



**GUIDELINES IN RESPONSE TO
THE STATE IT SECURITY POLICY
Version 1.5**

March 2008

USM IT SECURITY WORKGROUP:

**Suresh Balakrishnan, USM
David Bobart, UB
Mark Cather, UMBC
Mark Fleming, BSU
Mansur Hasib, UMBI
Kevin O'Neil, UMUC
Mitch PreVatte, CSU
Lynn Ray, TU
Robert Sink, UMCES
Fred Smith, UMB
Andrew Smith, CHPDM
Gerry Sneeringer, UMCP
Donald Spicer, USM**

TABLE OF CONTENTS

I.	Introduction.....	1
II.	IT Security Program Standard.....	2
III.	Nonpublic Information Standard.....	4
IV.	Access Control Standard.....	5
V.	Network Security Standard.....	8
VI.	Physical Security Standard.....	12
VII.	Microcomputer/PC/Laptop Security Standard.....	14
VIII.	Encryption Standard.....	15
IX.	Information Security Deviation/Risk Acceptance Standard.....	16
X.	Use of Electronic Resources Standard.....	17
XI.	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 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 Budget and Management (DBM) for state agencies and interprets those standards in the context of the USM institutions. The state standards are described in the document entitled *Information Technology Security Policy and Standards*, which is available on the DBM website at: www.dbm.maryland.gov.

II. IT Security Program Standard

1. Institutions must implement a Security Policy and an associated Security Program. The security program should be documented.
2. Institutions must have a formal risk management process for determining adequate security levels for IT resources.
 - Identify critical systems – high value, high risk, critical service, critical data
 - Perform a risk self assessment
3. Institutions must include security as part of the systems development life cycle
 - Demonstrate that security was considered during the development or enhancement of critical applications
 - Document development and change management for mission critical systems
4. Institutions must document and test disaster recovery plans for critical systems
Suggested reference sites for Disaster Recovery Planning include:
DBM: www.dbm.maryland.gov under Statewide IT Security
NIST: <http://www.itl.nist.gov/lab/bulletns/bltnjun02.htm>
<http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>
CERT: http://www.cert.org/nav/index_purple.html
5. Institutions should create 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
6. Institutions must establish and document processes for responding to incidents, including procedures for responding to alerts and State virus advisories
 - Establish and publicize an incident reporting mechanism
 - Identify the incident
 - Evaluate the incident (Is it an incident?)
 - Investigate, resolve, and document the incident
 - Follow-up, analyzing lessons learned as needed

- Annually, institutional Security Officers should generate statistics summarizing recorded incidents and include this information in the annual security program report
7. Institutions must review external connections for security implications on an annual basis. An external connection is defined as any mechanism through which the network can be accessed by an outside entity from an untrusted network (a computer not resident on the local network).
 - Internet connections
 - Dialup modems
 - Wireless
 - Individually owned computers
 8. Each institution must report on the status of its IT Security Program to the USM CIO on an annual basis. This report will be due by August 15th of each year. In addition, the USM Security Group will develop a suggested template for the format of this report.

III. Nonpublic Information Standard

1. Institutions must implement measures to protect nonpublic information from disclosure in conformance with the Maryland Public Information Act and applicable federal laws. (Note: Guidelines for the various federal laws are being developed by the USM Security Group and will be distributed as they are completed).

Some considerations:

- Avoid using Social Security Numbers as identifiers whenever possible.
 - Include the issue of disclosure of nonpublic information as part of the risk assessment
 - Have all employees who have access to nonpublic information sign non-disclosure agreements
 - Review access controls periodically
2. Institutions must establish an institutional policy for the protection of nonpublic information. The policy must outline the protection measures that the institution uses to protect nonpublic information at rest or in transit across networks. Protection measures can include the deletion of unneeded nonpublic information, the encryption of nonpublic information, or other equally secure safeguards. If encryption is used to protect nonpublic information, the USM encryption guidelines, in section VIII of this document, must be followed.
 3. 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, those data elements should be classified at the higher level of data criticality, as determined by the institutions involved (Reference: State IT Security Policy standard 5.1).

