DRAFT Information Security Standards

I. Introduction of Standards

Information Security Standards support the security posture of the University of Maine System ("the University"). These Standards specify a required level of attainment of University security controls, and prescribe ways in which the University will enforce the Information Security Policy.

University entities may adopt supplemental standards, so long as they do not lessen or contradict the University Information Security Policy and these Standards.

Standards are consistent with, and derived from, recognized standards organizations, including but not limited to, the National Institute of Standards (NIST), International Organization for Standards (ISO), and Federal Information Processing Standards (FIPS).

II. Security Objectives

The security objectives for information and information systems are:

CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

INTEGRITY: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

AVAILABILITY: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

III. Standards

The following are Standards for attainment of University Information Security Policy controls.

11. **Risk Assessment**
12. **Security Assessment**
13. **System and Communications Protection**
14. **System and Information Integrity**

Adherence to these Standards is mandatory for all users and entities, internal and external. Exceptions to these Standards are addressed in section **VII. Exception to Standards**.

IV. IT Security Standards

1. IT Security Standard: Access Control

Required for all data and systems:

1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Identify authorized users, i.e., through a process that verifies the identity of the user when requesting a new account or system access, and with an approval process, i.e., by a supervisor or department head. Employ the principles of least privilege and need to know when authorizing user access. Review active accounts on a prescribed basis to ensure they are still authorized.

1.2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Define access privileges by account, type of account, or both; i.e., through individual, shared, group, system, guest, emergency, developer, vendor, or temporary accounts. Other account attributes may be restrictions on time-of-day, point-of-origin.

1.20 Verify, control and limit connections to and use of external systems.

External systems are systems or system components for which the University does not have direct supervision of and authority over the application of security controls, i.e., BYOD, vendor, Cloud; but also includes other systems within the University beyond the defined system boundary, for example, systems from or to which data or processes flow but that do not necessarily have the same security controls.

1.22 Control information posted or processed on publicly accessible systems.

Identify individuals authorized to post information on publicly accessible sites, and ensure procedures to review content prior to posting, and to remove content if posted inappropriately.

Additionally, required for all data/systems with a University classification of Internal or Confidential:

1.3 Control the flow of information in accordance with approved authorizations.

Maintain policy on information flow restrictions between individuals. Utilize documentation such as information flow diagrams. Utilize authorization for information flow between individuals, for example, data manager or other authorized approval.

1.5 Employ the principle of least privilege for user accounts, systems administration and/or privileged accounts, and security functions.

The goal of least privilege is that privileges no higher than necessary are authorized, and allocation of privileges are limited to the minimum necessary. Privileged accounts include superuser user accounts, superuser systems administrator accounts, and for development and implementation accounts. Logging may be employed to monitor use of privileged accounts, and access authorizations may be configured to limit functions that are executable by accounts.

1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.

Define nonsecurity functions, and require use of non-privileged accounts when accessing non-security functions, i.e., through documentation and policy, and access control tools or configuration that limit security functions available to non-security accounts.

1.8 Limit unsuccessful logon attempts.

Utilize tools, i.e., documentation, policy and technical controls, to define the limits on the number of logon attempts, and lockout periods and procedures for releasing account locks.

1.9 Provide privacy and security notices consistent with data classification and rules.

Display warning banners before individuals log on to systems, or alternatives such as a signed terms of use authorization.

1.10 Use session lock and termination mechanisms to prevent access to and viewing of data after a period of inactivity.

Define the period of inactivity, and implement configuration or similar rules to prevent access after the period of inactivity, and pattern-hiding while locked.

1.12 Monitor, control and restrict remote access sessions.

Utilize tools to document functionality, terms and conditions for remote access, and authorization where applicable and commensurate with risk (i.e., supervisor or department head approval), for example, documentation and policy. Utilize tools, for example, VPNs, to enhance confidentiality of remote access sessions. Utilize automated tools to monitor for cyber attacks and compliance with policies.

1.14 Route remote access via managed access control points.

Utilize system design documentation, and configuration settings.

1.16 Authorize wireless access prior to allowing such connections.

Utilize tools to authorize wireless access, i.e., authentication protocols, credential protection, mutual authentication.

