USM IT SECURITY STANDARDS

Version 5.0

Revised June, 2022

USM IT SECURITY COUNCIL:

Lori Bennett, FSU
David Bobart, UB
Mark Cather, UMBC/USM
Duke Darrigo, SU
Michael Eismeier, USM
Kurt Florez, UMES
Cory Gekoski, UMB
Chinitra Graham, UMGC
Fred Hayes, USM
Edward Hodges, UB
Kiki Iyiegbu, BSU
Michael Kaiser, TU
James Kevin Moran, UMSG
Fred Smith, UMB
Gerry Sneeringer, UMCP
Michael Von Paris, TU
Rickey Williams, CSU

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 (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 https://csrc.nist.gov/publications/sp.

II. IT Security Program Standard

2.1   Institutions must implement a Security Policy and an associated Security Program. The Security Program must be documented and monitored. The CIO or designee must approve institutional security policies. Institutions must periodically assess IT security controls for effectiveness, develop and implement plans for corrective action, and monitor the effectiveness of information security controls on an ongoing basis.

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

2.3   Institutions must have a formal process for the periodic assessment of risk to operations, assets, individuals and reputation, resulting from the operation of information systems and the associated processing, storage, or transmission of confidential information. Once developed, the institutional risk assessment must be reviewed annually for changes in the risk environment; and at least every four years, the institutional risk assessment must be fully updated and revised. The institutional risk assessment process must include identification of systems that process and/or store confidential information, as defined in "Appendix A: Information Classification", and other high-risk systems. Institutional risk assessment processes will be based on the application of the framework in NIST SP 800-37, Risk Management Framework for Information Systems and Organizations. The institutional risk assessment must include a list of systems and other services defined as "high-risk" by the institution.

   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 will perform an institutional risk assessment and reasonably address the risks posed by confidential information on personal or contractor-owned devices and services.

2.5   Institutions must have documented Change Management procedures in place. Changes with material impact on the security of high-risk IT assets (e.g., firewall rules changes, granting of administrative rights, etc…) must be tracked, reviewed, and approved by a person who does not have a conflict of interest in the approval.

2.6   Institutions must develop and promulgate a Data Classification Policy. The 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. This policy must specify the data that can only be accessed by university-managed devices.

2.7   Institutions must have documented systems (hardware, software, network, or a combination) development lifecycle (SDLC) plans, including the phases of initiation, acquisition/development, baseline configurations and inventories 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. This standard applies to high-risk systems as defined by the institution.

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). See NIST Special Publication 800-160 Volume 1 for helpful guidance.

2.8   Institutions must conduct quarterly vulnerability scans against institutionally-managed high-risk servers and network devices (whether on-premise or in the cloud, consistent with the institutional risk program), and those results must be submitted to USM Internal Audit.

2.9   Institutions must provide security awareness training that covers essential university system and institution-specific security policies and security procedures. All training activities must be documented. At a minimum, the documentation must include the name of the community member, date of training, and information about the training material delivered.

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.

2.10   Institutions must create an Incident Response Plan based on the "USM IT Incident Response Plan" Template. Incidents involving the compromise of personal information (as defined under State Government Article 10-301, see Section III) or confidential information (as defined in Appendix A of these standards) must be reported to security@usmd.edu.

The USM IT Incident Response Plan Template can be downloaded from: https://itsecurity.usmd.edu

2.11   Institutions must report annually to the senior leadership of the institution on the risk posed to the institution by information technology, cybersecurity, and privacy to the institution. This report must be on record at the institution and must be available upon request from the USM.

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.

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

2.14 Institutions must comply with the Digital Millennium Copyright Act and designate a single point of contact for inquiries about copyright violations.

2.15 Institutions must establish a policy and implement measures to protect Confidential Information from disclosure in conformance with applicable State of Maryland and federal laws. These include having an institutional acceptable use policy, not using confidential information as identifiers, and having an institutional confidentiality/non-disclosure policy or requiring non-disclosure agreements prior to granting employees access to confidential data.

(Note that there is value in reducing the footprint of confidential information in the institution's environment to the extent that this is possible.)

2.16 USM institutions must utilize encryption for Confidential Information and Protected Health Information 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. When institutions utilize encryption, techniques such as whole disk encryption, file encryption, database encryption, and network-based encryption must be chosen as appropriate to address the risks posed to the institution by the information on the system. Any encryption utilized by an institution must be implemented in a manner which prevents loss of data and ensures continued appropriate access to information and systems. Where applicable and necessary for the institutional risk management program, encryption must be used with 3rd party IT solutions to protect Confidential Information.

(See NIST Special Publication 800-52 Rev.2 for guidance on encryption of data in transit, and FIPS 140-2 for guidance on encryption of data at rest).

2.17 When confidential 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 (i.e. the member of the institution with responsibility for the data).

