University of Maine System
Information Security Policy

Policy Statement

Purpose: The University of Maine System ("the University") is committed to protecting all information that is either wholly or partially owned by the University, has been entrusted to the University, and that supports the University missions and operations.

Information, regardless of format or system, has intrinsic value and potential adverse impact if the confidentiality, integrity or availability of such information is compromised.

This Policy describes the nature, scope, meaning of, and requirements for controls required to protect University information.

Scope: This Policy provides University faculty, staff, employees, and anyone who accesses or possesses University information, with security requirements for protecting the confidentiality, integrity, and availability of such information. These requirements include, but are not limited to, as prescribed by authorizing law, regulation, policy or other obligation.

Security requirements apply to all components of University personnel, information, and information systems.

University institutions or entities may adopt supplemental policy, standards or other guidance, so long as they do not lessen or contradict this Policy.

Roles and Responsibilities: The Board of Trustees of the University of Maine System ("the Board") is committed to a University-wide Information Security Program and security policy to convey direction and requirements for the appropriate use and protection of University information and information systems.

The Board is committed to an Information Security Office, headed by a Chief Information Security Officer ("CISO"), with the purpose of establishing, maintaining, supporting, enforcing, and assigning security roles in support of, this Policy.

An Information Security Governance Council ensures that this information security policy is implemented effectively and provides oversight to the information security program and alignment with organizational goals. The Information Security Governance Council is to be comprised of cross-functional members and work collaboratively with the Data Governance Council.

The University Information Security Program administers information security in a standards-, risk- and exception-based model. The office ensures continual planning, implementation, review, assessment, monitoring, prioritization, authorization, and improvement of the University information security posture.

The University CISO may assign supporting roles as appropriate, in assurance for and protection of information and information systems confidentiality, integrity and availability. Examples of roles may include, as appropriate, and are not limited to:

- Risk management and assessment
- Systems and security architecture, design and engineering
- Disaster recovery and backup integrity
- Procurement provisions
- Operational and/or user interest representation
- Compliance audit
- Compliance enforcement
- Safety and security of physical environment(s)

University of Maine System
Information Security Policy

Compliance: All individuals regardless of association, including but not limited to, faculty, staff, students, consultants, contractors, and business partners, who access or possess University information are required to comply with this policy.

The University complies with all applicable regulatory, statutory, contract, or other obligations as they pertain to security and privacy, and throughout the information life cycle.

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

Security Control Provisions

The following provisions apply for the security and protection of all University non-publicly accessible information, and, where applicable, for the protections of availability and integrity of publicly accessible information.

Information Security Policy Standards are published for the required level of attainment of this Policy; and for ways in which this Policy will be enforced.

1. **Access Control.** The University will manage access control requirements, including who may access information, and under what circumstances. Access control policy and standards authorize resource usage within or across organizational units, and are based on a need to know information and University authority. Access control policies and standards are enforced through mechanisms that translate a user's access request. The University will maintain access control in a safe state so that no permission can be leaked to an unauthorized or uninvited principal.

2. **Awareness and Training.** Humans and human behaviors are essential elements in a security program. The University will provide security awareness and training to all organizational users to ensure an understanding of information technology security basics and literacy; and address security knowledge for which all employees can reasonably be expected to have in positions and organizational roles.

3. **Audit and Accountability.** The University will ensure sufficient controls to provide auditable evidence for system transactions; that key records are available for a sufficient amount of time; and that in the event of system incidents, there are ways to identify, investigate, recover data, and rollback changes.

4. **Configuration Management.** The University will perform a collection of activities to establish and maintain the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the information and information systems life cycles.

5. **Identification and Authentication.** The University will ensure only established, identified and authorized users and processes interact with information and information systems; and that actions within systems are able to be traced to individuals or processes. Measures include but are not limited to, providing for identification, protection, detection, response, recovery, and restoration of information systems.

6. **Incident Response.** The University will identify, detect, investigate, respond to, report, and recover from security incidents and violations of security policies and practices.

7. **Maintenance.** The University will utilize controlled maintenance, to mitigate risks of unauthorized access or changes to information systems, and of failure to perform information system updates.

8. **Media Protection.** The University will maintain information in a manner that protects its security and integrity, while making it available for authorized use. Security measures are implemented commensurate with the risk to individuals or the University from unauthorized receipt, use, processing, storing, disclosure, modification or destruction; or loss of integrity.

9. **Personnel Security.** The University's ability to create and maintain a security program is based on the people that the University chooses to trust. For each person who has access to University information, the University will assign the correct level of privilege to perform necessary University functions. The University will remove information access when no longer needed.

10. **Physical Protection.** The University will physically protect tangible and intangible assets from physical harm. Physical security may include, but is not limited to, protecting entrances and exits, implementing surveillance systems, and protecting network infrastructure, backups, locks and passwords.

11. **Risk Assessment.** The University assesses risk to information and information systems, including threats, vulnerabilities, likelihood, and impact to operations and assets and other organizations.

12. **Security Assessment.** The University will assess security controls as part of the information life cycle. Security controls are safeguards or countermeasures used to implement security requirements, and ensure they are in place and operating as intended.

13. **System and Communications Protection .** The University will apply security engineering principles to monitor, control and protect communications at external boundaries and key internal boundaries; to prevent unauthorized and unintended information transfer; and to ensure security in systems design.

14. **System and Information Integrity.** The University will ensure the application of security, system configuration, and error handling in an information security program.

Last Revised: 6/24/2020
Last Reviewed: 6/24/2020