1.21 Limit use of portable storage devices on external systems.

External systems are systems or system components for which the University does not have direct supervision of and authority over the application of security controls, i.e., BYOD, vendor, Cloud; but also includes other systems within the University beyond the defined system boundary, for example, systems from or to which data or processes flow but that do not necessarily have the same security controls.

Additionally, required for all data/systems with a University classification of Restricted:

1.4 Separate duties of individuals to reduce the risk of malevolent activity without collusion.

Separate operational functions, system support functions (including management, programming, quality assurance, testing, security, etc.), and administration of audit functions. Assign duties requiring separation to separate individuals.

1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Non-privileged users are individuals that are not appropriately authorized for privileged functions, i.e., system support functions, creating and maintaining system accounts, performing system integrity checks, patching, or managing cryptographic keys and mechanisms. For example, non-privileged users should be unable to circumvent intrusion detection and prevention, or malicious code protection. Define privileged functions, define non-privileged users and prevent from executing privileged functions, and capture the execution of privileged functions in audit logs.

1.11 Terminate (automatically) a user session after a defined condition.

Document the defined condition/period, and ensure sessions are automatically terminated in accordance with this condition/period.

1.13 Employ (identify and implement) cryptographic mechanisms to protect the confidentiality of remote access sessions.

Identify and implement cryptography.

1.15 Authorize remote execution of privileged commands, and remote access to security-relevant information.

Identify commands and security-relevant information, and authorize, for example, by using documentation or technical controls.

1.17 Protect wireless access using authentication and encryption.

Authenticate individuals and devices that access system(s), paying particular attention to the IoT.

1.18 Control connection of mobile devices.

A mobile device is a device that is easily carried, designed to operate wirelessly, possesses removable or non-removable data storage, and includes a self-contained power source. Restrictions on mobile devices may include, for example, configuration management, device identification and authentication, mandatory protective software, malware scanning, virus protection, mechanisms to ensure critical updates and patches, and limiting to only essential hardware and apps. Identify allowed mobile devices, and authorize connections to/from those devices. Log and monitor mobile device connections.

1.19 Encrypt information on mobile devices and mobile computing platforms.
Encrypt information, and encrypt mobile devices.

2. IT Security Standard: Awareness and Training

Required for all personnel and entities, internal and external:

2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities; and of the applicable policies, standards, and procedures related to the security of those systems.
Training will include an understanding of information security, necessity, and user actions to maintain security and respond to suspected incidents; and awareness of operations security. Techniques can include training, email advisories, logon screen messages, posters and awareness events.

2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
Identify security roles and responsibilities, and security requirements. In addition to all users, provide where applicable, role-based training to developers, architects, procurement, administrators, and assessors.

Additionally, required for all personnel and entities, internal and external, with access to data/systems with a University classification of Restricted:

2.3 Security awareness training includes recognizing and reporting potential incidents introduced by staff and trusted partners (“insider threat”).
Insider threat is a term describing vulnerabilities introduced by employees and trusted partners. It may include mistaken, negligent or malicious action that compromise security controls, for example, sending sensitive information to an unintended recipient via email, being unaware of or not following security policy and procedures, or deliberate unauthorized disclosure of information or bypass of security controls.

3. IT Security Standard: Audit and Accountability

Required for all data/systems with University classification of Internal or Confidential (not required for data/systems with a classification of Public, but recommended):

3.1 Create and retain system audit logs and records in order to enable monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
Identify events that may include unlawful or unauthorized system activity, and which are significant and relevant to the security of systems and environments. For example, log password

changes, failed logons or accesses, use of administrative privileges, or use of third-party credentials, and date/time of the event.

3.2 Ensure that the actions of individual system users can be uniquely traced to those users.

Ensure the content of audit records is sufficient, and logs are verified as containing the documented content.

3.3 Review and update logged events.

Periodically re-evaluate the applicability of the types of logged events and adjust if warranted.

3.7 Provide a system capability to compare to and synchronizes internal system clocks with an authoritative source to ensure the integrity of time stamps for audit records.

Define authoritative source and verify integrity of time stamps.

