State of New Mexico Statewide Architectural Configuration Requirements
Title: IT Risk Management Standard
S-STD003.001
Effective Date: April 7, 2005

1. Authority

The Department of Information Technology (DoIT) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) including the adoption of statewide technical, coordination, and security standards per the Department of Information Technology Act, NMSA 9-27-1 et. seq. (1978).

2. Purpose

The purpose of this standard is to identify and establish a web-based ***Technology Infrastructure and Security Assessment*** application as the statewide vehicle for reporting compliance to statewide IT standards and security risks/vulnerabilities associated with IT infrastructure and security technologies for major budget units.

3. Scope

This applies to all Agencies. Agency is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches.

The Department Secretary, working in conjunction with the Department Chief Information Officer, shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each agency.

4. Standard

4.1 Each agency shall perform risk assessments, at least annually as described in 4.2, for information technology (IT) systems and their environments to determine security vulnerabilities. Security vulnerabilities are more heavily weighted toward the impact of the loss on agency operations, agency assets, or individuals than on the threat of loss.

4.2 Each agency shall submit an annual IT Security Assessment to DoIT (see Attachment A). The assessment indicates the effectiveness of security controls within the agency for categories of risks derived from Federal IT

Security guidelines. Categories of risks may change periodically; the following are representative categories:

1. IT Security
2. IT Risk Management
3. Account Management
4. Configuration Management
5. Authentication and Directory Services
6. Session Controls
7. Network Security
8. Encryption Technologies
9. System Administration
10. Incident Response and Reporting
11. Virus and Malicious Code Protection
12. Business Continuity & Disaster Recovery
13. Backups
14. Maintenance
15. Media Sanitizing/Disposal
16. IT Physical Security
17. Personnel Security
18. Security Training & Awareness
19. Application Software
20. Productivity Software Tools
21. Classification of Data
22. Database Access

4.2.1 Each category contains risk statements for which the agency shall select the appropriate check box of "Yes," "No," "To Some Extent (TSE)," or "N/A" to indicate the applicable level of effectiveness currently in place (from Policy to Procedure, through Implemented, to tested, and finally integrated). Each risk statement allows for comments to further explain the position of the agency.

4.2.2 Where a particular risk statement does not apply to an agency, the "N/A" box shall be checked for "Not Applicable."

4.2.4 Agency IT plans shall address vulnerabilities identified in IT Security Assessment.

5. Definitions

Refer to the N-DEF001.001 Glossary of Terms located on the DoIT website: http://www.doit.state.nm.us/standards.html

6. References

None

7. Attachments

Attachment A - Technical IT Security Assessment Sample

8. Version Control

S-STD-003.001

9. Revision History

Original 04/07/05
Format Updated 09/18/13

ATTACHMENT A – IT Security Assessment ***S A M P L E***

	State of New Mexico IT Security Assessment ***(On Critical Information Assets)***

Agency:	Date:
Contact Name:	Phone:
Email:	Fax:

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
1. IT SECURITY						
A. Security protections in place are commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, modification to, or destruction of agency information or information systems, or that a contractor or other organization uses on behalf of agency.	Yes No TSE° N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
B. Data/information contained in electronic transactions is protected via 1) identification, authentication, and authorization; 2) encryption, as necessary; and 3) electronic signature, as necessary.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. All information collected, processed, transmitted, stored, or disseminated in software application systems is adequately secured.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
D. Networks, hardware systems, and software application systems use cost-effective management, personnel, operational, and technical controls to provide appropriate confidentiality, integrity, and availability.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
E. Sufficient security controls are applied to information systems, resources, and data/ information to contain risk of loss or misuse of the information to an acceptable level that sup-ports the mission and operation of the agency.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
F. Information security management processes are integrated with agency strategic and operational planning processes, including planning and implementing any necessary remedial action to address IT security deficiencies.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
G. Applicable Statewide and budget-unit-specific IT security policies and standards are communicated to appropriate third-party organizations.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
H. An agency IT security program exists including assignment of roles and responsibilities, as well as creation of necessary procedures, adherence requirements, and monitoring controls.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
I. Overlapping IT security roles/responsibilities between agencies and/or contractors relative to security services received from, or provided to, other agencies are identified, defined, and resolved. Inter-agency Service Agreements are enacted relative to security services, as applicable.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
J. IT projects are implemented as described in *Compliance and Project Management – Enterprise Project Management Office* as well as relevant Federal and individual agency standards.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
2. IT RISK MANAGEMENT						
A. Risk assessments for IT systems and their environments are performed at least annually to determine security vulnerabilities. Security vulnerabilities are more heavily weighted toward the impact of the loss on agency operations, agency assets, or individuals than on the threat of loss.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
B. IT plans address vulnerabilities identified in IT Security Assessment.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
3. ACCOUNT MANAGEMENT						
A. Activities for establishing on-line accounts, levels of approval, access to confidential information, remote access, monitoring inactive accounts, forgotten passwords, and closing accounts are controlled.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Management communicates that accountability for actions taken on an IT resource (e.g., computer system, agency or State application system, etc.) belongs to the owner of the specific userID under which those actions take place.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. System, application, and information access is only granted via a formal and auditable procedure having a retrievable, associated written record of the request and subsequent authorization.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
D. The steps and timing for granting or withdrawing system and information access privileges are documented and maintained In accordance with *Statewide Standard S-STD0011, Personnel Security.*	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
E. All special access privileges, including high-level privileges (such as root access), system utilities, and privileges that provide access to sensitive network devices, operating system, or software application capabilities are documented and maintained.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
F. All holders of remote access privileges to agency IT resources, including third-party entities, are documented and maintained.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
4. CONFIGURATION MANAGEMENT						
A. A configuration management program governs changes to devices and/or associated software components in the production IT environment.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. A perpetual inventory, including configuration/version information for all IT devices and associated software assets, and IT applications, is maintained within agency.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
C. A high-level network/ systems diagram exists, supported by detail diagrams identifying the underlying structures of the agency computer/systems network.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
5. AUTHENTICATION AND DIRECTORY SERVICES						
A. All external connections to agency networks are routed through secure gateways, encrypted, and use strong authentication, such as challenge/response devices, one-time passwords, tokens, Kerberos, or smart cards, in addition to the standard method of authentication required for internal connectivity (i.e., multifactor authentication).	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Access to resources and services shall be in accordance with *Statewide Standard S-STD-011, Personnel Security,* and *Statewide Standard S-STD-011, Authentication and Directory Services*. Internal and external connectivity to networks to provide access to resources and services shall be in accordance with *Statewide StandardS-STD-005 , Network Security*.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Lightweight Directory Access Protocol (LDAP) is used to provide access to directory and application services.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
D. User authentication employs a userID associated with something (password) only the user/customer knows or something (token) only the user possesses.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
6. SESSION CONTROLS						
A. Automatic session timeouts are in place on multi-user information systems and remote communication systems. The maximum period of inactivity is set commensurate with the sensitivity of information housed on the individual system.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. All system users log off at the end of the business day. Where business requirements necessitate a deviation, rationale and procedures are documented.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Locking screensavers are used on all personal computers (including laptops) and are automatically activated by the computer's operating system after a specific period of inactivity determined by the agency.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
D. Password strength used on locking screen savers is determined by the capabilities of the applicable operating system. Passwords meet the requirements of *Statewide Standard S-STD-001, Authentication and Directory Services*, unless otherwise prevented by the capabilities of the operating system.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
E. Accounts are locked from further use following a maximum number of detected, unsuccessful login attempts. Resetting procedures ensure that only the correct account holder is requesting the reset.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
F. Where available, access logs are turned on and protected from accidental or deliberate overwriting, maintained for a period of time determined by business need, and stored in accordance with *Statewide Standard S-STD-010 P800-S870, Backups.*	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
7. NETWORK SECURITY						
A. All external traffic is routed through secure gateways, such as firewalls, employed at the edge of the agency's network, including the Internet Gateway.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Client platform devices, including State-owned assets, client devices used by remote workers and telecommuters, as well as third-party entities, connected to the agency's internal network should be protected from sending or receiving hostile threats from unauthorized network traffic or software applications.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Internetworking devices (including routers, firewalls, switches, etc.) are controlled to prevent unauthorized access.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
D. Roles, responsibilities, and related activities for implementing patch management on internetworking devices (including routers, firewalls, switches, etc.) are identified.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
E. Services provided through the Internet (web-enabled applications, FTP, Mail, DNS, VoIP, etc.) are deployed on a Demilitarized Zone (DMZ) or proxies from a DMZ.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
F. All external connections to networks are routed through secure gateways and protected by an approved encryption method.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
G. Wireless networks employ centralized user authentication in accordance with *Statewide Standard P800-S820, Authentication and Directory Services*, encryption technologies with automated key distribution, and VPN technologies, as appropriate.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
H. Intrusion detection mechanisms or intrusion prevention tools are incorporated into all servers connected to WANs and to all internetworking devices that serve as gateways between WAN network segments.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
I. Network and host vulnerability scanners are used to test for the vulnerabilities of internal systems and of network perimeter defenses, as well as adherence to security policy and standards.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
J. Hardcopy and electronic documentation of network device configurations, network diagrams, etc., is destroyed when superseded or no longer needed.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
8. ENCRYPTION TECHNOLOGIES						
A. Secure e-mail communications use S/MIME Version 3, or succeeding approved standards, for encryption, sender authentication, and message integrity services.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Security levels for specific PKI and PGP uses have been determined in conjunction with State's Policy Authority.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
9. INCIDENT RESPONSE AND REPORTING						
A. A SIPC membership application has been completed for the agency. Contact information for SIPC is up to date.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. All cyber intrusions are reported to SIPC within one hour of discovery. A SIPC Incident Report is completed for each cyber intrusion.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
10. VIRUS AND MALICIOUS CODE PROTECTION						
A. All workstations and servers are protected by virus-scanning software that has "notify and clean" enabled by default. Users are prevented from disabling virus-scanning software.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Each agency shall ensure that all remote workstations and servers used by State employees, contractors, and third-party entities that access agency internal networks are protected with virus-scanning software equivalent to that used by the agency. Virus-scanning software shall be configured and kept current.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Virus-scanning software regularly scans all files stored on direct attached storage devices to the workstation and any file accessed or modified by a workstation software application, whether deployed on the individual workstation device, host- or server-based, or application service provider (ASP) based.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
D. Specific individuals are responsible and accountable to configure and execute appropriate virus-scanning software on all network-attached (wired and wireless) workstations, and to maintain appropriate inoculants and patches for each virus or malicious code infection on all network servers that provide virus-scanning services to network-attached (wired and wireless) workstations and on all portable and stand-alone workstations.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
E. All incoming email, including attachments, is scanned for the existence of virus or malicious code. Viruses and malicious code are contained and eradicated upon discovery.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
F. Employees and contractors are provided a clear process, including appropriate contact points, to address, resolve, and report virus or malicious code infections.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
G. Protection techniques guard against virus and malicious code and potential intrusion from Instant Messaging (IM), peer-to-peer (P2P) file-sharing, and Internet Relay Chat (IRC).	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
11. BUSINESS CONTINUITY & DISASTER RECOVERY						
A. Phase I Business Impact Assessment, Phase II Strategy Development, and Phase III Strategy Implementation have all been completed.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
12. BACKUPS						
A. Backups are taken using a defined cycle frequently enough to meet the time-criticality of agency business processes, business continuity plans, as well as legal, regulatory, and contractual obligations.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
B. Backup media types (disks, RAID storage, optical archive, tape, etc.) used are based on business continuity planning for critical services and regulatory obligations relative to permanence of data/information.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Automated back-up management software is used to perform the backups on designated systems.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
D. The same controls as apply to the original data apply to the data being backed up.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
E. All operating system software, application software, related software, utilities, etc., necessary to configure and restore critical information and services are backed up.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
F. Backups are tested on a regular basis, as documented, for restorability, recoverability, and to ensure that restored information has not been compromised.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
13. MAINTENANCE						

