

PROJECT CODE
I112-15

INFORMATION TECHNOLOGY DEPARTMENT
INDEPENDENT SERVICE ORGANIZATION AUDIT
For the period 4/1/2014 – 10/1/2014

Office of the State Auditor
Division of State Audit

**LEGISLATIVE AUDIT AND FISCAL REVIEW
COMMITTEE MEMBERS**

***Representative Gary Kreidt – Chairman
Senator Ralph Kilzer – Vice Chairman***

Representatives

*Wesley R. Belter
Jeff Delzer
Ron Guggisberg
Patrick Hatlestad
Jerry Kelsh
Keith Kempenich
Andrew G. Maragos
Bob Martinson
Corey Mock
Marvin E. Nelson
Chet Pollert
Dan Ruby
Jim Schmidt
Robert J. Skarphol
Wayne Trottier*

Senators

*Judy Lee
David O'Connell
Terry M. Wanzek*

TABLE OF CONTENTS

Transmittal Letter	1
Executive Summary	2
Significant Finding.....	2
ITD’s Description of Controls	3
ITD’s Assertion	28
Independent Auditor’s Report	29
Scope	29
Service Organization’s Responsibilities	29
Service Auditor’s Responsibilities	30
Inherent Limitations.....	30
Opinion.....	30
Description of Tests of Controls	31
Restricted Use	31
Description of Tests of Controls and Results Thereof	32
Security Principle and Criteria Table	32
Policies.....	32
Communications	33
Procedures	33
Monitoring	35
Test of Security Controls	36
Recommendations related to Security.....	44
ITD lacks a formal risk assessment framework.....	44
No periodic review of enabled ports/services is being done	44
No policy requiring visitors to be escorted in the data centers.....	45
Enterprise Architecture Standards not reviewed according to Description of Controls.....	45
Availability Principle and Criteria Table	46
Policies:	46
Communications:	47
Procedures:	47
Monitoring:	49
Test of Security Controls	49
Processing Integrity Principle and Criteria Table.....	54
Policies:	54
Communications:	55
Procedures:	56
Monitoring:	58
Test of Security Controls	58
Confidentiality Principle and Criteria Table.....	58
Policies:	58
Communications:	59
Procedures:	60
Monitoring:	62
Test of Security Controls	63

TRANSMITTAL LETTER

May 6, 2015

The Honorable Jack Dalrymple, Governor
Members of the North Dakota Legislative Assembly
Mike Ressler, Chief Information Officer

Transmitted herewith is the ITD Service Organization Audit for the period April 1, 2014 to October 1, 2014. This audit resulted from the statutory responsibility of the State Auditor under NDCC § 54-10-01.

The Information Technology Department provides wide area network services, electronic mail, file and print server administration, database administration, storage, application server, and hosting services. The Information Technology Department serves all state agencies, including institutions under the control of the board of higher education, counties, cities, and school districts in this state.

Inquiries or comments relating to this audit may be directed to Donald LaFleur CPA, CISA, Information Systems Audit Manager, by calling (701) 328-4744. We wish to express our appreciation to the Office of Management and Budget, and the Information Technology Department for the courtesy, cooperation, and assistance provided to us during this audit.

Respectfully submitted,



Robert R. Peterson
State Auditor

EXECUTIVE SUMMARY

The purpose of our audit was to evaluate the fairness of the presentation of ITD's Description of Controls. We conducted our examination 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, 1) the description is fairly presented on the description criteria, and 2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period April 1, 2014 to October 1, 2014.

Significant Finding

We had the following findings:

- ITD lacks a formal risk assessment framework.
- No periodic review of enabled ports/services is being done.

ITD'S DESCRIPTION OF CONTROLS

System Description

Background

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. The department is responsible for all wide area network services planning, selection, implementation and operation for all state agencies, including institutions under the control of the State Board of Higher Education, counties, cities, and school districts. ITD's responsibilities also include computer hosting services, software development services and state wide communications services for state agencies, universities, political subdivisions and schools.

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.

People and Infrastructure

- The ITD exists for the purpose of leading state agencies in discovering, assessing, and implementing information technologies. ITD is committed to better understanding state agency needs and in assisting in the implementation of the proper technology 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. In support

of this mission, ITD has established the organizational structure depicted in Figure 1 below.

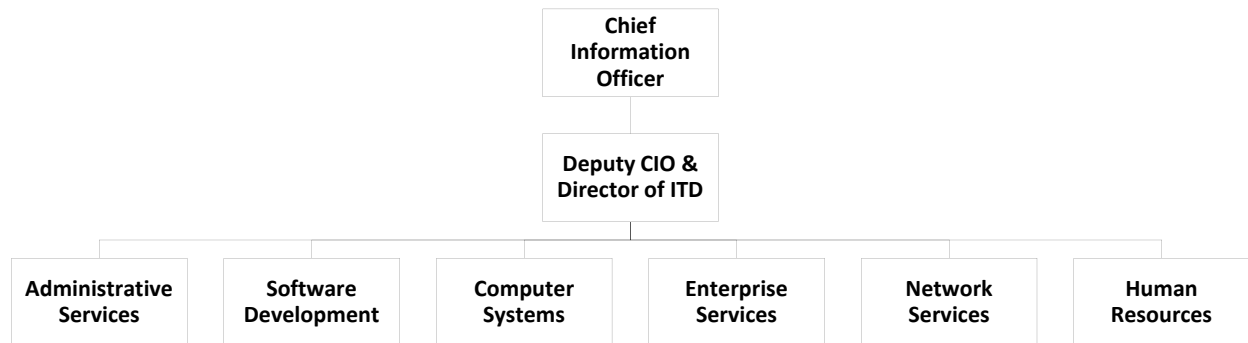


Figure 1 – ITD Organizational Structure

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

Administrative Service - 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 are 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 uninterruptible 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 state agencies 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 state agencies, local government, higher education, and K-12 schools. Ensure the reliability and security of 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 Resource - 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.

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) management of the devices, tools, or software that enable IT; (2) hosting computer systems or applications; and (3) network services that accommodate the data, voice, video, and multimedia traffic over a statewide backbone to support the missions of government and education.

The statewide network, known as the North Dakota Statewide Technology Access for Government and Education network (STAGEnet) , was created in 1999 and provides access for North Dakota State Government, K-12, Higher Education, and political subdivision (e.g., counties and cities). ITD does not own most of the information residing inside STAGEnet or ITD's other information systems. The information owner for most data is a state agency or political subdivision, and ITD will only grant access to information based upon authorization requests from Agency IT Coordinators.

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring of Controls

Control Environment

Management

The CIO has the authority and responsibility for information systems security surrounding State of North Dakota information technology assets. The CIO reports directly to the Governor.

ITD's 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, and the Directors of the six ITD divisions previously mentioned.

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.

Security Policies and Procedures

The ITD Cybersecurity Framework policies are developed and maintained by the ITD Security Section by directive of the State of North Dakota's CIO. The Cybersecurity Framework reflects core mission requirements for ITD to address cybersecurity policies in greater detail. Policies in the Cybersecurity Framework are reviewed by the ITD

Virtual Security Team and approved by the CIO. The Cybersecurity Framework policies are reviewed on an annual basis.

ITD has developed a collection of Enterprise Architecture (EA) Standards in collaboration with executive branch state agencies. These policy standards are reviewed annually and documented on the standard with a “Last Reviewed” date. The eleven EA Standards were all reviewed between July 2013 and March 2014. EA Standards are suitable across the scope of the entire enterprise. EA Standards are reviewed by both the Architecture Team and the Architecture Review Board. To ensure appropriate IT security considerations were addressed during development of the EA Standards, ITD’s Enterprise Information Systems Security Administrator is a member of both the Architecture Team and the Architecture Review Board.

All state security standards and policies are published on the North Dakota Enterprise Architecture web page, and access to modify these web pages is restricted to authorized users. The ITD Cybersecurity Framework policies address the topics listed in the table below.

Access Control	Active Directory	Anti-Spyware/ Anti-Virus
Auditing	Employee Security Awareness	Encryption
Incident Prevention & Response	Mobile Device Access Control	Physical Access
Public Workstation Access	Remote Access	State Network Security

In addition to the EA standards and the ITD Cybersecurity Framework, ITD’s Administrative Policies and Procedures Manual references administrative policies that pertain to the following information security topics:

- Background Checks
- Confidentiality
- Acceptable Use of Electronic Communication Devices
- Requests for Telephone Records
- Requests for E-Mail Records
- Microcomputer Usage
- Workstation Protection
- Smartphone Devices
- Physical Security

Security Access and Management

ITD has established Active Directory as the primary identity management repository providing users with a single set of credentials for network and application sign-on. 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)

The ITD Security Section has primary responsibility to administer and monitor the identity management repositories. As necessary, the Security Section will delegate administration of selected identity management repositories to other divisions and monitor the activity in those repositories.