Additionally, required for all data/systems with University classification of Restricted:

3.4 Alert in the event of an audit logging process failure.

Examples of audit logging processes include hardware/software errors, failures in audit record capturing mechanisms, and audit record storage capacity being reached or exceeded. Identify personnel to be notified in the event of a failure and the types of failures for which alerts are generated. Utilize automated alerts.

3.5 Correlate (collectively/across systems) audit record review, analysis, and reporting for the investigation of and response to, indications of unlawful, unauthorized, suspicious, or unusual activity.

Define review, analysis and reporting processes, for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. Correlate review, analysis and reporting.

3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.

Provide audit record reduction to allow more efficient use of high-volume log events.

3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Review security configuration/documentation and ensure that logging tools are performing according to documentation.

3.9 Limit management of audit logging functionality to a subset of privileged users.

Review security configuration/documentation and ensure that logging tools are performing according to documentation.

4. IT Security Standard: Configuration Management

Required for all data/systems with University classification of Internal or Confidential (not required for data/systems with a classification of Public, but recommended):

4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the system development life cycles.

Utilize system inventories/documentation, including baseline configurations. Baseline configurations are documented and reviewed, and include, for example, standard software packages, computers, servers, network components, mobile devices, current version numbers, update and patch information, configuration settings and network topology.

4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.

Baseline security configurations are defined and employed.

4.3 Track, review, approve or disapprove, and log changes to organizational systems.

Change control includes proposal, justification, implementation, testing, review, and disposition of changes, including upgrades and modifications. Changes include scheduled, unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

4.4 Analyze the security impact of changes prior to implementation.

Security impact analysis may include reviewing security plans to understand security requirements, and reviewing design documentation to understand the implementation of safeguards and change impact on safeguards.

4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

Define essential capabilities, and configure systems accordingly.

4.9 Control and monitor user-installed software.

Establish a policy for controlling user-installed software. Monitor installation of software by users, and ensure compliance with policy.

Additionally, required for data/systems with a University classification of Restricted:

4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. Only qualified and authorized individuals may initiate changes, including upgrades and modifications.

Identify authorized individuals, system maintenance policy and procedures, and ensure adherence to documented policy and procedures.

4.7 Restrict, disable or prevent the use of nonessential programs, functions, ports, protocols, and services.

For example, restrict the roles allowed to approve program execution, prohibit auto-execute, program blacklisting and whitelisting, or restrict the number of program instances executed at the same time. Examples or protocols to consider include Bluetooth, FTP, and peer-to-peer networking.

4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of whitelisted software can occur either prior to execution or at system startup.

5. IT Security Standard: Identification and Authentication

Required for all data/systems:

5.1 Identify system users, processes acting on behalf of users, and devices.

Identify users, i.e., through a unique username. Identify users within group accounts, e.g. through a unique username and managed group accounts.

5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Authenticate users, i.e., through a password, key card, or cryptographic device. Revoke authenticators when no longer needed, e.g. for staff, vendors, etc.

Additionally, required for data/systems with a University classification of Internal or Confidential:

5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

Document password complexity, change-of-character requirements, and ensure enforcement of these requirements.

5.8 Prohibit password reuse for a specified number of generations.

Define the number of generations. Utilize policy or technical controls to enforce the restriction.

5.9 Allow temporary password use only for system logons with an immediate change to a permanent password.

Utilize system security plan and technical controls.

5.10 Store and transmit only cryptographically-protected passwords.

Cryptographically-protected passwords include, for example, salted one-way cryptographic hashes of passwords.

5.11 Obscure feedback of authentication information.

Obscuring authenticator feedback includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

Additionally, required for data/systems with a University classification of Restricted:

5.3 Use multifactor authentication for network access to non-privileged accounts, and for both local and network access to privileged accounts.

Consider incrementally: 1 Identify privileged accounts; 2 implement MFA for local access to privileged accounts; 3 implement MFA for network access to privileged accounts; 4 Implement MFA for network access to non privileged accounts.

5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

Replay-resistant techniques include, for example, protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.

5.5 Prevent reuse of identifiers for a defined period.

Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device.

