BOARD OF REGENTS

SUMMARY OF ITEM FOR ACTION,
INFORMATION OR DISCUSSION

TOPIC: Discussion/Approval – Proposed IT/IS Security Standards for Board of Regents Policy

COMMITTEE: Audit Committee

DATE OF COMMITTEE MEETING: June 11, 2014

Attached (Attachment A) are security standards for which USM is requesting the audit committee's approval. These standards support current BOR Policy X-1.0. If approved by the audit committee, these policy standards will be submitted to the full Board with the Audit Committee's recommendation for approval.

Also attached (Attachment B) are recommendations with USM's responses to the MITRE Corporation's review of *State IT Security Policy*. These recommendations are incorporated as appropriate into the proposed security standards.

FISCAL IMPACT: none

CHANCELLOR'S RECOMMENDATION: Approval of the proposed security standards in support of BOR Policy X-1.0.

COMMITTEE ACTION: DATE:

BOARD ACTION: None. DATE:

SUBMITTED BY: David Mosca

USM IT SECURITY STANDARDS

Version 3.0

June 2014

USM IT SECURITY COUNCIL:

Mark Addy, TU
Suresh Balakrishnan, USM
Lori Bennett, FSU
David Bobart, UB
Mark Cather, UMBC
Shane Daniels, UMES
Duke Darrigo, SU
Greg Gisriel, UMUC
Fred Hayes, USM
Fred Kowalski, UB
Suresh Murugan, BSU
Sribala Narasimhadevara, CSU
Todd Pearce, UMUC
Raj Singh, UMUC
Fred Smith, UMB
Gerry Sneeringer, UMCP
Todd Spahr, TU
Donald Spicer, USM
Jeff Zankowitz, TU

TABLE OF CONTENTS

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 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 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.

II. IT Security Program Standard

1. Institutions must implement a Security Policy and an associated Security Program. The security program should be documented and monitored.

2. Institutions must have a formal risk management process for determining adequate security levels for IT resources.

   Institutions must implement a process to manage the risks associated with the operation and use of information systems that support their missions and business functions. Institutions must 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.

   Managing information security risk, like risk management in general, is not an exact science. It brings together the best collective judgments of individuals and groups within organizations responsible for strategic planning, oversight, management, and day-to-day operations providing both the necessary and sufficient risk response measures to adequately protect the missions and business functions of those organizations.

   At a minimum, USM institutions should determine adequate security levels for IT resources including:
   - Identify systems that process and/or store confidential data as defined in Section III, Confidential Information Standard
   - Perform a risk self assessment

   (Suggested references for Risk Management include: NIST SP800-30, SP800-37 Rev 1)

3. Institutions must include security as part of the systems development life cycle
   - Demonstrate that security was considered during the procurement, development or enhancement of critical applications
   - Document development and change management for mission critical systems

4. Institutions must conduct regular vulnerability assessments to verify security controls are working properly and to identify weaknesses.

   All USM institutions are required to conduct quarterly network scans on critical systems and submit the vulnerability scan results to USM Internal Audit for review. The objective is to ensure that institutions identify computer system vulnerabilities and take remedial action before the systems are compromised.

5. Institutions must implement a security awareness program
   - Suggested delivery mechanisms include employee and student orientation, web pages, and ongoing awareness activities.
   - Suggested program content includes anti-virus software (from MEEC agreement), password management, security of critical data,
     - Anti-virus software (from MEEC agreement)
     - Password management
     - Critical data security
     - Email: attachments, spam, harassment
     - Appropriate use, including copyrights
     - Updating/patching – operating systems, office, other software
   - Determine, document, and implement role-specific training within the larger security awareness program

6. Institutions must establish and document processes for responding to incidents, including procedures for responding to alerts and virus advisories
   - Establish and publicize an incident reporting mechanism
   - Identify the incident
   - Evaluate the incident
   - Investigate, resolve, and document the incident
   - Follow-up, analyzing lessons learned as needed

   If the incident involves the compromise of personal information, report the incident to the USM CIO's Office. Refer to Section III for the definition of personal information according to State Government Article, §10-1301 (SB 676 - 2012).

7. Each institution must develop and implement a data retention policy and retirement schedule that includes requirements for confidential data that are no longer needed.

8. Each institution must report on the status of its IT Security Program to the USM CIO on an annual basis. This report is due by August 15th of each year. The USM IT Security Council has developed a suggested template for the format of this report.