Identification and Authentication

All servers and workstations administered by ITD require users to logon 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 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 characteristics:

- a minimum password length
- a combination of upper and lower case letters and special characters
- a maximum and minimum password life
- password reuse restrictions
- automated disabling of User IDs after a specified number of invalid sign on attempts
- requiring disabled User ID’s to be manually enabled
-

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. Staff that require 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 managed by ITD's password management system. Administrators use their administrative credentials to access the password management system. Individual administrative credentials are changed every 60 days and immediately disabled when a staff member terminates their employment with ITD. Additionally, ITD automatically disables accounts after 90 days of inactivity.

ITD provides centrally-managed identification and authentication for all network infrastructure devices and is controlled through the following processes:

- Read/Write access is authenticated by Active Directory with group membership controlled by the centralized infrastructure.
- Read/Write community strings are uniquely defined per device.
- Shared Read Only community strings are only permitted for network management tools that reside inside the IP range for the Network Management VLAN.

The control of access to mobile devices is critical to the security of ITD systems. Accordingly, the following access control mechanism and standards have been established for mobile devices: a power-on password is used, automatic device locking occurs after a specified time of inactivity, and when configurable, devices are disabled after a specified number of successive invalid sign on attempts. If a device becomes disabled, all of its local information is automatically erased, and it must be reconfigured to connect to the State's servers.

Active Directory Administration

ITD has established a single forest architecture for its Active Directory. All state agency 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 roles/responsibilities reside with ITD. The Domain Administrator initially establishes each agency's OU, along with the first user, computer and group. This first group 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.

Network Security

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 Procedure (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. Firewall activity logs are integrated with ITD's security information and event manager which looks for repeated attempts to break one or multiple firewalls within the network. If found, the Security team coordinates with the Network Firewall Group if it becomes necessary to block attackers 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 a specified number of 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.

Virus and Malware Protection

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 most 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.

Data Encryption

Encryption is used when the electronic transmission of information involves sensitive data that passes over the public network. 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.

Data Classification

Agency information owners apply account management access rules based on changes in roles or termination of employment. Account management is applied by agency account managers according to information system security requirements and risk assessments. The ITD Cybersecurity Framework includes a section that addresses Establishing or Improving a System Security Plan, which indicates that a system is identified by its mission objectives, scope of dependent systems and assets, regulatory requirements and overall risk tolerance. Roles and responsibilities outlined in the Framework indicate that the owners are responsible for authorizing access privileges and risk profiles and ensuring there are regular reviews and updates to manage changes in risk profiles.

Agency Directors are responsible for information security in each agency, for reducing risk exposure and for ensuring the agency's information technology practices to not introduce undue risk to the enterprise. The director also is responsible for ensuring compliance with state enterprise security policies and with state and federal regulations.

Physical Security

The ITD Security Section will coordinate with the entities identified below to restrict physical access to ITD premises. The ITD Security Section will coordinate with ITD Division Directors to review access restrictions on an annual basis.

- ND Highway Patrol
- Dakota Carrier Network Facilities Staff
- ND Association of Counties Facilities Staff
- Montana Dakota Utilities Facilities Staff
- Northbrook Mall Management Facilities Staff

ITD resides within a locked facility and utilizes identification badges to grant access to restricted areas and to ensure that only authorized personnel are 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's data centers are required to sign-in at the reception areas and wear Visitor badges. Visitors are not permitted unescorted access while on ITD's data center premises. Visitors at ITD's main campus are required to sign-in and wear Visitor badges that provide them access to specific areas depending on the nature of their visit to ITD. 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 personnel 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.

Personnel Security

ITD's has formal hiring and management practices to ensure that employees are qualified for their job responsibilities.

ITD uses the ND Human Resource Management Services job classifications for all positions. The job classifications detail the minimum qualifications necessary for each position. A position information questionnaire (PIQ) is used to further define the position qualifications and personnel selection criteria.

Hiring procedures include performing a criminal background check on all employees. ITD performs an annual update of the employee information and has defined procedures that permit follow-up background checks to be performed on employees as needed.

ITD routinely processes confidential information and its employees are subject to the same restrictions and penalties regarding disseminations of confidential information as the entity that owns the information. Upon hire, and on an annual basis, ITD employees are required to sign an Acknowledgment of Secrecy Provision to ensure they are aware of the confidentiality requirements of the data they handle. In addition there is an annual acknowledgement required for other policies relevant to maintaining a strong control environment within ITD.

All employees complete either the ITD Security Awareness training or an agency security awareness program within the first three days of being granted access to the state government network.

Personnel training is accomplished through supervised on-the-job training, outside seminars, and in-house classes. Organizational policies and procedures are contained in ITD's Policy Manual which is available on ITD's intranet and covered as part of employee orientation.

Formal performance appraisals are conducted on an annual basis. Completed appraisals are reviewed by senior management and become a permanent part of the employee's personnel file.

Formal termination procedures document the process to obtain all ITD property from the employee and to remove both physical logical access upon termination. Additionally, user-access reviews are performed periodically to ensure all users are current and authorized.

Change Management

Change Advisory Board

Major changes or change requests that require down time are submitted to a Change Advisory Board (CAB). These changes must be approved by the CAB prior to implementation. The CAB is composed of technical members from state agencies as well as staff from ITD's software development, telecommunications, computer systems divisions, and ITD's Enterprise Information Systems Security Administrator. The CAB meets on a weekly basis.

Emergency Changes

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. When possible divisions are encouraged to use a status of "Accepted Divisionally" for a short period of time to trigger the escalation process which allows for additional internal input and discussion.

Configuration Management

The ITD Computer Systems Division maintains the configuration inventory of its Intel computing platform (hardware, O/S software, applications software, facilities and data files) using automated tools. This group also utilizes a web-based change management system to log changes. Changes are logged in the system and approved by the Computer Systems Manager or the System Architect.

The ITD Network Services Division manages of its network infrastructure using automated tools that provide location information, performance metrics and a history of configuration changes.

The ITD Security Section and Quality Assurance team within the Software Development Division conducts regularly scheduled vulnerability scans to pro-actively identify potential risks to ITD hosted web applications. The results will be made available to the Software Development staff who are primarily responsible for patching applications to reduce the risk profile for applications under ITD control.

ITD performs an annual physical inventory of fixed assets within the department to ensure that there is adequate physical control over the acquisition and deployment of computing and network hardware.

Incident Response and Problem Management

The organization has developed a formal Security Incident Response Team Policy. The ITD Security Incident Response Team is facilitated by the ITD Security Section and is responsible for ensuring that ITD responds to security incidents in a manner that

optimizes interdivisional communication and minimizes the impact of a given incident. An individual has been designated to coordinate the incident prevention/response/notification process throughout the organization. Agency incident response contacts are designated by each state agency (or customer of ND IT). The ITD coordinator communicates incidents or vulnerabilities to agency contacts. The agency contact communicates any incidents or vulnerabilities to appropriate agency personnel.

ITD maintains an Intrusion Detection System (IDS) to monitor for network or host anomalies and known attack signatures.

Help Desk

ITD's Customer Service Division operates a help desk and provides a central repository for customers to report problems, ask questions, request information, and receive resolutions and answers. The help desk includes a Service Center Manager, one full-time Service Management Software Analyst and five full-time Service Desk Analysts. Service Desk Analysts cover 7am - 5pm M-F and rotate on-call Saturday morning through Monday 7am. Computer Operations staff cover calls 5pm - 7am Monday through Friday.

ITD's Help Desk receives requests via telephone, the Help Desk web site and email. They log and track all requests using FrontRange Solutions – ITSM System. ITD has implemented ITSM with the following control parameters:

- Defined assignment groups, supervisors, and role-specific security
- Defined incident categories, call-types, sub-call-types, and incident priority matrix
- Defined detail screens to gather call-type specific information, and customer-specific details
- Acknowledgement, escalation, and communication procedures

Monitoring

The ITD management team, consisting of the CIO, Deputy CIO, and the Directors of the six ITD divisions, meets on a weekly basis to discuss overall departmental projects, operational issues, and progress towards departmental strategic goals.

Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. Each division of ITD has implemented performance measures that measure the results of various processes involved in running the data center and provided the associated services to customers. Key performance indicators are reviewed daily, weekly or monthly by appropriate levels of management, and action is taken as necessary.

Management and staff members meet on a regular basis to discuss internal operations and overall departmental direction. Within most divisions managers and supervisors

meet weekly to discuss projects, operational issues, and progress towards strategic goals. In addition to divisional meetings ITD holds an all ITD staff meeting twice per year to communicate with all employees about major initiatives, major policy changes, and progress towards strategic objectives.

The organization obtains independent assurance of compliance with laws, regulatory requirements and contractual obligations through audit functions conducted by the Office of the State Auditor. The State Auditor performs routine examinations of ITD's financial, performance, and IT controls.

ITD conducts an annual customer survey to ensure the department is meeting customers' expectations. The survey allows customers to rate their satisfaction with the services provided by ITD and to provide suggestions for improvements. Survey areas include the service desk, software development, network service, E-mail services, telephone services, application hosting, records management, IT planning and oversight services, and an overall ITD rating. Results are published in ITD's strategic plan and on ITD's website.