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
A. Configurations of critical systems' platform and network infrastructure, operating system software, software application, and related software configurations are documented and maintained. Formal change control exists for configurations of critical systems.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Sensitive data stored on systems being sent offsite for repair or maintenance operations is removed from the storage media in accordance with *Statewide Standard P800-S880, Media Sanitizing/Disposal.*	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Access to critical system hardware and software, wiring, and networks is restricted to personnel authorized by the agency and controlled by rules of least privilege required to complete the assigned task.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
14. MEDIA SANITIZING/DISPOSAL						
A. Any IT device, network component, operating system software, application software, or storage media containing public/official records has the final disposition of those records established with New Mexico State Library, Archives, and Public Records (ASLAPR) before it is disposed of through State Surplus or provided to another State organization.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Before disposal through State Surplus, data stored on any IT device is deleted in a manner that renders it unrecoverable.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Prior to off-site repair of IT devices, network components, operating system or application software, or storage media, all agency sensitive data is removed.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
D. Only authorized personnel remove sensitive data from IT devices.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
15. IT PHYSICAL SECURITY						
A. Information systems (mainframes, servers, etc.), media storage areas, and related communication wiring and network devices are located in secure locations that are locked and restricted to access by authorized personnel only.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Physical access security measures employed for back-up systems/facilities are equivalent to those of the primary facilities.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Information systems, media storage areas, and related communication wiring and network devices are protected against loss or malfunction of environmental equipment or services necessary for the operation of the facility that houses them.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
D. Computing and telecommunications equipment is inventoried in accordance with *Statewide Standard S-STD-002, Configuration Management*, accounted for, and safeguarded from loss and resulting unauthorized use.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

