USM IT SECURITY STANDARDS

Version 4.0

September 2016

USM IT SECURITY COUNCIL:

Rustam Abakaev, UB
Mark Addy, TU
Suresh Balakrishnan, USM
Lori Bennett, FSU
David Bobart, UB
Mark Cather, UMBC
Shane Daniels, SU
Duke Darrigo, SU
Greg Gisriel, UMUC
Fred Hayes, USM
Sribala Narasimhadevara, CSU
Todd Pearce, UMUC
Raj Singh, UMUC
Fred Smith, UMB
Joseph Smith, UMES
Gerry Sneeringer, UMCP
Todd Spahr, TU
Donald Spicer, USM
Michael Von Paris, TU

TABLE OF CONTENTS

I. Introduction 1

II. IT Security Program Standard 2

III. Confidential Information Standard 4

IV. Access Control Standard 5

V. Network Security Standard 8

VI. Contingency Planning Standard 9

VII. Physical Security Standard 10

VIII. Endpoint Desktop/Laptop Security Standard 11

IX. Encryption Standard 12

X. Virtualization Technologies Standard 13

XI. Third-Party/Cloud Technology Services Standard 14

XII. Mobile Device Standard 17

XIII. Record of Revisions 18

I. Introduction

The Board of Regents' Information Technology Policy, in compliance with Section 12-112 of the Education article of the Maryland Code, requires that the University System of Maryland (USM) adopt information technology policies and standards that are functionally compatible with state information technology policies and standards. The Regents' policy was approved in August 2001 and is available at: http://www.usmd.edu/Leadership/BoardOfRegents/Bylaws/SectionX/X100.html

This document addresses security standards established by the state Department of Information Technology (DoIT) for state agencies and interprets those standards in the context of the USM institutions. The state standards are described in the document entitled *Information Security Policy*, which is available on the DoIT website at: http://doit.maryland.gov/policies/Pages/default.aspx

Originally published as a set of guidelines, this document was formally adopted as USM Standards by the Board of Regents on June 27, 2014.

Throughout this document, standards are presented in normal text while commentary and suggestions are presented in italics.

There are a number of references in these standards to NIST Special Publications 800 series documents. These documents are computer security guidelines, recommendations, and reference materials published by the National Institute of Standards and Technology. These documents can be found at http://csrc.nist.gov/publications/PubsSPs.html.

II. IT Security Program Standard

2.1 Institutions must implement a Security Policy and an associated Security Program. The Security Program should be documented and monitored. The CIO or designee must approve institutional security policies.

2.2 Procedures required by the USM IT Security Standards must be documented.

2.3 Institutions must implement a formal process for determining the appropriate level of risk for IT resources. This process will include identification of systems that process and/or store confidential information as defined in Section III, Confidential Information Standard and other critical systems. This risk process must examine the issue of disclosure of confidential information.

Managing information security risk, like risk management in general, is not an exact science. It brings together the best collective judgment of individuals and groups within organizations responsible for strategic planning, oversight, management, and day-to-day operations. Institutions need to recognize that explicit, well-informed risk based decisions are necessary in order to balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure.

2.4 Institutions must develop and promulgate a Data Classification Policy. This policy must define classes of data that the institution considers to be a risk and the classes of data that the institution does not consider to be a risk.

2.5 Institutions must have documented systems (hardware, software, network, or a combination) development lifecycle (SDLC) plans, including the phases of initiation, acquisition/development, implementation, operations/maintenance, and sunset/disposal. Each phase of the SDLC plan must consider the risks posed by the data and operation of the system and include steps to address any risks in an appropriate manner.

The process of developing/acquiring, implementing, operating, and retiring systems (hardware, software, network, or a combination) is known as a System Development Life Cycle (SDLC).

2.6 Institutions must conduct regular assessments to identify computer system vulnerabilities and to take remedial action before the systems are compromised. The results of vulnerability scans against critical systems must be submitted to USM Internal Audit for review each quarter.

2.7 Institutions must implement a security awareness program.

A security awareness program is an essential element of a Security Program. An awareness program should be tailored to address risks identified for an institution's environment.

2.8 Institutions must document processes for responding to incidents and security advisories. Incidents involving the compromise of personal information (as defined under State Government Article 10-301, see Section III) must be reported to the USM Office of the CIO.