5.6 Disable user/account identifiers after a defined period of inactivity.

Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device.

6. IT Security Standard: Incident Response

Required for all users, entities, and data/systems with a University classification of Internal or Confidential (not required for Public, but recommended):

6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems.

Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive. As part of user response activities, incident response training is provided by organizations and is linked directly to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle or remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification/reporting of suspicious activities from external and internal sources. User response activities also include incident response assistance which may consist of help desk support, assistance groups, and access to forensics services or consumer redress services, when required.

Additionally, required for all users, entities, and data/systems with a University classification of Restricted:

6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Tracking information may include, for example, status, reporting requirements, information for and from forensics, incident details and evaluations of details, trends; and may be collected from, for example, incident reports, response teams, audit, network and physical access monitoring, and user/administrator reports.

6.3 Test the organizational incident response capability upon a prescribed schedule.

Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

7. IT Security Standard: Maintenance

Required for all data/systems with a University classification of Internal, Confidential and Restricted (not required for Public, but recommended):

7.1 Perform maintenance on organizational systems.

This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers.

7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit information, but are used specifically for diagnostic and repair actions on those systems. Controls may include, for example, policy and technical controls.

7.3 Ensure equipment removed for off-site maintenance is sanitized of any sensitive information.

Utilize tools such as policy, and maintenance records.

7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with incident handling policies and procedures.

7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections; and terminate such connections when nonlocal maintenance is complete.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. Enable MFA and require accordingly.

7.6 Supervise the maintenance activities of maintenance personnel without required access authorization (e.g., contractors, vendors, or consultants).

Contractors, vendors or consultants such as information technology manufacturers, vendors, consultants, and systems integrators, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on organizational risk assessments. Temporary credentials may be for one-time use or for very limited time periods. Utilize contracts, service-level-agreements, etc.

8. IT Security Standard: Media Protection

Required for all information, systems and devices:

8.3 Sanitize or destroy system media before disposal or release for reuse; ensuring that any licensed software and data have been removed prior to reallocation or disposal. Attention will be taken to sanitize or destroy removable media.

Sanitize or destroy media before disposal, or reuse.

Additionally, required for all information, systems and devices with a University classification of Internal or Confidential:

8.1 Protect (i.e., physically control and securely store) system media containing sensitive information, both paper and digital.

System media includes digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Protecting digital media includes, for example, limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes, for example, conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. Access to system media can be limited by physically controlling such media, which includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media.

8.2 Limit access to sensitive information on system media to authorized users, e.g. through physical controls or secure storage.

Access can be limited by physically controlling system media and secure storage. Physically controlling system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library.

8.7 Control the use of removable media on system components; for example, flash drives or removable hard drives.

This requirement restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization.

Additionally, required for all information, systems and devices with a University classification of Restricted:

8.4 Mark media with necessary markings and distribution limitations; and include where applicable, the University information classification scheme(s).

Media marking is use of human-readable security attributes, and identifying regulatory, contractual and administrative security obligations. Examples include, where applicable, system warning banners, room or area markings, container markings, mail markings, and page/form markings.

8.5 Control access to media (e.g., physical or procedural safeguards); and maintain accountability for media during transport outside of controlled areas.

For example, utilize secure areas, secure containers (locking bags/cases), and cryptography.

8.6 Implement cryptographic mechanisms to protect the confidentiality of information stored on digital media during transport, unless otherwise protected by alternative physical safeguards.

For example, utilize secure areas, secure containers (locking bags/cases), and cryptography.

8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

Identify individuals, organizations or projects; and use of policy/procedures for ensuring only identified devices are utilized.

8.9 Protect the confidentiality of backup(s) of information at designated storage locations; e.g., cryptographic mechanisms, and/or physical safeguards.

Identify storage locations of backups, and ensure safeguarding.

9. IT Security Standard: Personnel Security

Required for all personnel with access to data/systems with a University classification of Internal, Confidential or Restricted (not required for Public, but recommended):

9.1 Screen individuals prior to authorizing access to organizational systems containing sensitive information.

Utilize policy and physical or technical controls.