Control	Policy	Procedure	Implemented	Tested	Integrated	Comments*
16. PERSONNEL SECURITY						
A. Personnel policies and procedures show clear accountability for security administration. Security policies and procedures are available to and applied to every existing State employee and contractor, as well as to new State employees and contractors.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Job-related requirements for potential IT personnel or contractors working in primary facilities housing critical information systems or handling confidential information are used as a hiring consideration.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
17. SECURITY TRAINING AND AWARENESS						
A. Security awareness training content exists and is regularly reviewed and updated to ensure that it addresses the organizational mission including culture, business, technology, systems, and data/information.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. IT security roles and responsibilities of key personnel are defined and documented.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
18. PLATFORM INFRASTRUCTURE						

A. Platform devices have the appropriate level of security functionality incorporated as part of the installed operating system.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Shared platforms (including mainframes, servers, etc.) are controlled to prevent unauthorized access, both internal and external, in accordance with *Statewide Standard S-STD-005, Network Security*.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Roles, responsibilities, and related activities for implementing patch management on platform device operating systems are identified.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
D. Hardcopy and electronic documentation of shared platform device configurations, access lists, diagrams, etc., is destroyed, as appropriate, when no longer needed.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
E. All portable platform devices (laptops, PDAs, etc.) capable of storing information (documents, databases, etc.) that connect to agency networks adhere to authentication requirements, connectivity requirements, as well as all other applicable Statewide IT security standards have any automatic logon capability disabled.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

19. APPLICATION SOFTWARE						
A. All software applications are capable of securely exchanging information and integrating or interoperating with other software applications.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Security services associated with software applications, databases, and utility software adhere to Statewide IT security standards, allow for all security updates to be pushed to, or accepted by, all associated software products, and allow for an integrated lightweight directory access protocol (LDAP) directory service.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
20. PRODUCTIVITY SOFTWARE TOOLS						
A. Roles, responsibilities, and related activities for implementing patch management on productivity software are identified.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

21. CLASSIFICATION OF DATA						
A. Data/information is classified according to its degree of sensitivity in a universally understandable manner and that maintains its security classification as it traverses any physical or logical boundary.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Data/information is classified into "confidential" versus "public" information. (Agencies requiring additional classifications may create and document those classifications and related owner/custodian/recipient responsibilities at their discretion.)	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Aggregates of data/information are classified using the most secure classification level of any individual component. Extracts of data/information are secured to the same level as the file/database from which the data/information has been extracted.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

E. Data/information being shared is appropriately and consistently classified and protected comparably to when the data/information was within the original agency's immediate control. The value and classification of the data/information is communicated to the respective additional custodians/recipients.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
22. DATABASE ACCESS						
A. Database access is securely implemented with regard for availability, integrity, and confidentiality of the data.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
B. Entry and update of data stored in databases is accomplished only in accordance with the business rules established in software application systems. Data access and permissions are assigned within the context of the software application and in accordance with *Statewide Standard S-STD-001, Authentication and Directory Services.*	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	
C. Free-form data entry and update using direct database access are restricted. Direct database access, when required, is accomplished in accordance with *Statewide Standard S-STD-001, Authentication and Directory Services.* Owners of the data and information stored in the relevant databases provide written delegated authority or specific access permissions to ensure that relevant business rules implemented by the software application system for normal entry and update are not violated.	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	Yes No TSE N/A	

D. Direct database access for ad-hoc queries and end-user reporting is read-only. Software utilized for ad-hoc queries and end-user reporting conforms to database technology connectivity and access requirements.	Yes No TSE N/A	Yes No TSE N/A	