The ITD Security Section and Quality Assurance team within the Software Development Division will coordinate to conduct regularly scheduled vulnerability scans to proactively identify potential risks to ITD hosted web applications. The results will be made available to the Software Development staff who are primarily responsible for patching applications to reduce the risk profile for applications under ITD control.

System Monitoring

ITD has implemented various infrastructure monitoring solutions to monitor performance characteristics (utilization, capacity, response time, usage, and resource availability). ITD has configured the software to automatically detect and report/record incidents. System uptime is reported to management. Detailed information about a system such as CPU utilization, I/O, memory, and disk capacity are aggregated and reports are available upon request.

The ITD Computer Systems Division has implemented ongoing procedures to monitor performance and capacity of the mainframe and mid-tier operating systems within the computer facility, and maintains historical statistics for future capacity planning and budgetary planning purposes.

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
- Syslogs – firewall logs

ITD reviews system and operational logs for any event anomalies, and detected anomalies are investigated. The log activity is maintained for a minimum of 90 days. Logs are aggregated in the SIEM and offenses are reviewed on a daily basis.

Risk Assessment Process

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 the organization provides, and management has implemented various measures to manage those risks.

The owners are responsible for authorizing access privileges and risk profiles and ensuring there are regular reviews and updates to manage changes in risk profiles.

Agency Directors are responsible for information security in each agency, for reducing risk exposure and for ensuring the agency's information technology practices do not introduce undue risk to the enterprise. The director also is responsible for ensuring compliance with state enterprise security policies and with state and federal regulations.

In Fall 2013, the organization contracted with IBM Global Services to conduct a risk assessment of the North Dakota Department of Human Services (NDDHS) Fully Integrated Eligibility Determination System (FIELDS). A Moderate security categorization from Federal Information Processing Standard (FIPS) 199 was used to conduct this risk assessment. Accordingly, National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 3 moderate controls were used in the evaluation of FIELDS. This risk assessment was limited in scope in order to comply with requirements from the Federal Health and Human Services (HHS) Centers for Medicare & Medicaid Services (CMS). The Technical control risk assessment was limited to FIELDS; however, the risk assessment included Managerial and Operational controls that are common throughout ITD.

ITD continues to work with agencies to evaluate risk to systems on an ongoing basis. Specifically, risk assessments are in the planning stage for multiple systems from NDDHS and the Office of State Tax Commissioner.

Information and Communication Systems

A description of the North Dakota Statewide Technology Access for Government and Education network (STAGEnet) is maintained and made available to the public at <http://stagenet.nd.gov>. In addition, a complete listing of the services provided by ITD to the state is described at <http://www.nd.gov/itd/services>.

To ensure that the obligations of users accessing ITD-administered systems are appropriately communicated, all employees are required to complete either the ITD Security Awareness tutorial or an agency security awareness program within the first three days of being granted access to the state government network. In addition, all employees with access to the state government network shall be required to participate in annual security awareness programs such as videos or web based training programs

On an annual basis, both ITD employees and contractors are required to sign an acknowledgement document stating that they have read and will comply with the organization's policies and procedures, including the ITD Cybersecurity Framework policies.

ITD provides services to a variety of customers and ensures open and timely communicate 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 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 at ITD's website under "Publications".

Procedures have been implemented for sharing information with the Social Security Administration, which is accomplished through Information Exchange Agreements (IEA).

ITD's Virtual Security Team is responsible to identify security priorities and policies for the department and facilitate cross divisional communication and coordination of these security priorities. This team is coordinated by the ITD Security Section and the Computer Services and Software Development divisions must have at least one member in regular attendance at each monthly meeting.

Communicating Incidents and Security Breaches

The timely communication of security breaches to all necessary individuals is critical to the organization's ability to effectively respond and minimize impact. ITD's Service Desk is the "Single Point of Contact" for all incidents, problems, questions, requests, and feedback. Security incidents are routed to the ITD Security Section as part of triage processes within the ITD Service Desk. The Incident Management and Request Fulfillment section from the Service Level Agreement (SLA) for Enterprise Service Levels states that the Service Desk can be reached 24/7 online and provides both local and toll-free phone numbers. This document also indicates that impact and urgency are blended to assign the priority of an incident. A priority of 1-5 is typically assigned. Two exceptions apply:

1. Major Incidents occur when there is a life-threatening event, when multiple agencies cannot conduct core business, and/or when serious political ramifications are likely.
2. Quick Fixes are incidents that can be resolved immediately by ITD's Service Desk. Impact and Urgency are not considered.

Internal processes and logical controls of the Frontrange ITSM system allow for assignments to the ITD Security Section. In the event of a breach incident the Security Incident Response Team (SIRT) would be activated.

EA Standard ST003-04.1 *Incident Prevention, Response, and Notification* provides a coordinated enterprise communication process to address incident prevention, response, and notification. In addition, the Cybersecurity Framework includes a formalized Computer Security Incident Response Policy. This policy was formally approved in April 2014. To ensure employees are appropriately trained on recognizing and reporting computer security incident, ITD includes these topics in the annual required training from SANS and the IRS – Office of Safeguards.

Communicating Changes

All system change requests are submitted to a Change Advisory Board (CAB) for approval to proceed. The CAB is composed of technical members from state agencies as well as staff from ITD's software development, telecommunications, and computer systems divisions. The CAB meets on a weekly basis. To ensure security is appropriately considered for all changes, ITD's Enterprise Information Systems Security Administrator is a voting member of the CAB. Once approved, all scheduled changes are posted to the ITD public website.

When submitting a change request, the project team has the option to "Notify Customers" of the change. If this option is selected, communication occurs inherently when changes reach the "Approved" status. A reminder is also sent three days prior to when a change is scheduled, if the change was approved more than a week before it is scheduled. In addition, communication occurs when the change gets a status of

“Implemented,” which can be done via the ITSM client or by replying to a preformatted email sent to the Responsible Team Member.

A status of “Implemented” shall only be used when the change was successful. A status of “Cancelled” shall be used if the change is withdrawn or rescheduled prior to its scheduled implementation date, and a status of “Backed Out” shall be used when a change was attempted but could not be successfully completed.

Availability

The ITD Contingency Planning Specialist has been established and given responsibility for maintaining the organization’s disaster recovery plan and contingency plan to counteract interruptions to business activities, protect critical information technology infrastructure from the effects of disasters, and ensure timely resumption of the information technology infrastructure and associated services. The ITD COOP is the comprehensive strategy for backup and restoration based on business requirements.

Environmental Controls

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 back-up 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 are allowed access to the room through their key cards.

Disaster Recovery Site

The organization maintains a disaster recovery hot site. 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. ITD also maintains an off-site storage facility which is physically secured through a key card system to access the building and keycards to access the storage area

Data Backup and Recovery

The organization 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. Standard backup configuration allows for a maximum of five different versions of each file to be stored within a 17 day window. A single version of the file will be retained even if it was done outside the 17 day window. Upon deletion from a system, the most recent version of a file is retained for 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/cancelled 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.

Disaster Recovery Testing

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 recovery of their applications.

Processing Integrity

The organization's software development methodology employs Secure Coding Guidelines derived from CERS and Open Web Application Security Project (OWASP) industry best-practice. Application developed by ITD incorporates input-validation, output-encoding, and various threat mitigation strategies to prevent Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), frame-phishing, and SQL-injection. ITD also utilizes IBM Security AppScan as part of ongoing quality assurance efforts.

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).

North Dakota Century Code requires ITD to document information related to service support and delivery, which includes formal complaints regarding dependability, responsiveness, and cost. This information is communicated through an annual report and to agency IT Coordinators through IT Directional Meetings held three times per year.

The organization's Personnel and Administrative Policies and Procedures Manual states that software approved by ITD will be used solely for the following purposes:

- Performing assigned job duties
- Approved personnel training
- Approved administrative functions

The Enterprise SLA states that, "All changes will follow ITD's internal change management process, which is available for review upon request." The internal change management processes have restrictive policy elements surrounding them.

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

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

- | |
|--|
| <ol style="list-style-type: none">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. |
|--|

EA Standard AST002-04.1 – Application Development Methodology
--

Agencies or vendors providing application development shall have an established methodology.
--

EA Standard DIT003-06.1 – Enterprise DIT Security
--

- | |
|--|
| <ol style="list-style-type: none">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 the 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.

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.

EA Standard DIT003-06.1 – Enterprise Database Security

Migrating changes from acceptance test to production requires that the agency who owns the data have a formal acceptance testing and sign off process

Enterprise Architecture does include a process for granting of security waivers. Waivers are granted by the Architecture Review Board. Non-compliance with standards are to be reported to the Office of the State Auditor.

North Dakota Century Code 54-59-19 includes the following statement regarding the duties of the Information Technology Department:

The department shall prepare and present an annual report to the information technology committee. In addition to the presentation of the annual report to the information technology committee, the department shall present a summary of the annual report to the budget section. The report must contain information regarding the delivery of services to agencies, including service dependability, agency complaints, and information technology department responsiveness.