III. Auditability Standard

3.1   Commensurate with risk, institutions must maintain appropriate audit trails of events and actions related to all on premises and 3rd party IT systems and physical access controls. Audit trails and events must be regularly monitored for indications of suspicious, unusual, unlawful, unauthorized, or inappropriate activity. Signs of compromise or other high-risk events must be immediately reported to appropriate officials for prompt resolution.

   Examples of significant events which should be reviewed and documented (where possible) include additions/changes to critical applications, actions performed by administrative level accounts, additions and changes to users' access control profiles, and direct modifications to critical data outside of the application. Where it is not possible to maintain such audit trails, the willingness to accept the risk of not auditing such actions should be documented.

3.2   Institutions must monitor all audit solutions to detect any audit system failures. Any failures of the audit solution must immediately be reported to appropriate officials for prompt resolution.

3.3   All on premises and 3rd party systems must have synchronized clocks so that audit records can be accurately correlated between internal and external systems.

3.4   Access to audit information (e.g. SIEM logs) must be restricted in accordance with the principal of least privilege.

3.5   Commensurate with risk, institutions must utilize SIEM and/or other logging mechanisms to maintain audit trails of events and actions where possible.

IV. Access Control Standard

The Access Control Standard applies to all 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
- The institution must, at least annually, audit user accounts with access to confidential data to confirm that the privileges granted to each user are appropriate.
- As an individual's relationship to the institution changes, institutions must modify or remove access to systems and information as appropriate based on established processes.

4.2   Institutions must implement authentication and authorization processes that uniquely identify all users and appropriately control access to high-risk 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. Additionally, non-privileged accounts or roles need to be used when accessing non-administrative functions.

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. Systems which cannot meet the password requirements below must have a risk assessment in place accepted by the institution and should have mitigating controls in place.

NIST Special Publication 800-63-3 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 SP800-63-3 (or later) document.

4.4　For systems utilizing authentication, institutions must implement session locking after an institutionally defined period of inactivity and retain the session lock until access is reestablished using established authentication and authorization procedures.

4.5　Users must adhere to institutional password usage, construction, and change requirements. Systems must comply with EITHER (4.5.a or 4.5.b) AND (4.5.c) below:

  a.　Meet the eAuth guidelines as outlined in 800-63-3B Section 5.1.1.2 Memorized Secret Authenticators;
<div align="center">or</div>

  b.　Meet the following alternative requirements:
- Minimum password length: 12 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

  c.　Follow the following password management practices:
- Password must not be the same as the user ID
- Store and transmit only encrypted representation of passwords
- 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

4.6   Institutions must either adopt a plan to implement multi-factor authentication (MFA) that includes consideration of high-risk systems and user access privileges, or have MFA in place for such systems.

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

4.8   Third party and/or vendor access to high-risk systems must be approved and controlled by the department(s) that directly manage the system or software being accessed.

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 (e.g., VPN, VDI, Remote Desktop) must include logging of access and encryption of critical data in-transit.
- Remote access, execution of privileged commands, and any access to confidential data must be authorized prior to allowing connection.
- Remote access must be routed through managed access control points.

5.3 Banner text approved by Legal Counsel must be displayed at all system authentication points where initial user logon occurs, when technically possible and when doing so is not detrimental to the function of the network or system.

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 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, or have compensating controls in place. Vendor-provided administrator username (if possible) and password must be changed.

5.6 Updates and patches must be installed on all network devices in a timeframe determined based on factors such as risk, interdependence, and/or prevention. Patches deemed "critical" must be installed as soon as possible/practical, no later than quarterly. Justification for delay or non-implementation of critical patches should be documented.

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

5.8 Institutions must establish automated and manual processes for intrusion prevention and/or detection.
- Host-based or network-based, must be utilized
- There must be an escalation plan based on commonly encountered events that include immediate response capability when appropriate
- Limit access to make configuration changes to appropriate personnel as defined by the institution.
- Detection signatures must receive regular updates and remain current.
- If interrogation of encrypted network traffic is not technically feasible, compensating controls must be in place on high-risk systems.

VI. Disaster Recovery & Incident Response Standard

This standard is intended to ensure that USM Institutions have documented procedures in place and are sufficiently prepared to address incidents and unforeseen circumstances which may cause negative impact on a USM institution. The procedures should detail the appropriate response to both Security Incidents and Service Interruptions (e.g. unavailability of mission-critical systems, networks, services, or personnel).

6.1 Institutions shall develop and implement an IT Incident Response Plan and IT Disaster Recovery Plan. Institutions may maintain separate disaster recovery and incident response plans or merge them into one plan. If merged, the required concepts of both types of plans must be included in the one planning document.

6.2 IR Plan Requirements: The IT Incident Response Plan must minimally include the items in the "USM IT Incident Response Plan Template". This template can be downloaded from: https://itsecurity.usmd.edu

6.3 DR Plan Requirements: The IT Disaster Recovery Plan must, at a minimum, include the following:

- Documentation of each high-risk 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) or services

See NIST SP 800-34 Rev.1 (Contingency Planning Guide for Federal Information Systems) for additional guidance in developing a Disaster Recovery Plan.