9.2 Ensure that organizational systems containing sensitive information are protected during and after personnel actions such as terminations and transfers.

Utilize policy and procedures for terminating system access and credentials upon personnel termination or transfer; e.g. offboarding.

10. IT Standard: Physical Protection

Required for all tangible and intangible assets:

10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

Identify employees or permanent contractors by using badges or identification cards (for non-publicly accessible areas). Place computers, printers, copiers, etc. in a secure area.

10.3 Escort visitors and monitor visitor activity.

Ensure visitors are escorted and activity is monitored.

10.4 Maintain audit logs of physical access (and in accordance with records retention rules).

Define entry and exit points and controls on entry and exit points, and maintain records of electronic access and inventory of physical access devices.

10.5 Control and manage physical access devices, i.e., keys, key cards, combinations.

Verify authorization, i.e., supervisor or department head approval, before issuing physical access devices. Maintain an inventory of physical access devices.

Additionally, required for all tangible and intangible assets with a University classification of Internal or Confidential:

10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.

Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security safeguards applied to the support infrastructure prevent accidental damage, disruption, and physical tampering.

Additionally, required for all tangible and intangible assets with a University classification of Restricted:

10.6 Enforce safeguarding measures for information at alternate work sites.

Alternate work sites include sites where the organization is not in direct or continuous control of safeguarding controls; for example, employee homes, travel destination/locations.

11. IT Security Standard: Risk Assessment

Required for all assets and operations with a University classification of Internal, Confidential or Restricted (not required for Public, but recommended):

11.1 Periodically assess the risk to organizational assets and operations (including mission, functions, image, or reputation); and to individuals resulting from the operation of organizational systems and the associated processing, storage, or transmission of sensitive information.

Define frequency of assessments and perform according to defined frequency.

11.2 Scan for vulnerabilities in organizational systems and applications periodically, and when new vulnerabilities affecting those systems and applications are identified.

Define frequency of assessments and perform according to defined frequency.

11.3 Remediate vulnerabilities in accordance with risk assessments.

The consideration of risk influences prioritization of remediation efforts and the level of effort to be expended.

12. IT Security Standard: Security Assessment

Required for all systems with a University classification of Internal or Confidential (not required for Public, but recommended):

12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application; and on an ongoing basis.

Security assessments ensure safeguards and countermeasures are in place and operating as intended; ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; facilitate risk-based decisions; and ensure compliance to vulnerability mitigation.

12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Plans of action and milestones track timelines, resources and milestones.

12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with and/or connections to other systems.

System security plans correlate security requirements with security controls. They do not provide detailed technical descriptions (rather, are high level), but with enough information to enable design.

Additionally, required for all systems with a University classification of Restricted:

12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Frequency should be sufficient to support risk-based decisions.

13. IT Standard: System and Communications Protection

Required for all systems:

13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

Utilize boundary components, i.e., gateways, routers, firewalls, anti-malware, encrypted tunnels. Utilize documentation/architecture diagrams and any applicable technical tools to identify boundaries.

13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Identify publicly accessible components and implement subnetworks.

Additionally, required for all systems with a University classification of Internal or Confidential:

13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

Collaborative computing devices include, for example, networked white boards, cameras, and microphones.

Additionally, required for all systems with a University classification of Restricted:

13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Ensure effective information security throughout the software/system development lifecycle.

13.3 Separate user functionality from system management functionality.

System management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is physical or logical. Organizations can implement separation of system management functionality from user functionality by using different computers, different central processing units, different instances of operating systems, or different network addresses; virtualization techniques; or combinations of these or other methods, as appropriate.

13.4 Prevent unauthorized and unintended information transfer via shared system resources, e.g., registers, cached or main memory, hard disks or other shared storage or systems resources (also referred to as object reuse and residual information).

This requirement prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system.

13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

Ensure that only connections that are essential and approved are allowed.

13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

This requirement is implemented in remote devices (computers, tablets, etc.) through configuration settings to disable split-tunneling.

13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission; or otherwise protect by alternative physical safeguards.

Examples of components that can transmit information are internal and external networks, servers, laptop and desktop computers, mobile devices, printers, copiers, scanners and fax machines. Consideration should also be given to commercial commodity service providers (as opposed to fully dedicated services).