Incident response procedures address issues such as reporting mechanisms, incident identification and evaluation, resolution and documentation, and post-event analysis.

2.9 Institutions must adhere to their Institutional Records Management Program as required under Regents Policy VI-6.10.

2.10 Institutions must report annually to the USM CIO on the status of its IT Security Program. This report is due by August 15th of each year. The USM IT Security Council will provide a suggested template for this report. The President and the CIO of the institution must approve this report.

2.11 An information security deviation/risk acceptance request must be completed by the institution if it is determined that it is infeasible to comply with the USM standards. The request must be completed by the campus IT Security Officer and approved by the institutional CIO as well as the USM CIO. The cycle for completing these requests will normally coincide with the reporting cycle for the status of the IT Security Program, which is August 15th of each year.

2.12 USM institutions must develop acceptable use policies that address the responsible use of institutional computing resources, including electronic mail, network services, electronic documents, information, software, and other resources.

Institutional Acceptable Use Policies must:

- Address a user's responsibility to protect their accounts and passwords from unauthorized usage.
- Address the issues of copyright infringement and unauthorized software.

2.13 Each USM institution shall have personnel designated for providing authenticated notices of IT incidents and advisories to the institutional user community. Only these personnel will send such messages.

2.14 Institutions must have processes regarding software licenses that promote compliance with federal copyright law. Institutions must designate a single point of contact for inquiries about copyright violations, pursuant to federal law.

III. Confidential Information Standard

USM has defined confidential data to include:

- *Educational Records, as defined and when protected by 20 U.S.C § 1232g; 34 CFR Part 99 (FERPA), in the authoritative system of record for student grades*
- *Any Protected Health Information (PHI) as the term is defined in 45 CFR 160.103 (HIPAA)*
- *Personal information as defined in the Maryland Code under State Government Article, §10-1031:*

> *An individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:*
>
> *i. a social security number;*
> *ii. a driver's license number, state identification card number, or other individual identification number issued by a unit;*
> *iii. a passport number or other identification number issued by the United States government;*
> *iv. an individual taxpayer identification number; or*
> *v. a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.*

3.1 Institutions must establish a policy for the protection of confidential information from disclosure in conformance with applicable State of Maryland and federal laws.

3.2 Institutions must implement measures to protect confidential data from disclosure in conformance with applicable state and federal laws. These include not using confidential information as identifiers and requiring non-disclosure agreements prior to granting employees access to confidential data.

3.3 Institutions must have a documented framework for applying appropriate access controls, based on data criticality and sensitivity.

3.4 USM institutions must utilize encryption for confidential data (refer to Section IX) while the data are in transit or at rest on any media (including portable devices, flash storage, optical media, and magnetic media) or apply compensating controls that are equally secure, depending on the capabilities of the technology in use.

3.5 When data are shared with other institutions, the State, or federal agencies, that shared data should be managed with the security requirements determined to be the highest among the sharing institutions involved, and approved by the institutional CIO or data steward.

IV. Access Control Standard

The Access Control Standard applies to all critical systems, including those that contain confidential information.

4.1 There must be documented procedures for creating, managing, and rescinding user accounts. At a minimum, these procedures should address:

- The eligibility criteria for obtaining an account
- The processes for creating and managing accounts including the process for obtaining users' agreement regarding the acceptable use policy
- The processes for managing the retention of user account information
- All user account access to institutional information technology systems, including access for outside contractors, must be limited based on risk to the institution and the privileges needed to fulfill the institutional roles of the user

4.2 Institutions must implement authentication and authorization processes that uniquely identify all users and appropriately control access to critical systems.

4.3 Prohibit group or shared IDs, unless they are documented as Functional IDs. Where possible, individual accounts should be used to provide accountability for administrative changes.

Functional IDs are user accounts associated with a group or role that may be used by multiple individuals or user accounts that are associated with production job processes.

When Functional IDs are issued, the following controls should be in place:

- Eligibility criteria for obtaining an account
- Processes for creating and managing accounts including the process for obtaining users' agreement regarding the acceptable use policy
- Processes for managing the retention of user account information

Considering the diverse computing environments at USM institutions, the following password requirements are dependent upon operational capabilities of a particular system.