IV. Access Control Standard

The following guidelines apply to all critical systems, including those containing nonpublic 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:
 - Process for obtaining users' agreements regarding the campus AUP
 - Process for managing the retention of records
 - The Acceptable Use Policy (AUP) must address the teleworker's responsibility for maintaining a secure home computing environment
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
 - B. Follow strong password characteristics and management practices, requiring users to adhere to institutional usage, construction, and change requirements. The following password characteristics and management practices are recommended:
 - The user must select and/or change initial passwords, unless those passwords are randomly generated
 - Passwords must contain a minimum of six characters
 - When a user password is reset or redistributed, the identity of the user must be validated

Considering the heterogeneous computing environments at USM institutions, the following password characteristics and management practices are recommended, but are operationally dependent:

- 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
- Passwords should not contain more than two consecutive identical characters

- Automated controls must ensure that passwords are changed at least as frequently as every 90 days for high-privilege users and every 180 days for general users
- 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 nonpublic information

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. Guidance for conducting a risk analysis is available in OBM Circular A-130 and in [NIST SP 800-30, Risk Management Guide for Information Technology Systems](#).
- 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. Institutions must maintain appropriate audit trails of events and actions related to critical applications and 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 highly privileged users
 - Additions and changes to users' access control profiles
 - Direct modifications to critical data outside the application
 4. Institutions must ensure that all critical systems have the ability to log and report specific security incidents and all attempted violations of system security. In addition, institutions must establish and document processes for reviewing IT security violations on a daily basis.
 5. Institutions must segregate the functions of system administration, programming, processing, or authorizing business transactions, and **security administration**, providing for the appropriate separation of duties.

V. Network Security Standard

Dial-in Access

1. Institutions must develop processes for approving and managing:
 - Dial-in desktop modems
 - Remote control software (e.g., PCAnywhere)
 - Network scan tools
2. Institutions should institute appropriate controls for remote access services
 - Logging of access
 - Protecting critical data in-transit (e.g., encryption)

Banner Text

3. 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

4. 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. Institutions should consider establishing dedicated platforms for firewalls.
5. 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 and initial passwords should be changed upon installation of all firewall and network equipment.
6. Implement ingress and egress filtering at the edge of the institution's network to prevent IP spoofing.
7. 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

8. 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.
9. 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.
 10. Institutions must make available antivirus software for use at home and provide education regarding security issues. Employees working from home must accept responsibility for the security of their home computing environments.
 11. Institutions should develop and implement acceptable configurations for accessing applications using mobile code.
 12. Access Control Standards for Wireless Networks:
 - A. General Controls Guidelines
 - 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
 - Perform periodic assessments for access point discovery
 - Perform periodic security testing and assessment of the wireless network
 - Implement configuration/change control and management to ensure that equipment has the latest software release that includes security enhancements and patches for discovered vulnerabilities
 - Implement standardized configurations to maintain wireless network security, to ensure change of default values, and to ensure consistency of operations
 - Implement security training to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies
 - Monitor the wireless industry for changes to standards that enhance security features and for the release on new products
 - **Wireless networks should facilitate some form of cryptographic protocol, where necessary, examples being secure shell (SSH), Transport-Level Security (TLS), Internet Protocol Security (IPsec), or Virtual Private Networks (VPN)**
 - Use encryption (i.e., SSL, VPN or other) for any transmission of or access to sensitive information

- Additional countermeasures such as strategically locating access points, ensuring firewall filtering, and blocking and the installation of antivirus software should be implemented
- Ensure that all access points are administered from the wired LAN and never the wireless network

B. Establish a wireless security plan which must include:

- Identify who may use the technology
- Identify whether Internet access is required
- Describe who can install access points and other wireless equipment
- Provide guidelines on the location of and physical security for access points
- Describe the type of information that may be sent over wireless links
- Define standard security settings for access points
- Describe limitations on how the wireless devices may be used
- Provide guidelines on reporting wireless security incidents
- Define the frequency and scope of security assessments to include access point discovery

C. Access Point Configuration

- All default passwords should be changed
- If SNMP is not required, the institution should disable it
- If SNMP is required, institutions should use SNMPv3 or higher

D. Authentication

- Wireless networks should authenticate the identity of all users, where necessary

E. Intrusion Detection and Prevention Systems

- Institutions should monitor wireless networks to identify potentially infected devices

13. PBX Security

A. Disaster Recovery Planning

- See section II *IT Security Program Standard*, item 4.