The data/information owner agency must establish document retention standards consistent with the EA Electronic Records Management Guidelines.

The tables below outline Enterprise Architecture (EA) standards that have been established related to the records management by ITD system.

EA Standard DMT003-06.1 – Document Management

Stored records shall be indexed to allow search and retrieval across the enterprise.

EA Standard DIT002-04.1 – Electronic Data Backup

1. Agencies must review their data and identify backup requirements.
2. Backup procedures, frequencies and retention are defined, documented and must adhere to Continuum of Government guidelines.
3. At the completion of each scheduled backup, logs must be checked and verified to ensure successful data backup has occurred.
4. Offsite storage of backup media is required.
5. Backups must be tested periodically to validate recoverability.

Each agency or designated custodian ensures backup of data on a regular basis to minimize data loss.

Central Credit Card Payment Service

ITD provides a central credit card payment service that interfaces to PayPal. This central service is called from applications wanting to process credit cards. The processing of payments via the PayPal Manager allows for tracking of transactions. Additionally, ITD retains a data extract of the transactions. The state agencies that collect payment are responsible for logging/analysis of calls and customer complaints. The processing of payments via the PayPal Manager creates unique transaction identifiers. A centralized logging table contains a unique identifier. ITD retains a separate table with unique identifiers and transaction history; this table is retained indefinitely.

The processing of payments via the PayPal Manager allows for transaction history retention of 12 months. ITD retains a separate table with unique identifiers and transaction history; this table is retained indefinitely.

Confidentiality

The organization's software development methodology employs Secure Coding Guidelines derived from CERS and OWASP industry best-practice. Application developed by ITD incorporates input-validation, output-encoding, and various threat mitigation strategies to prevent Cross-Site Scripting (XSS), (CSRF), frame-phishing, and SQL-injection. ITD also utilizes IBM Security AppScan as part of ongoing quality assurance efforts.

On an annual basis, ITD employees and contractors are required to sign an acknowledgement 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 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.

The Technology Contract Template contains the following statement related to confidential information:

CONTRACTOR acknowledges that any unauthorized publication or disclosure of STATE’s Confidential Information or Proprietary Information to others may cause immediate and irreparable harm to STATE. If CONTRACTOR should publish or disclose such Confidential Information or Proprietary Information without authorization, STATE shall immediately be entitled to injunctive relief or any other remedies to which it is entitled under law or equity without requiring a cure period.

The Technology Contract Template includes the following statement related to reporting of its performance:

Once each calendar month during the term of this Contract, CONTRACTOR shall provide STATE with a written report comparing the actual performance of licensed product and services with the Service Level Requirement. Such report shall also contain such other information with respect to the performance of the licensed product and services as mutually agreed upon by the parties from time to time, and in conformity with reporting CONTRACTOR provides to its other customers utilizing the licensed product and services.

The Technology Contract Template includes the following in the Terms of Contract:

Note: Any exercise of an Extension, Renewal, or Renegotiation requires a written contract amendment identifying the amended terms and conditions. Contract

amendments should be drafted in consultation with an agency's assigned legal counsel.

The Technology Contract Template includes the following in the Terms of Contract:

In view of the fact that it is unknown how long the products and services will be employed by STATE and that STATE will require ongoing maintenance and support of the products for as long as the system is operational, therefore after completion of the initial term of the Contract including any extensions and renewals, STATE and CONTRACTOR may renegotiate the Contract upon mutual agreement of the parties.

The Technology Contract Template has been reviewed by the State of North Dakota – Office of Attorney General.

Complementary User-Entity Controls

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.

- Agency information owners apply account management access rules based on changes in roles or termination of employment. Account management is applied by agency account managers according to information system security requirements and risk assessments. The ITD Cybersecurity Framework includes a section that addresses Establishing or Improving a System Security Plan, which indicates that a system is identified by its mission objectives, scope of dependent systems and assets, regulatory requirements and overall risk tolerance. Roles and responsibilities outlined in the Framework indicate that the owners are responsible for authorizing access privileges and risk profiles and ensuring there are regular reviews and updates to manage changes in risk profiles.
- Agency Directors are responsible for information security in each agency, for reducing risk exposure and for ensuring the agency's information technology practices to not introduce undue risk to the enterprise. The director also is responsible for ensuring compliance with state enterprise security policies and with state and federal regulations.
- 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.

- The data/information owner agency must establish document retention standards consistent with the EA Electronic Records Management Guidelines.
- ITD utilizes an on-line Work Management System where authorized users can request additions, changes or deletes to access rights for systems maintained by ITD. Each user organization designates the individuals who are authorized to request program changes for their agency utilizing WMS.
- 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 for their organizational unit, 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 a state agency or political subdivision.
- 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 the organization is routinely reconciled to relevant user organization control totals

The list of user-organization control considerations presented previously does not represent a comprehensive set of all the controls that may be employed by user organizations. Other controls may be required at user organizations.

ITD's ASSERTION



Information Technology Department

4201 Normandy Street North • Bismarck, ND 58503-1201 • (701) 328-3190

October 3, 2014

Donald LaFleur
IS Audit Manager
ND State Auditor's Office
600 E Boulevard Avenue – Department 117
Bismarck, ND 58505

Dear Mr. LaFleur:

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 of the period May 1, 2014 to October 1, 2014.

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

We welcome the State Auditor's Office to assess the effectiveness of ITD's service operational controls as summarized in the system description.

If you have any questions or comments about this system description please do not hesitate to call me at (701) 328-1001, or contact Dan Sipes, our Deputy CIO and Director, at (701) 328-4317, or through email at dsipes@nd.gov.

Sincerely,

A handwritten signature in blue ink that reads "Mike Ressler". The signature is fluid and cursive.

Mike Ressler
Chief Information Officer
State of North Dakota – Information Technology Department
mressler@nd.gov

Enclosure

State of North Dakota
www.nd.gov/itd



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

INDEPENDENT AUDITOR'S REPORT

The Honorable Jack Dalrymple, Governor
Members of the North Dakota Legislative Assembly
Mike Ressler, Chief Information Officer

Scope

We have examined the attached description titled "Description of Information Technology Department Services for the period April 1, 2014 to October 1, 2014" and the suitability of the design and operating effectiveness of the controls to meet the criteria for security, availability, processing integrity, and confidentiality principles set forth in TSP section 100 *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* throughout the period April 1, 2014 to October 1, 2014 and the standards applicable to attestation engagements contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Information Technology Department's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

Service Organization's Responsibilities

The Information Technology Department has provided the attached assertion titled "ITD's Assertion Regarding its Description of Controls throughout the period April 1, 2014 to October 1, 2014" which is based on the criteria identified in management's assertion. The Information Technology Department is responsible for 1) preparing the description and assertion; 2) the completeness, accuracy, and method of presentation of both the description and assertion; 3) providing the services covered by the description; 4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and 5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in the Information Technology Department's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants and the standards applicable to attestation engagements contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, 1) the description is fairly presented on the description criteria, and 2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period April 1, 2014 to October 1, 2014.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a services organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a services organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in the Information Technology Department's assertion and the applicable trust services criteria

- a) The description fairly presents the system that was designed and implemented throughout the period April 1, 2014 to October 1, 2014.
- b) The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period April 1, 2014 to October 1, 2014, and user entities applied the complementary user-entity controls contemplated in the

design of the Information Technology Department's controls through-out the period April 1, 2014 to October 1, 2014.

- c) The controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period April 1, 2014 to October 1, 2014.

Description of Tests of Controls

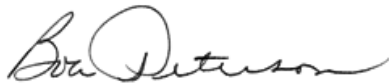
The specific controls we tested and the nature, timing, and results of our tests are presented in the section of our report titled "Description of Tests of Controls and Results Thereof."

Restricted Use

This report and the description of tests of controls and results thereof are intended solely for the information and use of the Information Technology Department; user entities of the Information Technology Department; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risk that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

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



Robert R. Peterson
State Auditor



Edwin J. Nagel, Jr., CPA
Director

Bismarck, North Dakota

May 6, 2015

DESCRIPTION OF TESTS OF CONTROLS AND RESULTS THEREOF

Security Principle and Criteria Table

The system is protected against unauthorized access (both physical and logical)

Policies

The entity defines and documents its policies for the security of its system.

- 1.1 The entity's security policies are established and periodically reviewed and approved by a designated individual or group.
- 1.2 The entity's security policies include, but may not be limited to, the following matters:
- a. Identifying and documenting the security requirements of authorized users
 - b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements
 - c. Assessing risks on a periodic basis
 - d. Preventing unauthorized access
 - e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access
 - f. Assigning responsibility and accountability for system security
 - g. Assigning responsibility and accountability for system changes and maintenance
 - h. Testing, evaluating, and authorizing system components before implementation
 - i. Addressing how complaints and requests relating to security issues are resolved
 - j. Identifying and mitigating security breaches and other incidents
 - k. Providing for training and other resources to support its system security policies
 - l. Providing for the handling of exceptions and situations not specifically addressed in its system security policies
 - m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements
 - n. Providing for sharing information with third parties

1.3 Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned.