NIST Special Publication 800-63-2 describes the Federal Electronic Authentication (eAuth) Guidelines. eAuth provides a methodology for creating flexible password requirements based upon operational needs and the risks that are present. The process of risk evaluation and how it applies to the selection of requirements can be found in the SP800-63-2 (or later) document.

4.4 Users of critical systems must adhere to institutional usage, construction, and change requirements. Systems may comply with EITHER 4.4.1 or 4.4.2 below:

4.4.1 Meet the eAuth guidelines as outlined in NIST Special Publication 800-63-2 (or later);

or

4.4.2 Meet the following alternative requirements:

- Minimum password length: 8 characters
- Passwords must contain a mix of alphanumeric characters. Passwords must not consist of all digits, all special characters, or all alphabetic characters
- Automated controls must ensure that passwords are changed at least annually for general users, and at 90-day intervals for administrative-level accounts
- User IDs associated with a password must be disabled for a period of time after not more than 6 consecutive failed login attempts. A minimum of 10 minutes is required for the reset period

4.4.3 Follow the following password management practices:

- Password must not be the same as the user ID
- Password must not be stored in clear text
- Password must not be displayed on screens
- Initial passwords and password resets must be issued pre-expired forcing the user to change the password upon first use
- Password reuse must be limited by not allowing the last 10 passwords to be reused. In addition, password age must be at least 2 days
- When a user password is reset or redistributed, the validation of the user identity must be at least as strong as when originally established
- Expired passwords must be changed before any other system activity is allowed

4.5 There must be documented processes that ensure that access rights reflect employee status, including changes in employee status. For critical systems, employees' access rights will be modified, as appropriate, by the close of business on the same day, after the employees' change of status is communicated to IT

4.6 Critical systems must have a documented process for annual verification of users' access rights.

4.7 Institutions must maintain appropriate audit trails of events and actions related to critical applications and confidential data. The following significant events must be reviewed and documented:

- Additions and changes to critical applications
- Actions performed by administrative level accounts
- Additions and changes to users' access control profiles
- Direct modifications to critical data outside of the application

4.8 Procedures must be in place to routinely (for example daily or weekly) review audit records of critical systems for indications of unusual or suspicious activities or suspected violations. Findings must be reported to appropriate officials for prompt resolution.

4.9 The functions of system administration, programming, processing/authorizing business transactions, and security administration must be segregated. This provides for the appropriate separation of duties. If not possible, compensating controls must be established to mitigate the risk.

V. Network Security Standard

5.1 Networked equipment shall be configured and maintained so as to not cause network performance degradation, not cause excessive, unwarranted traffic flows, and be suitably hardened against network security threats.

5.2 Appropriate controls for remote access services must include logging of access and encryption of critical data in-transit.

5.3 Banner text approved by Legal Counsel must be displayed at all system authentication points where initial user logon occurs, when technically possible.

5.4 Networks must be protected by firewalls at identified points of interface based on system sensitivity and data classification. Firewalls should be configured to block all unneeded services, prevent direct access to hosts on trusted network from untrusted networks, and maintain comprehensive audit trails. Management access must be encrypted and limited to designated personnel.

5.5 All network devices (e.g., switches, routers) should have all non-needed services disabled. Default administrator username (if possible) and password must be changed. Updates and patches must be installed in a timeframe determined based on factors such as risk, interdependence, and/or prevention.

5.6 Implement ingress and egress filtering at the edge of the institution's network to prevent IP spoofing.

5.7 Institutions must establish automated and manual processes for intrusion prevention and/or detection.

- Host-based and/or network-based, must be utilized
- Alerts must be regularly monitored
- There must be an escalation plan based on commonly encountered events that include immediate response capability when appropriate
- Access to management consoles are limited to appropriate personnel
- Detection signatures must be updated on a regular schedule
- If interrogation of encrypted network traffic is not possible, host-based measures must be in place on critical systems

5.8 Institutions must create a Service Interface Agreement (SIA) when providing a connection to an external entity. The SIA must document the scope, use, and restrictions that apply to the connection.

VI. Contingency Planning Standard

If an institution uses their disaster recovery plan to handle a real event, that event can be documented and, depending on the event and the extent of remediation and recovery, may be able to take the place of an institution's annual test.