B. Physical security

- See section VI Physical Security Standard

C. Change controls

- Log internal or external changes/access/deletes to PBX software; adhere to section II IT Security Program Standard, item 3.

D. Switch Software Updates

- Establish a patch management program for addressing emerging vulnerabilities with updated software.

E. Maintenance Port Access Security

- If switch maintenance is performed via modem:
 - Change modem telephone number every 90 days.
 - Disconnect modem when not in active, authorized use.
- If switch access is controlled by a password, change password every 90 days
- Log all access to switch software

Note: The use of remote access/modem security devices, as supported by some PBXs, such as encrypted one-time passwords (challenge/response scenario), remote access logging, login lockout, and security violation notifications, may provide alternate compensating controls.

F. Direct Inward System Access [DISA]

- Discourage activating this feature; document reasons for enablement

G. Call Detail Recording

- This facility should be activated and call activity monitored.

14. Data transmitted by facsimile must be protected to the same level as any data communicated by network or PBX, based on system sensitivity and data classification.

VI. 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, diskettes, 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, diskettes, compact disks, tape cartridges, ribbons, and other similar items **that contain sensitive data** shall be destroyed by a NIST-approved method such as shredding, incineration, overwriting, or degaussing. All IT equipment shall not be released from the university's control until the equipment is sanitized and all stored information has been cleared and documented. This requirement applies to all permanent disposal of equipment regardless of the identity of the recipient, including equipment transferred to schools. It also applies to equipment sent for maintenance or repair.

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 should be overwritten with software and protected consistent with the sensitivity of data on the IT storage media. These procedures should be documented.

Storage and Marking

4. IT systems and electronic media should be protected and marked respectively in accordance with the data sensitivity. Users should not store sensitive data on electronic media that cannot be adequately secured against unauthorized access. Data to be electronically transferred to a remote storage location should be transferred only by a secure method.

Personnel

5. USM personnel policies regarding recruitment and selection should be followed when hiring IT personnel. When deemed necessary, consider performing background checks.

VII. Microcomputer/PC/Laptop Security Standard

General Controls

1. Institutions must implement the following controls on all institutionally-owned microcomputers that store and/or access nonpublic information:
 - User ID and password to control access at logon
 - Employees will be held accountable for securing sensitive information on portable computing devices when the devices are taken out of the workplace
 - Standard virus protection programs must be installed, updated, and maintained on all microcomputers, LAN servers, and mail servers. These programs must:
 - Be configured to run checks for viruses at startup and operate in memory-resident mode to check for viruses during normal processing
 - Be updated as soon as updates are available from the vendor

Software Licenses and Use

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

Laptop Security and Mobile Computing

3. Institutionally owned laptops used to access sensitive information on State systems shall meet the same security standards as desktops used for those purposes.

Personally Owned Data Processing Equipment

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

VIII. Encryption Standard

Encryption is a valuable tool for protecting sensitive data. If an institution decides to utilize encryption, the institution should 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 guidelines:

- Institutions using encryption should 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 should have an established process that provides for minimal operational capabilities such as issuance, association and validation

IX. 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 guidelines. 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.

X. 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 guidelines 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, nonpublic 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.

XI. Record of Revisions

Revision	Date	Section	Description
Version 1.5	Jan. 2008	VIII	Added encryption guidelines
		Cover Page	Modified date and version number and added new members
Version 1.3	March 2008	III	Enhanced III.2 of the NPI standard
	Aug. 2006	Document	Added section numbers and revised the format
		Record of Revisions	Added Record of Revisions section
		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.
			Changed 9 th bullet to allow for a 10-minute automatic reset
		IV.2.E	Deleted
		V.8	Added intrusion prevention systems
		V.12.E	Added intrusion prevention systems
V.13	PBX Security guidelines added		
VI.4	Added guidance for data electronically transferred to a remote storage location		