Communications

The entity communicates its defined system security policies to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

2.2 The security obligations of users and the entity's security commitments to users are communicated to authorized users.

2.3 Responsibility and accountability for the entity's system security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.

2.4 The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.

2.5 Changes that may affect system security are communicated to management and users who will be affected.

Procedures

The entity placed in operation procedures to achieve its documented system security objectives in accordance with its defined policies.

3.1 Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.

3.2 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

a. Logical access security measures to restrict access to information resources not deemed to be public.

b. Identification and authentication of users.

c. Registration and authorization of new users.

d. The process to make changes and updates to user profiles.

e. Distribution of output restricted to authorized users.

f. Restriction of access to offline storage, backup data, systems, and media.

g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

3.3 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

3.4 Procedures exist to protect against unauthorized access to system resources.

3.5 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.

3.6 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

Criteria related to execution and incident management used to achieve objectives

3.7 Procedures exist to identify, report, and act upon system security breaches and other incidents.

Criteria related to the system components used to achieve the objectives

3.8 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary

3.9 Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.10 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.

3.11 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.

Change Management-related criteria applicable to the system's security

3.12 Procedures exist to maintain system components, including configurations consistent with the defined system security policies.

3.13 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

3.14 Procedures exist to provide that emergency changes are documented and authorized timely.

Monitoring

The entity monitors the system and takes action to maintain compliance with its defined system security policies.

4.1 The entity's system security is periodically reviewed and compared with the defined system security policies.

4.2 There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.

4.3 Environmental, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment.

Test of Security Controls

ITD Control	Test of Control	Results
Responsibility for Security		
The CIO has the authority and responsibility for information systems security surrounding State of North Dakota information technology assets.	Reviewed ND Century Code for responsibility of CIO	No exceptions noted
The ITD Security Section has primary responsibility to administer and monitor the identity management repositories.	Reviewed the administration of all identity management repositories with ITD	No exceptions noted
Security Policy		
The ITD Cybersecurity Framework policies are developed and maintained by the ITD Security Section by directive of the State of North Dakota’s CIO.	Reviewed the Cybersecurity Framework roles and responsibilities to ensure the security section had these responsibilities.	No exceptions noted
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.	Reviewed the Cybersecurity Framework for these items.	No exceptions noted
Policies in the Cybersecurity Framework are reviewed by the ITD Virtual Security Team and approved by the CIO.	Discussed the process for developing policies in the Cybersecurity Framework with ITD.	No exceptions noted
The Cybersecurity Framework policies are reviewed on an annual basis.	The Cybersecurity Framework was developed in April, 2014. No review was needed yet.	No exceptions noted
The ITD Cybersecurity Framework includes a section that addresses Establishing or Improving a System Security Plan, which indicates that a system is identified by its mission objectives, scope of dependent systems and assets, regulatory requirements and overall risk tolerance.	Reviewed the Cybersecurity Framework for this section.	No exceptions noted
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.	Reviewed the procedures for the risk assessment. This assessment is based on agency applications. While it does a great job of assessing risk where used ITD lacks a comprehensive risk	No formal risk assessment

ITD Control	Test of Control	Results
	assessment for their operations.	
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.	Reviewed these policies to ensure they were in place.	No exceptions noted
<p>In addition to the EA standards and the ITD Cybersecurity Framework, ITD’s Administrative Policies and Procedures Manual references administrative policies that pertain to the following information security topics:</p> <ul style="list-style-type: none"> • Background Checks • Confidentiality • Acceptable Use of Electronic Communication Devices • Requests for Telephone Records • Requests for E-Mail Records • Microcomputer Usage • Workstation Protection • Smartphone Devices • Physical Security 	Reviewed ITD’s Administrative Policies and Procedures to ensure the policies were in place.	No exceptions noted
All employees complete either the ITD Security Awareness training or an agency security awareness program within the first three days of being granted access to the state government network.	We tested all ITD employees to ensure they had completed the Security Awareness Training.	No exceptions noted
IT Standards are reviewed annually and documented on the standard with a “Last Reviewed” date.	Re reviewed all the standards for last reviewed date.	Only 6 of 48 standards were reviewed in last year.
Communication of Security Policy		
Upon hire, and on an annual basis, ITD employees are required to sign an Acknowledgment of Secrecy Provision to ensure they are aware of the	We tested all ITD employees to ensure they had signed the acknowledgement form.	No exceptions noted

ITD Control	Test of Control	Results
confidentiality requirements of the data they handle.		
On an annual basis, both ITD employees and contractors are required to sign an acknowledgement document stating that they have read and will comply with the organization’s policies and procedures, including the ITD Cybersecurity Framework policies.	We tested all ITD employees to ensure they had signed the acknowledgement form.	No exceptions noted
All state security standards and policies are published on the North Dakota Enterprise Architecture web page, and access to modify these web pages is restricted to authorized users.	We reviewed the web page and the access rights to it.	No exceptions noted
Active Directory Procedures		
ITD has established Active Directory as the primary identity management repository providing users with a single set of credentials for network and application sign-on.	Reviewed the IT Standard that establishes Active Directory as primary identity management repository.	No exceptions noted
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.	Reviewed the IT Standard that establishes Active Directory as primary identity management repository.	No exceptions noted
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.	Reviewed the IT Standard that establishes Active Directory as primary identity management repository.	No exceptions noted
All servers and workstations administered by ITD require users to logon prior to being granted access to system resources.	Reviewed the Active Directory domain policy.	No exceptions noted
Unique user IDs and passwords are assigned to each user	Reviewed the IT Standard that establishes rules for accessing systems.	No exceptions noted

ITD Control	Test of Control	Results
Staff that require Administrator access are issued a separate set of credentials to administer IT systems.	Reviewed these accounts to ensure they existed and were necessary.	No exceptions noted
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.		
ITD automatically disables accounts after 90 days of inactivity.	Reviewed the process for identifying and alerting ITD to accounts not used in 90 days and how they are disabled.	No exceptions noted
To ensure security and confidentiality, all Active Directory login credentials are encrypted during transmission.	Reviewed the setup of Active Directory with ITD.	No exceptions noted
Physical Security Procedures		
ITD resides within a locked facility	Walkthrough of ITD facilities, noted the doors required badges to enter. We also reviewed door logs for the main data center and secondary data center.	No exceptions noted
<p>"The ITD Security Section will coordinate with the entities identified below to restrict physical access to ITD premises. The ITD Security Section will coordinate with ITD Division Directors to review access restrictions on an annual basis.</p> <ul style="list-style-type: none"> • ND Highway Patrol • Dakota Carrier Network Facilities Staff • ND Association of Counties Facilities Staff • Montana Dakota Utilities Facilities Staff • Northbrook Mall Management Facilities Staff 	Discussed the coordination with ITD. We noted that since moving to their new facility ITD no longer has staff at ND Association of Counties or Northbrook Mall. We reviewed door access logs from Highway Patrol.	No exceptions noted

ITD Control	Test of Control	Results
ITD maintains a video surveillance system for critical ITD entry points.	Reviewed video surveillance with ITD Security and noted the systems during our walkthrough.	No exceptions noted
ITD receives usage reports from the Highway Patrol who manages the door access system.	Received the door logs from ITD.	No exceptions noted
ITD utilizes identification badges to grant access to restricted areas and to ensure that only authorized personnel are in restricted areas.	Selected three critical doors and tested the logs from Highway Patrol against the door authorization list for a sample of weeks.	No exceptions noted
Visitor logs serve as audit records for physical visit reconstruction.	Noted in our visits and walkthrough that we were required to sign visitor logs.	No exceptions noted
Visitors are not permitted unescorted access while on ITD’s data center premises.	No policy was found to support this.	No Policy
Contractors who have had security background checks are allowed unescorted access to ITD premises specific to the project they are working on.	During our tests of door logs we noted two contractors who had accessed the data center. Both were reviewed for background checks.	No exceptions noted
Network Firewall Procedures		
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.	Reviewed the process for submitting and approving service requests for firewalls.	No exceptions noted
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. ITD's policy over firewall control is to lock down all access and open only authorized ports and hosts that require access.	During review of the approval process for service requests for firewalls it was noted that no periodic review of allowed ports and services is done.	No periodic review of authorized ports and services.