6.1 Institutions shall develop and implement their IT Disaster Recovery Plan for systems that the institution identifies as critical and test and update the plan at least annually.

6.2 The IT Disaster Recovery Plan must minimally include the following critical items:

- Documentation of each critical system including
  - Purpose
  - Software
  - Hardware
  - Operating System
  - Application(s)
  - Data
  - Supporting network infrastructure and communications
  - The contact information for the person or group responsible for the system
- System restoration priority list
- Description of current data back-up and restoration procedures
- Description of back-up storage location(s)

VII. Physical Security Standard

7.1 Commensurate with the assessment of risks, physical access controls must be in place for the following:

- Data Centers
- Areas containing servers and associated media
- Networking cabinets and wiring closets
- Power and emergency backup equipment
- Operations and control areas

7.2 Access to data centers and secured areas will be granted for those employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas. Authorization should be based on need and approved by the manager responsible for the secured area.

7.3 USM institutions are responsible for:

- Issuing picture ID badges to all employees and contractors in IT areas
- Ensuring that all portable storage media containing confidential information such as hard drives, flash drives, magnetic tapes, laptops, and CDs are protected commensurate with the risk posed to the institution
- Ensuring that proper environmental and physical controls are established to prevent accidental or unintentional loss of sensitive/confidential information residing on IT systems
- Ensuring that any physical access controls are auditable

The following media destruction and reuse standards apply to all electronic storage media equipment that is owned or leased (including, but not limited to: workstations, servers, laptops, cell phones, and multi-function printer/copiers).

7.4 When no longer usable, electronic storage media that contain sensitive data shall be destroyed and/or sanitized. Institutions must use methods that are in accordance with the NIST SP800-88rev1 *Guidelines for Media Sanitization.* This requirement applies to the permanent disposal of all storage media and equipment containing storage media regardless of the identity of the recipient. It also applies to equipment sent for maintenance or repair.

7.5 The procedures performed to sanitize electronic media must be documented and data destruction records retained whether performed in-house or by a campus contractor.

7.6 Media must be overwritten before being released internally for reuse.

7.7 Institutions should determine when it is appropriate to perform a criminal background check prior to hire.

VIII. Endpoint Desktop/Laptop Security Standard

Refer to Section XII for security of mobile devices

8.1 Controls must be implemented on all institutionally-owned desktop and laptop computers that store and/or access confidential information:

- User ID and password is required to access the computer
- Implement appropriate desktop solutions that, to the extent possible, detect malware and update automatically to identify new threats
- Identify personally identifiable information (PII) stored on such systems
- Host-based firewalls should be operational and properly configured to protect the computer when it is outside of the secured USM network

8.2 Implement and document processes for managing exposure to vulnerabilities through the timely deployment of operating system and application patches.

8.3 Using a risk-based approach, implement and document processes that minimize provisioning of local administrative rights so that only those employees who require it are given those rights.

8.4 Institutions will establish security measures for processing or storing sensitive information on personal or contractor-owned data processing equipment.

IX. Encryption Standard

9.1 Consistent with Section III, Confidential Information Standard, USM institutions must establish minimum standards for the use of encryption.

9.2 Institutions using public key or certificate-based encryption must have an established process that provides for minimal operational capabilities such as issuance, association, and validation.

9.3 Institutions must take steps to ensure that encrypted information is not lost through changeover of personnel.

X. Virtualization Technologies Standard

10.1 Institutions must carefully plan prior to the installation, configuration and deployment of virtualization solutions to ensure that the virtual server environment is as secure as a non-virtualized environment and in compliance with all relevant institutional policies. Security should be considered from the initial planning stage at the beginning of the systems development life cycle to maximize security and minimize cost.

10.2 The security of a full virtualization solution is heavily dependent on the individual security of each of its components, including the hypervisor, host computer, and host OS (if applicable), guest OS, applications, and storage. Institutions should secure all of these elements and maintain their security based on sound security practices, such as restricting access to administrative interfaces, keeping software up to date with security patches, using secure configuration baselines, performing monitoring and analysis of logs at all layers of the solution, and using host-based firewalls, antivirus software, or other appropriate mechanisms to detect and stop attacks. Non-virtual servers should also follow these practices as necessitated by risk.

