verify that there is no security risk associated with the equipment.

ITD Response:
ITD agrees with this finding. ITD has implemented a process for ensuring that after the annual inventory is complete, systems not found are evaluated for risk and documented accordingly.

Not all core ITD components are tested and documented *(Recommendation #8)*

Condition:
ITD had 1 core component listed in their Disaster Recovery that did not have formal

documentation that any testing occurred.

Effect:
ITD was not monitoring and documenting all core components to ensure testing was completed.

Cause:
ITD does not have formal documentation on all disaster recovery core components.

Criteria:
ITD's "Description of Service Organization's System" states Disaster Recovery of core ITD components are tested on a regular basis.

Recommendation:
We recommend ITD test and document disaster recovery of all their core components.

ITD Response:
ITD agrees with this finding. ITD does test all core components. However formal documentation is not completed in some instances. ITD has implemented a process to ensure that all testing is properly documented.