13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address or port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.

Utilize policy and procedures.

13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of information; and utilize cryptography in compliance with all agreements, laws, contractual or other requirements or recommendations.

Utilize policy and procedures.

13.13 Control and monitor the use of mobile code; and prevent and detect the introduction and use of unauthorized mobile code.

Mobile code includes, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave, Flash, VBScript, and Word/Excel macros.

13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application.

13.15 Protect the authenticity of communications sessions.

Authenticity protection includes, for example, protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into communications sessions. This control addresses communications protection at the session vs. packet level.

13.16 Protect the confidentiality of information at rest (i.e., cryptography).

The focus of protection at rest is not on the type of storage device or the frequency of access but rather the state of the information. Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also employ other safeguards including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest.

14. IT Standard: System and Information Integrity

Required for all systems:

14.1 Identify, report, and correct system flaws in a timely manner.

Monitor for security-relevant updates, i.e., patches, service packs, hot fixes, anti-virus signatures. Remediate in a timely manner noting the timeframe and remediation result documentation.

14.2 Provide protection from malicious code at designated locations within organizational systems.

Utilize anti-malware at system entry and exit points, i.e., firewalls, remote-access servers, workstations, email servers, web servers, proxy servers, and mobile devices.

14.4 Update malicious code protection mechanisms when new releases are available.

Monitor for new releases and implement when available.

14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

Define frequency of scans, and perform according to defined frequency.

Additionally, required for all systems with a University classification of Internal, Confidential or Restricted:

14.3 Monitor system security alerts and advisories, and take action in response.

There are many publicly available sources of system security alerts and advisories.. Identify, monitor, and record action.

14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system. Organizations can monitor systems, for example, by observing audit record activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions.

14.7 Identify unauthorized use of organizational systems.

Define authorized and unauthorized use of systems. Unusual or unauthorized activities or conditions related to inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

V. Exceptions to Standards

Information security and support considerations such as regulatory compliance, confidentiality, data integrity and availability are most easily met when University users employ centrally supported standards. However, it is understood that standards may not always be feasible or appropriate for a user/dept/campus. Exceptions from these Standards may be considered when there is a justifiable business and/or research case, resources are sufficient to properly implement and maintain the alternate configuration, the exception process is followed, and other University policies and standards are upheld.

Request for exception from Standards

Users will submit a Standards Exception Request to their supervisor or Department Chair. The supervisor or Department Chair will then decide if there is a business case for the exception, and forward to the Information Security Office to determine if it is a pre-approved exception, and/or if it meets the criteria for pre-approval. If it is not one of the pre-approved exceptions, the Information Security Office will either authorize the exception, or submit the Standards Exception Request to authorizing individual(s). If the Standards Exception Request is approved, then it is determined if the entity requesting the exception has access to sensitive data. If yes, then the request will be authorized by an identified and designated individual or entity.

Information included for exceptions requests

The Exception Request should contain the following information:

- For which System(s) is/are the Exception Request?
- What is the reason an exception is being requested? What is the business case?
- Who/What is requesting the exception?
- Is the exception intended to be short term, or permanent?
- By when is the exception needed?

Questions that will be considered upon receiving a request:

- What is the estimated impact/risk?
- Is there another way to effectively handle the business case?
- What methods are available to roll back the exception if needed?
- Has the the exception been tested?
- Is it technically feasible?
- Is it practical to maintain?
- Is there a financial cost involved in the exception?
- What is the time schedule for implementation?

VI. Contact Information

For questions or comments on these Standards, please contact the Information Security Office at infosecurity@maine.edu, or 207-581-9105.

VII. Glossary of Terms

Accountability: A process of holding users responsible for actions performed on an information system.
Adverse Effect: A harmful or abnormal result. These are defined examples in FIPS 199 with potential of impact (LOW MODERATE or HIGH) with respect to the likelihood of compromise.
Limited adverse effect: The loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to

perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Serious adverse effect: The loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Severe or catastrophic adverse effect: The loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Alternative work site: Any working area that is attached to the wide area network either through a public switched data network or through the Internet.