III. Confidential Information Standard

1. USM has defined confidential data to include:
    - Under State Government Article, §10-1301 (SB 676 - 2012), personal information is defined as:

      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.

    - 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

    - In addition, any Protected Health Information (PHI), as the term is defined in 45 Code of Federal Regulations 160.103 (HIPAA)

2. Institutions must implement measures to protect confidential information from disclosure in conformance with applicable State of Maryland and federal laws.

   Some considerations:
    - Avoid using Social Security Numbers as identifiers whenever possible.
    - Include the issue of disclosure of confidential information as part of the risk assessment
    - Have all employees who have access to confidential information sign non-disclosure agreements
    - Review access controls periodically

3. Institutions must establish an institutional policy for the protection of confidential information. The policy must outline the protection measures that the institution uses to protect confidential information at rest or in transit across

networks. Protection measures can include the deletion of unneeded confidential information, the encryption of confidential information, or other equally secure safeguards. If encryption is used to protect confidential information, the USM encryption standards, in section IX of this document, must be followed.

4. Institutions must have a documented framework for applying appropriate access controls, based on data criticality and sensitivity. Also, 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 following standards apply to all critical systems, including those containing confidential information:

1. Institutions must have documented procedures for creating, managing, and rescinding user accounts. Minimally, the procedures should address:
   - Eligibility criteria for getting accounts
   - Processes for creating and managing accounts including:
     - Processes for obtaining users' agreements regarding the campus Acceptable Use Policy (AUP)
     - Processes for managing the retention of user account information

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

   A. Prohibit group or shared IDs, unless they are documented as "Functional IDs." 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. Establish procedures for identifying and retiring group or shared IDs. Passwords associated with functional IDs must not be stored in clear text, must have a minimum of eight (8) characters and consist of mixed alphabetic and numeric characters, and must not be displayed on the screen. Functional IDs are exempt from the other user password characteristics described below.

   B. Follow strong password characteristics and management practices, requiring users to adhere to institutional usage, construction, and change requirements. Considering the heterogeneous computing environments at USM institutions, the following password characteristics and management practices are recommended, but are operationally dependent:
      - Passwords must contain a minimum of eight characters
      - The password must not be the same at the user ID
      - Passwords must not be stored in clear text
      - Passwords must never be displayed on the screen
      - Initial passwords and password resets distributed to the user must be issued pre-expired (unless randomly generated), forcing the user to change the password upon logon
      - Passwords must contain a mix of alphanumeric characters. Passwords must not consist of all numbers, all special characters, or all alphabetic characters
      - Passwords must not contain leading or trailing blanks
      - Automated controls must ensure that passwords are changed at least annually for general users, and at 90-day intervals for administrative level accounts

- Password reuse must be prohibited by not allowing the last 10 passwords to be reused with a minimum password age of at least two days
- User IDs associated with a password must be disabled for a period of time after not more than six consecutive failed login attempts, while allowing a minimum of a 10-minute automatic reset of the account, for critical administrative systems containing confidential information
- 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

Federal Electronic Authentication Guideline

An acceptable alternative for authentication that is based on federal authentication guidelines is the *Electronic Authentication Guideline,* as outlined in NIST Special Publication 800-63.

To determine password parameters, construction rules and authentication protocols, perform the following:

- Conduct a risk assessment for e-authentication of the system. The risk analysis measures the severity of potential harm and the likelihood of occurrence of adverse impacts to the system, if there is an error in identity authentication.
- Map identified risks to the applicable assurance level. After all of the risks have been identified, institutions should tie the potential impact of the risks to the proper level of authentication to be implemented.
- Select technology based on e-authentication technical guidance.

The required level of authentication assurance should be determined, based on the potential impacts of an authentication error on:

- Inconvenience, distress, or damage to standing or reputation;
- Financial loss or liability;
- Harm to the organization or public interests;
- Unauthorized release of sensitive information;
- Personal safety; and/or
- Civil or criminal violations.

OMB defines four levels of authentication assurance for electronic transactions and identifies the criteria for determining the level of e-authentication assurance required for specific applications and transactions. These criteria are based on risks and their likelihood of occurrence. As the consequences of an authentication error and misuse of credentials become more serious, the required level of assurance increases: Level 1 is the lowest assurance, and Level 4 is the highest. The levels are determined by the degree of confidence needed in the process used to establish identity and in the proper use of the established credentials.