ITD Control	Test of Control	Results
ITD utilizes the state Virtual Private Network (VPN) for all remote access connections other than those that are externally available outside the state firewall.	Reviewed the IT Standard for remote access and noted it requires the VPN be used.	No exceptions noted
ITD utilizes a content filtering appliance to filter access to Internet sites and materials it deems inappropriate for business use.	Reviewed filtering with ITD, they utilize a commercial filtering product to accomplish this.	No exceptions noted
Security Incident Response Procedures		
The organization has developed a formal Security Incident Response Team Policy.	Reviewed the Security Incident Response Team policy.	No exceptions noted
The ITD Security Incident Response Team is facilitated by the ITD Security Section.	Reviewed the Security Incident Response Team policy and discussed Incident Response with ITD Security Section.	No exceptions noted
The ITD Security Incident Response Team is facilitated by the ITD Security Section and is responsible for ensuring that ITD responds to security incidents in a manner that optimizes inter-divisional communication and minimizes the impact of a given incident.	Reviewed the Security Incident Response Team policy and discussed Incident Response with ITD Security Section.	No exceptions noted
ITD maintains an Intrusion Detection System (IDS) to monitor for network or host anomalies and known attack signatures.	Reviewed the Security Information and Event Management (SIEM).	No exceptions noted
Firewall activity logs are integrated with ITD’s security information and event manager which looks for repeated attempts to break one or multiple firewalls within the network.	Discussed firewall logs and how they are integrated and used by the Security Information and Event Management (SIEM).	No exceptions noted
ITD maintains a Security Information Event Management (SIEM) system to store centralized log information.	Reviewed the Security Information and Event Management (SIEM) with ITD Security and reviewed what	No exceptions noted

ITD Control	Test of Control	Results
	logs were being integrated with it.	
Logs are aggregated in the SIEM and offenses are reviewed on a daily basis.	Reviewed reports and triggers used in the Security Information and Event Management (SIEM).	No exceptions noted
Blocking all traffic from nation states that present sustained and systemic risk to the health of STAGEnet	Reviewed the settings blocking the nation states.	No exceptions noted
Vulnerability Assessments		
ITD performs regular vulnerability assessments on its computing and network infrastructure to proactively identify systems with high risk profiles.	Reviewed vulnerability scanning process with ITD Security	No exceptions noted
The ITD Security Section and Quality Assurance team within the Software Development Division conducts regularly scheduled vulnerability scans to pro-actively identify potential risks to ITD hosted web applications.	This process is new and has not been performed on more than a couple applications.	New process, no opinion can be expressed in this audit.
Hiring and Training Employees		
ITD uses the ND Human Resource Management Services job classifications for all positions.	Reviewed classification system with ITD. Tested all ITD employees to ensure classification system was used.	No exceptions noted
Personnel training is accomplished through supervised on-the-job training, outside seminars, and in-house classes.	Reviewed training procedures with ITD. Tested 20 employees to ensure they had adequate training.	No exceptions noted
Management Controls and Monitoring		
ITD’s 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.	Reviewed process for formulating, implementing, and monitoring controls with ITD.	No exceptions noted
Management and supervisory personnel are responsible for monitoring the quality of internal control	Reviewed ITD’s management and staff meetings to see that controls were discussed,	No exceptions noted

ITD Control	Test of Control	Results
performance as a routine part of their activities.	updated and communicated to staff.	
Each division of ITD has implemented performance measures that measure the results of various processes involved in running the data center and provided the associated services to customers.	Reviewed performance measures with ITD. Reviewed meeting agenda to see that they were discussed at management meetings.	No exceptions noted
Key performance indicators are reviewed daily, weekly or monthly by appropriate levels of management, and action is taken as necessary.	Reviewed performance measures with ITD. Reviewed meeting agenda to see that they were discussed at management meetings.	No exceptions noted

Recommendations related to Security

ITD lacks a formal risk assessment framework

While critical business processes have been identified, there is not a systematic approach to identifying, assessing, and mitigating or accepting risks to those business processes. Without a formal risk assessment process management may not have adequate information to make sound decisions in the use of assets to mitigate risk. While ITD does assess risks they have not yet established a formal risk assessment process. Management should ensure that reassessments occur and that risk assessment information is updated with results of audits, inspections and identified incidents. Such a framework should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level.

Recommendation:

We recommend the Information Technology Department develop a systematic risk assessment framework.

ITD's Response:

ITD agrees with the recommendation and plans to develop a formal risk assessment process as part of our Cybersecurity Framework. ITD does have dedicated security staff who evaluate risk related to enterprise security issues and coordinate application specific risk assessments. However, we do agree that there is value in formalizing an overall risk assessment process.

No periodic review of enabled ports/services is being done

A review isn't being done on services and ports that are enabled. Unnecessary services and ports are potential targets for hackers. ITD has not developed a process for reviewing open ports/services after initially authorizing them. ITD states their objective is to ensure they have procedures in place to ensure they are only running services and opening ports necessary.

Recommendation:

We recommend ITD do a periodic review of all their enabled services and ports to see if they are still being used or needed

ITD's Response:

ITD agrees with the recommendation and plans to add formal processes around periodic reviews of system configurations. ITD does lock down all services and ports when initially configuring systems and does perform ad hoc reviews as part of on-going tuning and/or trouble-shooting processes. However, we do agree that there is value in formalizing our practices in this area.

No policy requiring visitors to be escorted in the data centers

ITD's Personnel and Administrative Policies and Procedures Manual currently does not indicate when visitors are to be escorted. Employees may not be aware and allow visitors to be unescorted in these areas. ITD's policies and procedures manual states visitors be required to sign in/out but does not specifically describe escorted access. ITD's description of controls states visitors are not permitted unescorted access while on ITD's data center premises.

Recommendation:

We Recommend the Information Technology Department update current policy to define escorted access to ITD facilities.

ITD's Response:

ITD agrees with the recommendation and will develop a formal policy that documents the current practice of visitor escort in the data centers.

Enterprise Architecture Standards not reviewed according to Description of Controls

Only 6 of 32 Enterprise Architecture Standards were reviewed within the year. Standards in time can become outdated due to Technology moving at incredible rates. It appears ITD is not reviewing their EA standards according to their description they gave us which states Enterprise Architecture Standards are reviewed annually.

Recommendation:

We Recommend the Information Technology Department do a yearly review of their Enterprise Architecture Standards.

ITD's Response:

ITD agrees with the recommendation and this is the intent of the agencies participating in the Enterprise Architecture process. While the Enterprise Architecture web site has not been updated with the most current review date, 17 out of the 32 standards have been reviewed within the last year and progress continues on the remaining standards.

Availability Principle and Criteria Table

The system is available for operation and use as committed or agreed.

Policies:

The entity defines and documents its policies for the availability of its system.

1.1 The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.

1.2 The entity's system availability and related security policies include, but may not be limited to, the following matters:

a. Identifying and documenting the system availability and related security requirements of authorized users.

b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements

c. Assessing risks on a periodic basis

d. Preventing unauthorized access.

e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access.

f. Assigning responsibility and accountability for system availability and related security.

g. Assigning responsibility and accountability for system changes and maintenance.

h. Testing, evaluating, and authorizing system components before implementation.

i. Addressing how complaints and requests relating to system availability and related security issues are resolved.

j. Identifying and mitigating system availability and related security breaches and other incidents.

k. Providing for training and other resources to support its system availability and related security policies.

l. Providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies.

m. Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.

n. Recovering and continuing service in accordance with documented customer commitments or other agreements.

o. Monitoring system capacity to achieve customer commitments or other agreements regarding availability

1.3 Responsibility and accountability for developing and maintaining the entity's system availability and related security policies, and changes and updates to those policies, are assigned.

Communications:

The entity communicates the defined system availability policies to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

2.2 The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.

2.3 Responsibility and accountability for the entity's system availability and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.

2.4 The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.

2.5 Changes that may affect system availability and system security are communicated to management and users who will be affected.

Procedures:

The entity placed in operation procedures to achieve its documented system availability objectives in accordance with its defined policies.

3.1 Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.

3.2 Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.

3.3 Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.

3.4 Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.

Security-related criteria relevant to the system's availability

3.5 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

- a. Logical access security measures to restrict access to information resources not deemed to be public.
- b. Identification and authentication of users.
- c. Registration and authorization of new users.
- d. The process to make changes and updates to user profiles.
- e. Restriction of access to offline storage, backup data, systems and media.
- f. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

3.6 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

3.7 Procedures exist to protect against unauthorized access to system resources.

3.8 Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.

3.9 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

Criteria related to execution and incident management used to achieve objectives

3.10 Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.

Criteria related to the system components used to achieve the objectives

3.11 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.

3.12 Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.13 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability and related security policies.

3.14 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources to fulfill their responsibilities.

Change management-related criteria applicable to the system’s availability

3.15 Procedures exist to maintain system components, including configurations consistent with the defined system availability and related security policies.

3.16 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

3.17 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).

Monitoring:

The entity monitors the system and takes action to maintain compliance with its defined system availability policies.

4.1 The entity’s system availability and security performance is periodically reviewed and compared with the defined system availability and related security policies.

4.2 There is a process to identify and address potential impairments to the entity’s ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.

4.3 Environmental, regulatory, and technological changes are monitored, and their effect on system availability and security is assessed on a timely basis; policies are updated for that assessment.