6.4 Institutions must update their IT Incident Response and IT Disaster Recovery Plans annually.

6.5 The institution must test the institution's IT Incident Response Plan at least annually and their disaster recovery plan at least annually. The tests must be documented. If an institution uses their incident response plan or disaster recovery plan to handle a real security or service interruption event, that event may be documented and take the place of the annual test. If a single event or test exercises both the disaster recovery and incident response plans, the one event or test can be used to meet both annual testing requirement.

VII. Physical Security Standard

7.1   Campuses must perform a risk assessment of the physical access controls which are in place protecting the IT facilities (such as server rooms, network closets, and wiring cabinets). Commensurate with this risk assessment, appropriate physical access controls must be in place, such as:

- Maintaining a list of all employees and third parties who are authorized to operate independently and unescorted in secure IT facilities as defined in Section 7.1
- Escorting any individual who is not authorized to operate independently and unescorted in these secure IT facilities and observing their activities at all times while in said facility.
- Ensuring that all portable storage media containing confidential 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 critical information residing on IT systems
- Ensuring that physical access devices are controlled and managed appropriately, and (commensurate with risk) that physical access is auditable.

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

7.2   When no longer usable, electronic storage media that contain confidential 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.

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

7.4   Media must be cleansed in accordance with NIST SP 800-88 before being released internally for reuse. The cleansing technique used should be commensurate with the risk associated with the data stored on that media.

VIII. Endpoint Security Standard

This section applies to Institutionally Owned Devices. These requirements are commensurate with risk and <u>must</u> be applied to the extent that they are practical.

8.1   Controls must be implemented on all endpoints:
- User ID/password, Complex Passcode, Biometric, or other widely accepted authentication technology must be required to access the device.
- Implement appropriate solutions that detect malware and update automatically to identify new threats.
- Host-based firewalls <u>should</u> be operational and properly configured to protect the device when it is outside of the secured institutional network.

8.2   Identify confidential information stored on systems. Where possible and practical, institutions must minimize the storage of confidential information on endpoint systems.

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

8.4   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.

8.5   The institution must establish a procedure for reporting lost/stolen devices and the ability to remotely locate lost/stolen devices.

8.6   The institution must establish a procedure for the remote removal of institutionally-owned data from devices.

IX. Third-Party/Cloud Technology Services Standard

This Standard is intended for USM Institutions that choose to outsource technology services to third-party cloud providers

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*

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 where there is a potential for high risk to the institution. See Appendix A: Definition of Confidential Information to determine the classification of data involved.

9.1   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

9.2   Institutions must annually 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.

9.3   Third-party contracts should include the following as applicable:

- 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 destruction, loss, alteration, or damage to the materials;
    - unauthorized access to confidential information
    - unauthorized access to the services and materials; and
    - 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 9.1). 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.
- 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:

- o The unilateral right of the Service Provider to limit, suspend, or terminate the service (with or without notice and for any reason).
  - o 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) [reference Section III – Auditability Standard]

X. Policy on Non-Institutionally-Owned Devices and Services

Each institution must develop guidelines to govern the use of non-institutionally owned devices (such as personally owned laptops and other computing devices) and non-institutionally purchased/controlled services (such as personally purchased file storage services) for access to institutional resources. These guidelines must address the following areas:

- Risk of confidential data falling into the wrong hands.
- Risk of mission-critical data being lost to the institution (e.g. important research data being outside of the institution's backup scheme).
- Risk of institutional data being stored in non-institutionally purchased/controlled services (e.g. private Google Drive, DropBox, etc.).
- Develop an Institutional Agreement with staff that addresses the following responsibilities of the end-user:
  - Take reasonable steps to secure such a device;
  - Take reasonable steps to secure their home network;
  - Report any potential compromise or loss of the device being used to access institutional resources;
  - Ensure that only an authorized user can use the device to access institutional resources; and
  - Destroy/remove all institutional data upon separation from the institution, or upon the request of the institution.

Appendix A: Information Classification

Institutions should organize their policies and procedures based on the following data classifications.

- Educational Records: 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.
- Protected Health Information: Any Protected Health Information (PHI) as the term is defined in 45 CFR 160.103 (HIPAA).
- Confidential Information: Personal information as defined in the Maryland Code under State Government Article, §10-1301 - §10-1308:

> 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.

Additionally, institutions should consider the risk posed by information under the following laws and regulations:

i. Gramm-Leach-Bliley Act (GLBA)
ii. Federal Trade Commission Red Flag Rules
iii. Payment Card Industry / Data Security Standards (PCI/DSS)
iv. Maryland Confidentiality of Medical Records Act (MCMRA)