Level 1 — Little or no confidence in the asserted identity's validity;

Level 2 — Some confidence in the asserted identity's validity;

Level 3 — High confidence in the asserted identity's validity; and

Level 4 — Very high confidence in the asserted identity's validity.

Once a level of authentication assurance has been established, password parameters, construction rules and authentication protocols should be utilized that correspond with the requirements of NIST SP 800-63, depending on the level of authentication assurance identified.

C. Implement and document processes to 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

D. Implement and document processes for periodically (at least annually) verifying employees' access privileges

3. Authorized users are responsible for the security of their passwords and accounts.

4. Institutions must maintain appropriate audit trails of events and actions related to critical applications and confidential data, as required by state and federal laws/regulations. Further, these significant actions and 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 the application

5. Institutions must ensure that all critical systems have the ability to log and report security incidents and attempted violations of system security based on an analysis of the risks to the institution. During the risk analysis process, institutions must determine and document in writing the method and frequency with which the logs and reports will be reviewed.

6. Institutions must segregate the functions of system administration, programming, processing/authorizing business transactions, and security administration, providing for the appropriate separation of duties or implement compensating controls to mitigate the risk.

V. Network Security Standard

Local Network Access

1. Network devices 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.

2. Authorized users shall adhere to the Agency's Policy on Acceptable Use of the Information Infrastructure.

3. In accessing the network, authorized users shall adhere to, and network connecting devices shall conform to, the policies set forth in this document.

Dial-in Access

4. Institutions must develop processes for approving and managing:
   - Dial-in desktop modems
   - Remote control software (e.g., PCAnywhere)
   - Network scan tools

5. Institutions must institute appropriate controls for remote access services
   - Logging of access
   - Protecting critical data in-transit (e.g., encryption)

Banner Text

6. Institutions must have a banner text displayed at all system authentication points where initial user logon occurs (refer to the account administration processes in the Access Control Standard). Use the State banner text or functionally compatible language approved by campus counsel

Firewalls and Network Devices

7. Institutional networks must be protected by firewalls at identified points of interface as determined by system sensitivity and data classification. Firewalls should be configured to block all services not required and disable unused ports, hide and prevent direct accessing of trusted network addresses from untrusted networks, and maintain comprehensive audit trails. Management access must be limited to appropriate personnel; and must utilize a secure communication channel (encryption).

8. All network devices (e.g., servers, routers) should have all non-needed services disabled and the security for those devices hardened. All devices must have updates and patches installed on a timely basis to correct significant security flaws. Default administrator username and password must be changed.

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

10. The responsible campus security personnel must determine the timeframe for applying security patches and updates based on such factors as risk, inter-dependence, and criticality of service.

Intrusion Detection and Intrusion Prevention Systems

11. Institutions must establish automated and manual processes for intrusion detection and/or prevention.
    - Host-based, network-based, or a combination of both (preferred) may be utilized
    - IDS/IPS alerts must be regularly monitored
    - Institutions must establish a severity and escalation list based upon commonly encountered events that include immediate response capability when appropriate. These plans should be incorporated into the IT Security Program.
    - Management access to IDPS devices must be limited to appropriate personnel.
    - Signatures used in intrusion detection/prevention systems must be updated on a regular schedule.

12. Institutions must develop a Service Interface Agreement (SIA), documenting the scope, use, and restrictions for all external entities connected to the institutional network. This excludes access primarily intended for use by faculty, students, and staff.

13. Access Control Standards for Wireless Networks:

    A. General Controls Standards
        - Complete a security assessment of the wireless system before production implementation. The assessment should include an evaluation of potential risks to the campus networks that are accessible from a wireless domain
        - Maintain a current, documented diagram of the topology of the wireless network and document all wireless access points
        - Ensure proper physical security mechanisms are in place to prevent the theft, alteration, or misuse of access points
        - Internal LAN services that are accessible from wireless networks should utilize encrypted data transmission using unique user authentication
        - Change default administrator credentials
        - Utilize only secure access point management protocols and disable telnet
        - Restrict hardware implementation to utilize Wi-Fi certified devices that are configured to use the latest security features
        - Change default SNMP strings if used, otherwise disable SNMP
        - Change default SSID
        - Implement configuration/change control and management to ensure that equipment has the latest software release that includes security enhancements and patches for discovered vulnerabilities

B. Access Point Configuration
   - All default passwords must be changed
   - If SNMP is not required, the institution should disable it

C. Authentication
   - Wireless networks should authenticate the identity of all users, where necessary, and maintain restricted access to critical resources

VI. Contingency Planning Standard

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

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

- Documentation of each critical system including
  - Purpose
  - 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

Secured IT Areas

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

   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.