Test of Security Controls

ITD Control	Test of Control	Results
Responsibility for Availability		
The ITD Contingency Planning Specialist has been established and given responsibility for maintaining the organization’s disaster recovery plan and contingency plan to counteract interruptions to business activities, protect critical information technology infrastructure from the effects of disasters, and ensure timely resumption of the information technology infrastructure and associated services.	Reviewed the job description and Disaster Recovery Plan for responsibilities.	No exceptions noted
Environmental Controls		
ITD's Data Center environmental controls include fire suppression, raised	Performed a walk-through of the data center and reviewed	No exceptions noted

ITD Control	Test of Control	Results
floors, water detectors, smoke alarms and air conditioning units.	environmental protections with ITD	
The Facility Management Division provides a UPS for back-up power and power regulation, and a generator for extended power loss.	Performed a walk-through of UPS room and reviewed the operation with Facilities Management. Reviewed inspection and maintenance reports on the UPS	No exceptions noted
Contingency Planning		
The organization maintains a disaster recovery hot site.	Performed a walk-through of hot site. Reviewed consultant study of the adequacy of the hot site location.	No exceptions noted
ITD performs regular testing its Disaster Recovery Plan at the hot site facility.	Reviewed three tests done in our audit time frame and the results documented.	No exceptions noted
Requirements for backup of systems is primarily covered by the Enterprise Service Level Agreement and thereafter the Hosting Service Level Agreement.	Reviewed the Enterprise service level agreement and Hosting service level agreement for backup requirements.	No exceptions noted
ITD also maintains an off-site storage facility which is physically secured through a key card system to access the building and keycards to access the storage area	Performed a walk-through of off-site storage facility.	No exceptions noted
Media-storage areas (key-locked cabinets, tape vaults, etc.) are doubly secured via badge-reader and traditional key-lock countermeasures.	Performed a walk-through of media storage facilities.	No exceptions noted
Change Management		
Major changes or change requests that require down time are submitted to a Change Advisory Board (CAB). These changes must be approved by the CAB prior to implementation.	Reviewed policies and procedures for submitting changes to the Change Advisory Board.	No exceptions noted
When submitting a change request, the project team has the option to “Notify Customers” of the change. If this option is selected, communication occurs inherently when changes reach the “Approved” status. A reminder is also	Reviewed notification system with ITD and process for marking changes so customers are notified.	No exceptions noted

ITD Control	Test of Control	Results
<p>sent three days prior to when a change is scheduled, if the change was approved more than a week before it is scheduled. In addition, communication occurs when the change gets a status of “Implemented,” which can be done via the ITSM client or by replying to a preformatted email sent to the Responsible Team Member.</p>		
<p>Once approved, all scheduled changes are posted to the ITD public website.</p>	<p>Reviewed website to see scheduled changes were posted.</p>	<p>No exceptions noted</p>
<p>Divisional staff may expedite the voting process, and assume full responsibility, by changing the status to “Approved” at any time. When possible divisions are encouraged to use a status of “Accepted Divisionally” for a short period of time to trigger the escalation process which allows for additional internal input and discussion.</p>	<p>Reviewed procedures for emergency changes with ITD.</p>	<p>No exceptions noted</p>
<p>Emergency changes must be logged.</p>	<p>Reviewed process for logging and accepting emergency changes.</p>	<p>No exceptions noted</p>
<p>Monitoring System Performance</p>		
<p>ITD has implemented various infrastructure monitoring solutions to monitor performance characteristics (utilization, capacity, response time, usage, and resource availability).</p>	<p>Reviewed system used to monitor ITD’s infrastructure, reviewed current reports and thresholds set within the system.</p>	<p>No exceptions noted</p>
<p>Virus and Malware Prevention Procedures</p>		
<p>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.</p>	<p>Reviewed the policy.</p>	<p>No exceptions noted</p>
<p>ITD uses virus and spyware detection programs on all workstations and most servers.</p>	<p>Selected a sample of nine employees and four servers to ensure virus and spyware</p>	<p>No exceptions noted</p>

ITD Control	Test of Control	Results
	detections programs were present.	
In addition ITD deploys additional appliances at key locations on the network to monitor virus activity.	Reviewed network diagram with ITD to see where the appliances where installed.	No exceptions noted
All incoming files, including email, are scanned in real-time for malware.	Reviewed ways files come into ITD and how the scanning occurs.	No exceptions noted
In addition, all files are scanned for malware on a weekly basis.	Reviewed sample of nine employees and four servers to ensure weekly scans were occurring.	No exceptions noted
Service Desk		
ITD's Customer Service Division operates a help desk	Reviewed the help desk function with ITD.	No exceptions noted
ITD's Customer Service Division provides a central repository for customers to report problems, ask questions, request information, and receive resolutions and answers.	Reviewed the service level agreements for the help desk.	No exceptions noted
Communication with Users		
Quarterly IT Directional meetings to inform entities on current initiatives and issues.	Reviewed minutes from meetings on ITD’s web site.	No exceptions noted
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.	Reviewed the annual report on ITD’s web site.	No exceptions noted
ITD conducts an annual customer survey to ensure the department is meeting customers’ expectations.	Reviewed results from last customer survey.	No exceptions noted
Establish Services and Boundaries		
A description of the North Dakota Statewide Technology Access for Government and Education network (STAGEnet) is maintained and made	Reviewed the website and description.	No exceptions noted

ITD Control	Test of Control	Results
available to the public at http://stagenet.nd.gov .		
The department is responsible for all wide area network services planning, selection, implementation and operation for all state agencies, including institutions under the control of the State Board of Higher Education, counties, cities, and school districts.	Reviewed the website and description.	No exceptions noted

Processing Integrity Principle and Criteria Table

System processing is complete, accurate, timely, and authorized.

Policies:

The entity defines and documents its policies for the processing integrity of its system.

1.1 The entity's processing integrity and related security policies are established and periodically reviewed and approved by a designated individual or group.

1.2 The entity's system processing integrity and related security policies include, but may not be limited to, the following matters:

a. Identifying and documenting the system processing integrity and related security requirements of authorized users

b. Classifying data based on their criticality and sensitivity; that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements

c. Assessing risks on a periodic basis

d. Preventing unauthorized access

e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access

f. Assigning responsibility and accountability for system processing integrity and related security

g. Assigning responsibility and accountability for system changes and maintenance

h. Testing, evaluating, and authorizing system components before implementation

i. Addressing how complaints and requests relating to system processing integrity and related security issues are resolved

j. Identifying and mitigating errors and omissions and other system processing integrity and related security breaches and other incidents

k. Providing for training and other resources to support its system processing integrity and related system security policies

l. Providing for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies

m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements

1.3 Responsibility and accountability for developing and maintaining entity's system processing integrity and related system security policies; changes, updates, and exceptions to those policies are assigned.

Communications:

The entity communicates its documented system processing integrity policies to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

If the system is an e-commerce system, additional information provided on its website includes, but may not be limited to, the following matters:

a. Descriptive information about the nature of the goods or services that will be provided, including, where appropriate,

i. condition of goods (whether they are new, used, or reconditioned).

ii. description of services (or service contract).

iii. sources of information (where it was obtained and how it was compiled).

b. The terms and conditions by which it conducts its e-commerce transactions including, but not limited to, the following matters:

i. Time frame for completion of transactions (transaction means fulfillment of orders where goods are being sold and delivery of service where a service is being provided)

ii. Time frame and process for informing customers of exceptions to normal processing of orders or service requests

iii. Normal method of delivery of goods or services, including customer options, where applicable

iv. Payment terms, including customer options, if any

v. Electronic settlement practices and related charges to customers

vi. How customers may cancel recurring charges, if any

vii. Product return policies and limited liability, where applicable

c. Where customers can obtain warranty, repair service, and support related to the goods and services purchased on its website.

d. Procedures for resolution of issues regarding processing integrity. These may relate to any part of a customer's e-commerce transaction, including complaints related to the

quality of services and products, accuracy, completeness, and the consequences for failure to resolve such complaints.

2.2 The processing integrity and related security obligations of users and the entity's processing integrity and related security commitments to users are communicated to authorized users.

2.3 Responsibility and accountability for the entity's system processing integrity and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.

2.4 The process for obtaining support and informing the entity about system processing integrity issues, errors and omissions, and breaches of systems security and for submitting complaints is communicated to authorized users.

2.5 Changes that may affect system processing integrity and system security are communicated to management and users who will be affected.

Procedures:

The entity placed in operation procedures to achieve its documented system processing integrity objectives in accordance with its defined policies.

3.1 Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair processing integrity commitments and (2) assess the risks associated with the identified threats.

Security-related criteria relevant to the system's processing integrity

3.6 Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:

- a. Logical access security measures to access information not deemed to be public
- b. Identification and authentication of authorized users
- c. Registration and authorization of new users
- d. The process to make changes and updates to user profiles
- e. Distribution of output restricted to authorized users
- f. Restriction of access to offline storage, backup data, systems, and media
- g. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)

3.7 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, offline storage media, backup media and systems, and other system components such as firewalls, routers, and servers.

3.8 Procedures exist to protect against unauthorized access to system resources.

3.9 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.

3.10 Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.

Criteria related to execution and incident management used to achieve objectives

3.11 Procedures exist to identify, report, and act upon system processing integrity issues and related security breaches and other incidents.

Criteria related to the system components used to achieve the objectives

3.12 Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary

3.13 Procedures exist to provide that issues of noncompliance with system processing integrity and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.14 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.

