Information Security Policies & Standards

Policy as approved by the Board of Trustees on 3/14/2011 is in black print.

Standards (operating draft) as of 8/13/2011 are in blue print.

The University of Maine System Information Security Standards

1 SECURITY POLICY

1.1 INFORMATION SECURITY POLICY

The Board of Trustees of the University of Maine System establishes this information security policy in support of the mission and goals of the University of Maine System ("UMS") and all component entities thereof. The objective of this information security policy is to convey the Board's direction for the appropriate use and protection of UMS information assets and to specify the requirements for protecting those information assets.

This document applies to all UMS faculty, staff, employees, contractors, consultants, business partners and anyone who accesses or possesses UMS information assets.

Compliance with this policy and all supporting standards is mandatory.

1.1.1 Information security policy document

This information security policy document is approved by the Board of Trustees of the University of Maine System and shall be published and communicated to all employees, students, and others permitted access to UMS information assets.

1.1.1 Information in this document refers to information that is either wholly or partially owned by UMS, or that has been entrusted to UMS with the expectation that the information will enjoy protections of confidentiality, integrity, or availability by statute, contract, or other agreement.

1.1.2 Review of the information security policy

This information security policy shall be reviewed annually, or more frequently as significant changes occur in the UMS environment, to ensure its continuing suitability, adequacy, and effectiveness.

2 ORGANIZATION OF INFORMATION SECURITY

2.1 INTERNAL ORGANIZATION.

2.1.1 Chief Information Security Officer

An Information Security office, headed by a Chief Information Security Officer (CISO), is created to establish, maintain, support, and enforce a System-wide risk-based information security program in support of this policy.

It is the goal of the office of the CISO to enable UMS through the usability and reliability of information by:

- Complying with all applicable rules, regulations, statutes, laws, and contractual obligations as they pertain to security and privacy throughout the information life cycle.
- Maintaining a security posture that provides the maximum possible operational advantage; and
- Providing reasonable and prudent levels of confidentiality, integrity and availability specific to the value of and risk to all types of information, and consistent with prevailing standards of practice.

2.1.2 Information Security Governance Council

An Information Security Governance Council shall be established to ensure that this information security policy is implemented effectively in supporting information security standards. The governance council shall be comprised of:

- The System Chief Information Security Officer, who shall chair the council
- The System University Counsel
- The System Vice Chancellor for Finance and Administration
- The System Chief Human Resources and Organizational Development Officer
- The System Chief Information Officer
- One executive representative from each university appointed by the president

The Information Security Governance Council shall:

- Meet quarterly, or more often if deemed necessary;
- Ensure that information security goals are identified, meet UMS requirements, and are integrated in relevant processes;
- Formulate, review, and approve information security policy change requests as needed for submission to the Board of Trustees for adoption;
- Formulate, review, and approve information security standards in support of this information security policy;
- Review the effectiveness of the implementation of the information security program, and take action to improve effectiveness where needed;
- Provide clear direction and visible management support for security initiatives;
- Review and advocate for resources needed for information security;
- Approve assignment of specific roles and responsibilities for information security across UMS;
- Initiate plans and programs to maintain information security awareness;
- Establish their own process and procedures for ensuring that information security needs are addressed without delay;
- Periodically report to the Board of Trustees as requested.

2.1.3 Allocation of information security responsibilities

Information security responsibilities shall be clearly defined for all employees, and all authorized users of UMS information assets.

Allocation of information security responsibilities shall be done in accordance with this information security policy. Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly identified.

Individuals with allocated security responsibilities may delegate security tasks to others. Nevertheless they remain responsible and shall determine that any delegated tasks have been correctly performed.

Management shall support the information security policy, assign security roles and coordinate and review the implementation of security across UMS.

A source of specialist information security advice shall be established and made available within UMS. Contacts with external security specialists or groups, including relevant authorities, shall

be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents.

2.1.3 When seeking specialist information security advice, expertise (faculty) within UMS should not be overlooked and used when available.

2.1.4 Authorization process for information processing facilities

A management authorization process for new information processing facilities shall be defined and implemented.

2.1.4 No computing device (shall be connected to the UMS network, other than to a guest network, without approval of campus IT or System ITS for non-campus access.
Single-user devices such as laptops may be self-registered by the owner upon first connection to the UMS network using their UMS ID and password.

Multi-user devices must be registered by their owner or administrator via the campus IT organization. The approval process shall include evaluating risks associated with the new device, identification of ownership or a designated contact person, and providing information to the device owner as to UMS requirements associated with the connection of the device to the UMS network.

Guest networks may be provided for the use of guests to a UMS campus or site.

2.1.5 Confidentiality agreements

Requirements for confidentiality or non-disclosure agreements reflecting UMS' needs for the protection of information shall be identified and regularly reviewed.