   USM institutions are responsible for:
   - Issuing picture ID badges to all employees and contractors
   - Ensuring that all portable storage media containing sensitive information such as hard drives, flash drives, magnetic tapes, laptops, and CDs are physically secured
   - Ensuring that proper environmental and physical controls are established to prevent accidental or unintentional loss of sensitive information residing on IT systems
   - Ensuring that any physical access controls are auditable

Storage Media Disposal

2. 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 SP800-88 *Guidelines for Media Sanitization* such as shredding, incineration, overwriting, or degaussing. Unless a piece of storage media, that contains sensitive data, is being released to a disposal contractor that is under contract with the institution, all storage media, containing sensitive data, shall not be released from the institution's control until the media is sanitized and all stored information has been cleared and documented. This requirement applies to the permanent disposal of all storage media and equipment containing storage media regardless of the identity of the recipient, including equipment transferred to schools. It also applies to equipment sent for maintenance or repair.

   The procedures performed to sanitize electronic media must be documented and retained. Documentation for media sanitization/disposal must be created whether it is done in-house or contracted out to a certified disposal company.

This policy applies to all electronic storage media equipment that is owned or leased (including, but not limited to: workstations, servers, laptops, cell phones and Multi-Function Printers/Copiers).

Media Reuse

3. When no longer required for mission or project completion, media (tapes, disks, hard drives, etc) to be used by another employee in the university must be overwritten with software and protected consistent with the sensitivity of data on the IT storage media. These procedures must be documented.

Data Classification and Storage

4. All institutions must develop 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.

5. All institutions must develop a Data Use Standards document that defines which types of storage can be used to hold each of the classes of data that are outlined in the institution's Data Classification Policy.

6. Institutions must inform their community of the Data Classification Policy and Data Use Standards.

Personnel

7. USM personnel policies regarding recruitment and selection must be followed when hiring IT personnel. When deemed necessary, perform background checks.

VIII. Desktop/Laptop Security Standard

General Controls

1. Institutions must implement the following controls on all institutionally-owned desktop and laptop computers that store and/or access confidential information:
    1. User ID and password to control access at logon. Software must be installed to protect the system from malicious programs such as viruses, trojans, and worms. The software should be configured to update signatures regularly
    2. Implement and document processes for managing exposure to vulnerabilities through the timely deployment of patches

Malware

2. For critical systems, institutions must protect against malicious code (e.g., viruses, worms, Trojan horses, etc.) by implementing solutions that, to the extent possible, include a capability for automatic updates. Intrusion detection/prevention tools and techniques must be employed to monitor system events, detect attacks, and identify unauthorized use of information systems and/or confidential information.

User Administrative Rights

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.

Software Licenses

4. 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.

Personally Owned Data Processing Equipment

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

IX. Encryption Standard

Encryption is a valuable tool for protecting sensitive data. USM institutions must utilize encryption for confidential data (see Section III, Confidential Information Standard). The institution must comply with encryption-related guidance from the National Institute for Standards and Technology (NIST) special publications, the Federal Information Processing Standards (FIPS), and the following USM standards:

- Institutions using encryption must establish minimum standards for its use, such as controlling issuance and protecting cryptographic keys as appropriate
- Documented key management should be established that defines variables such as intervals, distribution and revocation
- 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

In addition, confidential data on all portable devices and media must be encrypted.

X. Virtualization Technologies

Institutions must implement careful planning prior to the installation, configuration and deployment of virtualization solutions to ensure that the virtual 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 costs.

XI. Cloud Computing Technologies

Institutions may find compelling reasons to outsource aspects of their Information Technology environment to a *cloud* service provider. Cloud offerings include Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Network as a Service (NaaS). Cloud providers offer economies of scale, the ability to quickly enable service, and reductions in the costs of maintaining local infrastructure such as data centers and servers.

While there may be advantages to taking a service to the cloud, there is also a loss of local control. Before outsourcing a service to the cloud, an institution must have assessed the risks associated with such a service, the need to ensure data integrity, and the level of accessibility that must be maintained. A service should not be moved to the cloud if the institution regards the risk as too great to accept.