Recommendations for securing virtualization technologies can be found in NIST SP800-125, Guide to Security for Full Virtualization Technologies.

XI. Third-Party/Cloud Technology Services Standard

This Standard is intended for USM Institutions that choose to outsource technology services to third-party cloud providers. Institutions must assess, and take steps to mitigate, the risk of unauthorized access, use, disclosure, modification, or destruction of confidential institutional information. This standard only applies to third-party cloud technology service agreements for mission critical systems as well as where confidential information will be transmitted, collected, processed, stored, or exchanged with the cloud service provider. See USM Standard III. Confidential Information Standard to determine the classification of data involved.

Examples of third-party cloud technology services include:

- *Cloud Services*
  - *Software-as-a-Service (SaaS)*
  - *Infrastructure -as-a-Service (IaaS)*
  - *Platform-as-a-Service (PaaS)*
  - *Network-as-a-Service (NaaS)*
- *Web Hosting*
- *Application Hosting*
- *Database Hosting*
- *Cloud Data Backup*
- *Offsite Cloud Storage*

11.1 In conjunction with the Institution's procurement department and security team, stakeholders shall perform the following activities during the life-cycle of the third-party cloud technology service:

- Assess the risks associated with the third-party cloud service. Institutions must ensure that the security of a vendor's cloud solution provides comparable protection to a premises-based solution including the need to ensure confidentiality, integrity, availability, security, and privacy.

- Commensurate with the risk, request and, if available, obtain, review, and document control assessment reports performed by a recognized independent audit organization. Examples of acceptable control assessment reports include (but are not limited to):
  - AICPA SOC2/Type2
  - PCI Security Standards
  - ISO 27001/2 Certification
  - FedRAMP

11.2 Institutions must periodically review the most recent control assessment reports as well as the providers' compliance with IT security, privacy, and availability deliverables in the contract. They must also reassess the risk of the cloud solution to ensure that the solution continues to provide adequate protection to institutional information assets.

11.3 Third-party contracts should include the following:

- Requirements for recovery of institutional resources such as data, software, hardware, configurations, and licenses at the termination of the contract
- Service level agreements including provisions for non-compliance
- Provisions stipulating that the third-party service provider is the owner or authorized user of their software and all of its components, and the third-party's software and all of its components, to the best of third-party's knowledge, do not violate any patent, trademark, trade secret, copyright or any other right of ownership of any other party
- Provisions that stipulate that all institutional data remains the property of the institution
- Provisions that require the consent of the institution prior to sharing institutional data with any third parties
- Provisions that block the secondary use of institutional data
- Provisions that manage the retention and destruction requirements related to institutional data
- Provisions that require any vendor to disclose any subcontractors related to their services
- Requirements to establish and maintain industry standard technical and organizational measures to protect against:
    - accidental damage to, or destruction, loss, or alteration of the materials;
    - unauthorized access to confidential information
    - unauthorized access to the services and materials;
    - industry known system attacks (e.g., hacker and virus attacks)
- Requirements for reporting any confirmed or suspected breach of institutional data to the institution
- Requirements that the institution be given notice of any government or third-party subpoena requests prior to the contractor answering a request
- The right of the Institution or an appointed audit firm to audit the vendor's security related to the processing, transport or storage of institutional data
- Requirement that the Service Provider must periodically make available a third-party review that satisfies the professional requirement of being performed by a recognized independent audit organization (refer to 11.1). In addition, the Service Provider should make available evidence of their business continuity and disaster recovery capabilities to mitigate the impact of a realized risk (if available)
- Requirement that the Service Provider ensure continuity of services in the event of the company being acquired or a change in management
- Requirement that the contract does not contain the following provisions:
    - The unilateral right of the Service Provider to limit, suspend, or terminate the service (with or without notice and for any reason)

    - A disclaimer of liability for third-party action
- Requirement that the Service Provider make available audit logs recording privileged user and regular user access activities, authorized and unauthorized access attempts, system exceptions, and information security events (as available)

XII. Mobile Device Standard

For the purpose of these standards, mobile devices encompass all portable technology capable of storing data with the exception of laptops, which are covered in Section VIII

12.1 All institutions must develop a mobile device standards document that provides guidance related to the following topics:

- The protection of data stored and processed on mobile devices
- The classes of data that are permitted to be used or stored on mobile devices
- The business use of personal mobile devices
- The proper methods for securing mobile devices that are owned by the institution

XIII. Record of Revisions

Revision	Date	Section	Description
Version 4.0	September 2016	All	Reorganization of document to correct inconsistencies, ambiguous language, and to clearly separate commentary from requirements
		I	Added date of BOR approval, comments on formatting of document, and explanation of NIST SP800 Series
		II.2	Added requirement for documented procedures
		II.3	Separated commentary from standard
		II.4	Data classification requirement moved from former VII.4
		II.5	Revised SDLC standard
		II.7	Merged requirement for regular assessments and requirement to report quarterly to USMIA
		II.8	Modernized security awareness item
		II.10	Added reference to BOR records management policy
		II.11	Added requirement for approval of CIO and President
		II.12	Risk acceptance standard merged into Program Standard
		II.13	AUP standard merged into Program Standard
		II.14	Security advisory section separated from AUP item to create a new item
		II.15	Section of copyright moved here from desktop standard

		III.1	Separated definition from requirement
		III.2	Replaced considerations with a list of requirements
		III.4	Removed examples. Added "or apply compensating controls that are equally secure"
		IV	Rearranged order of requirements for clarity
		IV.1	Added control for user account access for outside contractors and all users
		IV.3, IV.4	Simplified and clarified wording of functional account requirements
		IV.4.2	Changed control for failed login attempts to apply to all systems
		IV.5	Made clear the choice between eAuth and a fixed list of password requirements
		IV.5.1	Replaced lengthy description of eAuth with a reference to NIST SP800-63-2
		IV.5.2	Removed requirement for no leading spaces, this is an implementation issue, not a security issue.
		IV.7	Clarified annual access review requirement; moved user responsibility for password protection to AUP section
		IV.9	Log review language made consistent with DoIT wording
		V	Removed requirement to follow requirements; detailed wireless references removed; network security applies to all network media; deleted dial-in access language
		V.3	Recognized limitations on display of banners

		V.4	Simplified statement
		V.5	Recognized consideration of risk factors in patch installation timing, remove reference to servers
		V.7	Statement of preference removed; alert escalation rephrased; added text on encrypted network traffic
		V.8	Cleaned up language of SIA item
		VI.1	Clarified the language in 6.1
		VII.3	Scoped badging requirement to IT service areas
		VII.4,VII.5	Simplified language
		VII.7	Removed policy that policies must be followed
		VIII.1	Clarified the language in the first bullet and added requirement for host-based firewalls
		IX.3	Ensured keys are escrowed
		X	Replaced wholesale, added reference to SP800-125
		XI	Complete rewrite
***	***	***	***
Version 3.0	June 2014	Cover Page II.5, V.5, V.13.B, VII.2, VII.3, VII,4, VII.5, VII,6, VII.7, VIII.1.1, IX	As per MITRE's recommendations, the "USM Guidelines" have been repurposed as "USM IT Security Standards". Updated membership
		II.2	Clarified the definition of systems that process and/or store confidential data, as per MITRE recommendation #2.

		II.7	Added a standard to Section II requiring institutions to implement a data retention policy and retirement schedule.
		III	Defined nonpublic/confidential information, as per MITRE recommendation #2.a. Replaced the term 'nonpublic" with "confidential". Per the recommendation of the Office of Legislative Audits, added "Educational Records, as defined and when protected by 20 U.S.C. § 1232g; 34 CFR Part 99 (FERPA), in the authoritative system of record for student grades" to the definition of Confidential Information.
		II.5	Modified the standard to require documentation and implementation of role-specific training, as per MITRE recommendation #3.
		IV.4	Modified the section to incorporate MITRE's recommendation (#4) to capture all access to confidential data in audit trails.
		IX	Modified the Encryption Standard, to include encryption requirements for portable devices and media, as per MITRE's recommendation # 5.
Version 2.0	September 2013	Cover Page	Modified date and version number and updated membership
		VI, X, XI, XII	Added the following new sections to the USM Guidelines: VI - Contingency Planning Standard X - Virtualization Technologies XI - Cloud Computing Technologies XII - Mobile Devices
		II.2	Added details regarding risk management
		II.4	Deleted. New section VI on Contingency