2.1.5 Non-disclosure agreements shall be developed as required for specific or unique circumstances. These confidentiality agreements shall be reviewed annually to ensure continued applicability. This standard applies to the content of the agreements, and not to the management of the executed documents.

2.1.6 Contact with authorities

Appropriate contacts with relevant authorities shall be maintained.

2.1.6 Each Campus and the System Office shall establish and maintain working relationships with authorities whose involvement may be required to support or respond to issues and incidents surrounding information security. Appropriate contact information will be maintained to be easily accessible within UMS in case of need. These should include local, county, state, and federal law enforcement agencies.

This requirement may be met as part of an organizational crisis management plan.

2.1.7 Contact with special interest groups

Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

2.1.7 Each Campus and the System Office supporting computer devices shall establish and maintain contacts sufficient to provide their security practitioners with regular and current information pertaining to good security practices, standards, vulnerabilities, and the current threat environment. These should include bug, vulnerability, and virus notification distribution lists; SIGs applicable to environments and programs prevalent within UMS, Contacts shall be made with professional associations such as Educause, Infragard, REN-ISAC, ISSA, ISACA, HTCIA, and DHS and internal resources such as faculty who may be able to provide guidance in such areas.

2.1.8 Independent review of information security

UMS' approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

2.1.8 The Office of the CISO shall contract with an independent firm not less than every two years to conduct a security assessment of the security posture of the Campuses and the System.
Where possible this assessment may and should be performed in concert with other security audits that may be periodically required by statute, contract, or policy.

2.2 EXTERNAL PARTIES

The security of UMS' information and information processing facilities shall not be reduced by the introduction of external party products or services.

Any access to UMS' information processing facilities and processing and communication of information by external parties shall be controlled.

Where there is a business need for working with external parties that may require access to UMS' information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment shall be carried out to determine security implications and control requirements. Controls shall be agreed and defined in an agreement with the external party.

2.2.1 Identification of risks related to external parties.

The risks to UMS' information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.

2.2.1 When there is a need to grant access to UMS' information or information processing facilities, the associated risk shall be evaluated by the UMS business process owner and the owner of the information assets involved. Campus IT or UMS ITS shall be consulted when an information processing facility is involved. The results shall be documented with the contract or agreement in question.

2.2.2 Addressing security when dealing with customers

All identified security requirements shall be addressed before giving customers access to UMS' information or assets.

2.2.2 Security requirements related to customers can vary considerably depending on the information assets accessed and can be addressed using customer agreements.

Customers are considered to be individuals using UMS services acting in a non-employee role.

2.2.3 Addressing security in third party agreements

Agreements with third parties involving accessing, processing, communicating or managing UMS' information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

2.2.3 Agreements with third parties involving accessing, processing, communicating or managing UMS' information or information processing facilities, or adding products or services to information processing facilities shall include a clause that specifies all relevant security requirements, or explicitly states that there are no relevant security requirements.

3 RISK ASSESSMENT AND TREATMENT

3.1 ASSESSING SECURITY RISKS

Risk assessments shall identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to UMS.

The results shall guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of UMS or individual information systems.

3.1 The risk shall be evaluated by the Information Owner in conjunction with the Campus or System IT office utilizing standardized risk analysis procedures. Examples of such procedures can be found in NIST SP800-30 or ISO 27005.

3.2 TREATING SECURITY RISKS

For each of the risks identified following the risk assessment a risk treatment decision shall be made. Possible options for risk treatment include:

- Applying appropriate controls to reduce the risks;
- Knowingly and objectively accepting risks, providing they clearly satisfy UMS' policy and criteria for risk acceptance;
- Avoiding risks by not allowing actions that would cause the risks to occur;
- Transferring the associated risks to other parties, e.g. insurers or suppliers.

3.2 Each Information Owner shall drive to conclusion by one of the above criteria and track all medium or high risks identified during risk and vulnerability management activities, and file the results for review as needed. If appropriate controls cannot reduce the risk level below medium, the acceptance of risk must be filed with the campus IT, who will consult with the CISO, within 30 days of assessment. The CISO, in consultation with the campus IT and the Information Owner, will make a determination if the risk can be accepted, and whether the computing device containing the information may remain on the network. The results of the risk assessment shall remain on file for as long as the condition or process evaluated remains in effect.

4 ASSET MANAGEMENT

4.1 RESPONSIBILITY FOR ASSETS

All assets shall be accounted for and have a nominated owner.

Owners shall be identified for all assets and the responsibility for the maintenance of appropriate controls shall be assigned. The implementation of specific controls may be delegated by the owner as appropriate, but the owner remains responsible for the proper protection of the assets.

4.1.1 Inventory of assets

All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.