The following activities should be performed during the life cycle of the service:

Preliminary Activities:

- Identify security, privacy, legal, and other organizational requirements for cloud services to meet, as a criterion for selecting a cloud provider. Include, if applicable, in assessment/analysis document requirements for recovery of institutional resources such as data, software, hardware, configurations, and licenses at the termination of the contract.
- Prior to contracting with a cloud service provider, consider the security and privacy controls of a cloud provider's environment and assess the level of risk involved with respect to the control objectives of the organization. A review of the provider's SOC 2 report and/or its responses to the Cloud Security Alliance Critical Controls Matrix is helpful.

Initiating and Coincident Activities:

- Ensure that all contractual requirements are explicitly recorded in the service agreement, including privacy and security provisions, and that they are endorsed by the cloud provider.
- Involve a legal advisor in the review of the service agreement and in any negotiations about the terms of service.
- Periodically, assess the performance of the cloud provider and the quality of the services provisioned to ensure all contract obligations are being met and to manage and mitigate risk.

Concluding Activities:

- Alert the cloud provider about any contractual requirements that must be observed upon termination.
- Revoke all physical and electronic access rights assigned to the cloud provider and recover physical tokens and badges in a timely manner.

XII. Mobile Devices

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. IT Information Security Deviation/Risk Acceptance Standard

An information security deviation/risk acceptance request must be completed by the institution if it is determined that it is infeasible to comply with these standards. The request must be completed by the campus 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.

XIV. Use of Electronic Resources Standard

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.

1. Institutions must develop standards for the use of electronic mail, the Internet, and other institutional computing resources. Institutions must implement measures ensuring the security of electronic communications of sensitive, confidential information.

2. Institutional acceptable use policies must address the issues of copyright infringement as well as the use of unauthorized software.

3. Each USM institution shall have personnel designated for providing authenticated notices of IT incidents and advisories to the institutional user community. Employees other than the designated personnel shall not forward IT incident advisories to the institutional user community.

XV. Record of Revisions

Revision	Date	Section	Description
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

Comments on

GUIDELINES IN RESPONSE TO THE STATE IT SECURITY POLICY

Provided by MITRE

The University of Maryland asked the MITRE Corporation to review the document titled “Guidelines in Response to the State IT Security Policy, Version 2.0”. The Office of the Chancellor and President Loh’s office would like to make a decision regarding the ratification of this Guidelines document as a “standard” by the University System Board of Regents. The following provides MITRE’s comments and recommendations to help inform this decision.

Overall the document provides reasonable policy guidelines. Below, we identified areas for enhancement and expansion on the scope of the guidelines.

1. Consider changing the title of the document from "Guideline" to something like “Control Standard”. “Guideline” is not authoritative enough and it could be interpreted as optional. The intent is probably to make this mandatory.

   USM comments: Changed the title to USM IT Security Standards to reflect the repurposed document.

2. The definition of "critical systems" should be very clear. The statement: "Identify critical systems – high value, high risk, critical service, critical data" should be clarified. For example, state that if you have SSNs on your system it is a critical system; and if you have healthcare information on a system it is critical, etc. Clarity is important because the university allows non-IT staff and faculty to stand up IT systems. Furthermore, such detail can inform what system audits and scans should be looking for.

   USM comments: Modified Section II.2, IT Security Program Standard, to clarify the definition of critical systems. The standard states: Identify systems that process and/or store confidential data as defined in Section III, Confidential Information Standard.

   a. Non-public information is not defined. It is important to carefully

define non-public information and make this definition understandable to non-IT system owners.

USM comments: Renamed Section III, Nonpublic Information Standard to Confidential Information Standard and specifically defined confidential information to include personal information and protected health information.

3. Consider role-specific training within the larger security awareness program. For example, Windows system owners, with administrative privileges, should receive Windows-specific security training to ensure they are able to effectively apply the security policy to systems they manage.

   USM comments: Modified Section II.5 to require documentation and implementation of role-specific training.

4. Consider capturing all access to non-public data in audit trails and reviewing to determine if the access is "appropriate." For example, the person has a business need, the access occurs at a time and from a place that seems reasonable for his/her role.

   USM comments: Refer to modified Section IV.4 and Sections IV.2.C and IV.2.D.

5. Consider requiring encryption on all portable devices and media that hold non-public information. Or if possible, do not store non-public information on portable devices and media.

   USM comments: Modified Section IX, Encryption Standard, to include encryption requirements for portable devices and media.

6. Consider defining a policy for the retirement of non-public data, once it is no longer needed on University IT systems.

   USM comments: Added to Section II, IT Security Program Standard, a new standard requiring USM institutions to implement a data retention policy and retirement schedule.