Audit: An independent examination of security controls associated with a representative subset of organizational information systems to determine the operating effectiveness of system controls; to ensure compliance with established policy and operational procedures; and to recommend changes in controls, policy, or procedures where needed.

Authentication: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system; see Identification.

Authorization: Access privileges granted to a user, program, or process.

Availability: Timely, reliable access to information and information services for authorized users.

Baseline security requirements: A description of the minimum security requirements necessary for an information system to enforce the security policy and maintain an acceptable risk level.

Compromise: The disclosure of sensitive information to persons not authorized to receive such information.

Confidentiality: The preservation of authorized restrictions on information access and disclosure.

Configuration management: A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle.

Cryptography: The process of rendering plain text information unreadable and restoring such unreadable information to a readable form.

Data: A representation of facts, concepts, information, or instruction suitable for communication, processing, or interpretation by people or information systems.

Decryption: The process of converting encrypted information into a readable form. This term is also referred to as deciphering.

Encryption: See Cryptography.

External network: Any network that resides outside the security perimeter established by the telecommunications system.

External information systems: See Non-Agency-Owned Equipment.

Firewall: Telecommunication device used to regulate logical access authorities between network systems.

Identification: A mechanism used to request access to system resources by providing a recognizable unique form of identification such as a Login ID, User ID, or token; see Authentication.

[User] Identifier: A unique string of characters used by an information system to identify a user or process for authentication.

Information: See Data.

Information system: A collection of computer hardware, software, firmware, applications, information, communications, and personnel organized to accomplish a specific function or set of functions under direct management control.

Integrity: The protection of information systems and information from unauthorized modification to ensure the quality, accuracy, completeness, nonrepudiation, and authenticity of information.

Internet: Two or more networks connected by a router; the world's largest network, which uses TCP/IP to connect government, university, and commercial institutions.

[Cryptographic] Key: Information used to establish and periodically change the operations performed in cryptographic devices for the purpose of encrypting and decrypting information.

Least privilege: A security principle under which users or processes are assigned the most restrictive set of privileges necessary to perform routine job responsibilities.

Malicious code (Malware): Rogue computer programs designed to inflict a magnitude of harm by diminishing the confidentiality, integrity, and availability of information systems and information.

Network: A communications infrastructure and all components attached thereto whose primary objective is to transfer information among a collection of interconnected systems. Examples of networks include local area networks, wide area networks, metropolitan area networks, and wireless area networks.

Non-Agency-Owned Equipment: Any technology used to receive, process, store, or transmit information that is not owned and managed by the agency but is owned by a contractor and centrally managed by their own IT department.

Non-repudiation: The use of audit trails or secure messaging techniques to ensure the origin and validity of source and destination targets (i.e., senders and recipients of information cannot deny their actions).

Organization: An agency or, as appropriate, any of its operational elements.

Password: A private, protected, alphanumeric string used to authenticate users or processes to information system resources.

Potential impact: The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect, a serious adverse effect, or a catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Privileged user: A user that has advanced privileges with respect to computer systems. Such users in general include administrators.

Protocol: A set of rules and standards governing the communication process between two or more network entities.

Risk: The potential adverse impact on the operation of information systems, which is affected by threat occurrences on organizational operations, assets, and people.

Risk assessment: The process of analyzing threats to and vulnerabilities of an information system to determine the potential magnitude of harm, and identify cost effective countermeasures to mitigate the impact of such threats and vulnerabilities.

Router: A device that forwards data packets between computer networks, creating an overlay internetwork.

Safeguard: Apply protective measures prescribed to enforce the security requirements specified for an information system; synonymous with security controls and countermeasures. **Safeguards:** protective Safeguard measures

Security policy: The set of laws, rules, directives and practices governing how organizations protect information systems and information.

System: See Information system.

Threat: An activity, event, or circumstance with the potential for causing harm to information system resources.

User: A person or process authorized to access an information system.

Voice over Internet Protocol (VoIP): A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet protocol networks, such as the Internet.

Vulnerability: A known deficiency in an information system, which threat agents can exploit to gain unauthorized access to sensitive or classified information.