			Planning has been added
		II.4 (II.5 in v 1.7)	Revised guideline on vulnerability assessments
		II.6	Deleted requirement for reporting statistics on incidents
		III.1	Revised to state "in conformance with applicable State of Maryland and federal laws."
			Deleted note
		IV.1	Revised guideline on managing user accounts
		IV.2.A	Added password construction guidelines for functional IDs
		IV.2.B	Revised frequency of password changes for general users
			Added password reuse guideline
			Added expired passwords guideline
			Deleted reference to NIST SP 800-30 as guidance for conducting risk analysis under the Federal Electronic Authentication Guideline
			Revised high privilege users to administrative level accounts
		IV.4	Revised high privilege users to administrative level accounts
		IV.6	Clarified language Added compensating controls
		V.14	Deleted "mobile code" guideline
		V.15	Revised General Controls Guidelines for Wireless Networks

		V.16	Deleted PBX Security guideline
		V.17	Deleted facsimile security guideline
		VII	Storage Media Disposal Specified guideline for releasing storage media containing sensitive information Added reference to NIST SP800-88 Combined Media Reuse and Storage and Marking sections into Data Classification and Storage section Added guideline regarding Data Classification Policy and Data Use Guidelines
		VIII	Revised Section title as State policy delineates Laptops from other mobile devices due to its desktop-like protection capabilities Added guideline on deployment of patches Updated guideline on anti-virus software Deleted guideline on Mobile Computing as there is a new section on Mobile Devices (Section XII) Clarified some language
Version 1.7	August 2011	Cover Page	Modified date and version number and updated membership
		Introduction	Revised language to DoIT from DBM
		II.2	Added suggested reference sites for risk management
		II.4	Revised guidelines for the Disaster Recovery Plan

		II.7	Removed the guidelines on external connections
		III.3	Revised the guidelines for sharing data
		IV.2.B	Added additional password guidelines Revised guideline on minimum password length to eight characters Removed guideline on identical characters in passwords
		IV.3	Added guideline making authorized users responsible for the security of their passwords and accounts
		V	Added and moved "Local Network Access" to the top of the section -- V.1
		V.4 renumbered as V.7	Added language about management access and securing communication channels
		V.5 renumbered as V.8	Revised guideline to incorporate administrator responsibilities and updates of signature-based solutions
		V.8 renumbered as V.11	Revised to incorporate management access guideline
		V.10 renumbered as V.13	Revised language
		V.12.A renumbered as V.15.A	Revised to incorporate documentation of wireless access points Revised to incorporate management access and administrator credentials guidelines Added additional guidelines as described in State Information Security Policy version 2.3 section 7.8
		V.12.B	Deleted – Wireless Security Plan

		V.12.C	Deleted guideline requiring use of SNMPv3 or higher
		V.12.E	Deleted – Wireless intrusion detection
		V.13.A-G	Deleted – PBX Security
		V.16	Incorporated modified State PBX Security Guidelines
		VI.4	Added additional guidelines as described in State Information Security Policy version 2.3 section 7.9
		VII.3	Revised language
		XI	Modified Record of Revisions
Version 1.6	July 2009	Cover Page	Added new members
	Sept. 2009	VII.3	Revised the "Laptop Security and Mobile Computing" guideline to include other mobile computing devices
	Aug. 2009	IV.4	Revised guideline to incorporate risk analysis
		VIII	Added encryption guidelines
Version 1.5	Jan. 2008	Cover Page	Modified date and version number and added new members
		III	Enhanced III.2 of the NPI standard
	March 2008	Document	Added section numbers and revised the format
		Record of Revisions	Added Record of Revisions section
Version 1.3	Aug. 2006	Cover Page	Modified date and version number
		Introduction	Added new Introduction section
		IV.2.A	Added provision to include "functional

			IDs," as described in the State IT Security Policy and Standards v 1.3
		IV.2.B	Added federal electronic authentication guidelines, based on NIST SP 800-63, as an alternative standard for authentication.
		IV.2.E	Changed 9th bullet to allow for a 10-minute automatic reset
		V.8	Deleted
		V.12.E	Added intrusion prevention systems
		V.13	Added intrusion prevention systems
		VI.4	PBX Security guidelines added
			Added guidance for data electronically transferred to a remote storage location