3.15 Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting processing integrity and security have qualifications and resources to fulfill their responsibilities.

Change management-related criteria applicable to the system's processing integrity

3.16 Procedures exist to maintain system components, including configurations consistent with the defined system processing integrity and related security policies.

3.17 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

3.18 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).

Availability-related criteria applicable to the system's processing integrity

3.19 Procedures exist to protect the system against potential risks (for example, environmental risks, natural disasters, and routine operational errors and omissions) that might impair system processing integrity.

3.20 Procedures exist to provide for restoration and disaster recovery consistent with the entity's defined processing integrity policies.

3.21 Procedures exist to provide for the completeness, accuracy, and timeliness of backup data and systems.

Monitoring:

The entity monitors the system and takes action to maintain compliance with the defined system processing integrity policies.

4.1 System processing integrity and security performance are periodically reviewed and compared with the defined system processing integrity and related security policies.

4.2 There is a process to identify and address potential impairments to the entity’s ongoing ability to achieve its objectives in accordance with its defined system processing integrity and related security policies.

4.3 Environmental, regulatory, and technological changes are monitored, their impact on system processing integrity and security is assessed on a timely basis, and policies are updated for that assessment.

Test of Security Controls

ITD Control	Test of Control	Results
Custodian of User Data		
ITD will only grant access to information based upon authorization requests from Agency IT Coordinators.	Reviewed procedures for granting access and tested one week of granted access to ensure the request came from a user agency.	No exceptions noted

Confidentiality Principle and Criteria Table

Information designated as confidential is protected by the system as committed or agreed.

Policies:

The entity defines and documents its policies related to the system protecting confidential information, as committed or agreed.

1.1 The entity’s system confidentiality and related security policies are established and periodically reviewed and approved by a designated individual or group.

1.2 The entity's policies related to the system’s protection of confidential information and security include, but are not limited to, the following matters:

- a. Identifying and documenting the confidentiality and related security requirements of authorized users
- b. Classifying data based on its criticality and sensitivity that is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements

- c. Assessing risk on a periodic basis
- d. Preventing unauthorized access
- e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access
- f. Assigning responsibility and accountability for confidentiality and related security
- g. Assigning responsibility and accountability for system changes and maintenance
- h. Testing, evaluating, and authorizing system components before implementation
- i. Addressing how complaints and requests relating to confidentiality and related security issues are resolved
- j. Handling confidentiality and related security breaches and other incidents
- k. Providing for training and other resources to support its system confidentiality and related security policies
- l. Providing for the handling of exceptions and situations not specifically addressed in its system confidentiality and related security policies
- m. Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements
- n. Sharing information with third parties

1.3 Responsibility and accountability for developing and maintaining the entity's system confidentiality and related security policies, and changes and updates to those policies, are assigned.

Communications:

The entity communicates its defined policies related to the system's protection of confidential information to responsible parties and authorized users.

2.1 The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.

2.2 The system confidentiality and related security obligations of users and the entity's confidentiality and related security commitments to users are communicated to authorized users before the confidential information is provided. This communication includes, but is not limited to, the following matters:

- a. How information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, back-up, and distribution or transmission of confidential information.
- b. How access to confidential information is authorized and how such authorization is rescinded.
- c. How confidential information is used.
- d. How confidential information is shared.
- e. If information is provided to third parties, disclosures include any limitations on reliance on the third party's confidentiality practices and controls. Lack of such disclosure indicates that the entity is relying on the third party's confidentiality practices and controls that meet or exceed those of the entity.
- f. Practices to comply with applicable laws and regulations addressing confidentiality.

2.3 Responsibility and accountability for the entity's system confidentiality and related security policies and changes and updates to those policies are communicated to entity personnel responsible for implementing them.

2.4 The process for informing the entity about breaches of confidentiality and system security and for submitting complaints is communicated to authorized users.

2.5 Changes that may affect confidentiality and system security are communicated to management and users who will be affected.

Procedures:

The entity placed in operation procedures to achieve its documented system confidentiality objectives in accordance with its defined policies.

3.1 Procedures exist to (1) identify potential threats of disruptions to systems operations that would impair system confidentiality commitments and (2) assess the risks associated with the identified threats.

3.2 The system procedures related to confidentiality of inputs are consistent with the documented confidentiality policies.

3.3 The system procedures related to confidentiality of data processing are consistent with the documented confidentiality policies.

3.4 The system procedures related to confidentiality of outputs are consistent with the documented confidentiality policies.

3.5 The system procedures provide that confidential information is disclosed to parties only in accordance with the entity's defined confidentiality and related security policies.

3.6 The entity has procedures to obtain assurance or representation that the confidentiality policies of third parties to whom information is transferred and upon which the entity relies are in conformity with the entity's defined system confidentiality and related security policies and that the third party is in compliance with its policies.

3.7 In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, the entity has procedures to protect confidential information in accordance with the system confidentiality practices in place when such information was received, or obtains customer consent to follow the new confidentiality practice with respect to the customer's confidential information.

System security-related criteria relevant to confidentiality

3.8 Procedures exist to restrict logical access to the system and the confidential information resources maintained in the system including, but not limited to, the following matters:

- a. Logical access security measures to restrict access to information resources not deemed to be public
- b. Identification and authentication of all users.
- c. Registration and authorization of new users.
- d. The process to make changes and updates to user profiles.
- e. Procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.
- f. Procedures to limit access to confidential information to only authorized employees based upon their assigned roles and responsibilities.
- g. Distribution of output containing confidential information restricted to authorized users.
- h. Restriction of access to offline storage, backup data, systems, and media.
- i. Restriction of access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls).

3.9 Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

3.10 Procedures exist to protect against unauthorized access to system resources.

3.11 Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.

3.12 Encryption or other equivalent security techniques are used to protect transmissions of user authentication and other confidential information passed over the Internet or other public networks.

Criteria related to execution and incident management used to achieve the objectives

3.13 Procedures exist to identify, report, and act upon system confidentiality and security breaches and other incidents.

Criteria related to the system components used to achieve the objectives

3.14 Procedures exist to provide that system data are classified in accordance with the defined confidentiality and related security policies.

3.15 Procedures exist to provide that issues of noncompliance with defined confidentiality and related security policies are promptly addressed and that corrective measures are taken on a timely basis.

3.16 Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined confidentiality and related security policies.

3.17 Procedures exist to help ensure that personnel responsible for the design, development, implementation, and operation of systems affecting confidentiality and security have the qualifications and resources to fulfill their responsibilities.

Change management-related criteria relevant to confidentiality

3.18 Procedures exist to maintain system components, including configurations consistent with the defined system confidentiality and related security policies.

3.19 Procedures exist to provide that only authorized, tested, and documented changes are made to the system.

3.20 Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).

3.21 Procedures exist to provide that confidential information is protected during the system development, testing, and change processes in accordance with defined system confidentiality and related security policies.

Monitoring:

The entity monitors the system and takes action to maintain compliance with its defined confidentiality policies.

4.1 The entity's system confidentiality and security performance is periodically reviewed and compared with the defined system confidentiality and related security policies.

4.2 There is a process to identify and address potential impairments to the entity’s ongoing ability to achieve its objectives in accordance with its system confidentiality and related security policies.

4.3 Environmental, regulatory, and technological changes are monitored, and their impact on system confidentiality and security is assessed on a timely basis. System confidentiality policies and procedures are updated for such changes as required.

Test of Security Controls

ITD Control	Test of Control	Results
Ensuring Confidentiality of Data		
<p>The Technology Contract Template contains the following statement related to confidential information: CONTRACTOR acknowledges that any unauthorized publication or disclosure of STATE’s Confidential Information or Proprietary Information to others may cause immediate and irreparable harm to STATE. If CONTRACTOR should publish or disclose such Confidential Information or Proprietary Information without authorization, STATE shall immediately be entitled to injunctive relief or any other remedies to which it is entitled under law or equity without requiring a cure period.</p>	<p>Reviewed the template and recent contracts to ensure the confidentiality provision is in place. All contracts issued in the audit period were tested (nine contracts).</p>	<p>No exceptions noted</p>
<p>To ensure employees are appropriate trained on recognizing and reporting computer security incident, ITD includes these topics in the annual required training from SANS and the IRS – Office of Safeguards.</p>	<p>Tested all ITD employees to ensure they had received training.</p>	<p>No exceptions noted</p>
<p>Procedures have been implemented for sharing information with the Social Security Administration, which is accomplished through Information Exchange Agreements (IEA).</p>	<p>Reviewed agreements with the Social Security Administration.</p>	<p>No exceptions noted</p>
<p>Encryption is used when the electronic transmission of information involves sensitive data that passes over the public network.</p>	<p>Reviewed procedures used to encrypt data.</p>	<p>No exceptions noted</p>
<p>If a mobile device becomes disabled, all of its local information is automatically erased, and it must be reconfigured to connect to the State’s servers.</p>	<p>Reviewed procedures used for mobile devices. Tested on a test device to see that erasure happened.</p>	<p>No exceptions noted</p>