4.1.1 Sufficient information shall be maintained on assets to allow and enhance recovery efforts should a disaster or other incident occur. Towards that end, each Campus and the System Office shall identify what information, if any, should be maintained on assets depending on their importance for recovery, and shall maintain an inventory of assets, including hardware, software, and communications equipment, and key services upon which the provision of IT services is dependent.

It is not required to duplicate existing inventories, as long as the required information is maintained, readily available for purposes of vulnerability management and incident response, and provided to UMS ITS in a useable format upon request.

This inventory shall include as applicable:

- Type of asset,
- Model or Package name/number,
- Release or version number,
- Physical location,
- Asset value estimate or purchase cost,
- The highest classification of information contained in the asset,
- A criticality rating,
- A designated asset owner, or primary point of contact.

4.1.2 Ownership of assets

All information and assets associated with information processing facilities shall be owned by a designated part of UMS.

4.1.2 All information processing facilities owned by UMS shall have a designated owner or primary point of contact recorded in the asset management database established under section 4.1.1.

4.1.3 Acceptable use of assets

Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

4.1.3 Acceptable Use of Information Resources

Preamble

The University of Maine System (all of its Campuses and subordinate components) endeavors to develop and provide access to collections, services, facilities, equipment, and programs which meet the information and educational needs of the University community, and to advance the research, instruction, and service missions of UMS.

In fulfillment of this purpose, and in response to advances in technology and the changing needs of the community, UMS supports access to information resources, including the Internet, to the greatest extent possible. In return, the University expects users of information resources to be aware of and act in compliance with all relevant federal and state laws, local ordinances, and University policies. It further expects its users to be familiar and to behave consistently with the several general principles which together constitute appropriate, responsible, and ethical behavior in an academic environment, particularly in regard to the use of the University's information resources. Those principles include: Freedom of Expression, Respect for Privacy, Respect for Property Rights, Respect for Personal and Cultural Differences, Freedom from Harassment, Respect for and Compliance with Intellectual Property Rights and Copyright Law.

The University of Maine System affirms that it will be a partner with users in promoting education and understanding of the appropriate, efficient, and successful use of information resources.

Responsibilities

All users of University of Maine System information resources are expected to behave responsibly, legally, and ethically in their use of all information resources. To that end, it is the responsibility of those users to:

- honor all state and federal laws, copyright provisions, Board of Trustees policies, and software licensing agreements to which the institution is a party;
- be aware of and comply with University and the University's agencies' procedures and regulations for accessing and operating computer and related hardware, software, and other information resources;
- cooperate with legitimate requests by University staff;
- take precautions to protect accounts and passwords by selecting obscure passwords, changing them frequently, and not sharing such information or the use of the accounts with others; properly logoff or logout whenever leaving a computer in an area which is accessible to others;
- treat others with dignity and respect; respect the privacy and confidentiality rights of others, including their files and accounts;
- use UMS information resources only for purposes which are legal and consistent with the University's mission.

Consistent with the above, unacceptable uses and behaviors include, but are not limited to:

- damaging or attempting to alter computer equipment;
- violating, or attempting to violate, computer system security;
- violating, or attempting to violate, software license agreements;
- incurring unauthorized or unreasonable costs for the University;
- accessing files, data, or passwords of others without authorization;
- disrupting or monitoring electronic communications without authorization;
- harassing other computer users or University staff;
- violating the privacy of others;
- libeling or slandering others;
- using any University workstation for any illegal purpose;
- copying or distributing copyright-protected material without legal right or authorization;
- intentionally and unnecessarily exposing others to material for which they have no legitimate purpose.

Information Technology Assets provided to (Faculty and Staff) are for University Business and limited personal use consistent with Board Policies on Intellectual Property and Conflict of Interest.

Results of Inappropriate Behavior

It is important to recognize that inappropriate behavior has an adverse effect on the work of others, on the ability of University staff to provide good service, and/or on information resources themselves. Thus it is expected that users of information resources at UMS will be constructively responsive to others' complaints, and receptive to University staff's reasonable requests for changes in behavior or action.

University staff will attempt to resolve differences and problems among information users by asking for the cooperation of those involved, and for compliance with University policies.
The University will pursue infractions or misconduct that cannot be resolved informally with the general means it has available to it within the University and with law enforcement, as appropriate.

Serious infractions or misconduct may result in temporary or permanent loss of access privileges.

Guiding Principles

The University of Maine System supports the democratic principle of freedom of access to information for every citizen.

UMS does not attempt to limit access to, or otherwise protect users of information resources from any particular materials available in any format, beyond the choices it makes in selecting materials or providing

electronic links to information sources of particular merit. UMS does limit access to Compliant and Business Sensitive Data based on a need to know.

UMS does not monitor, and has no control over, information accessible through the Internet. The University disclaims any warranty for any information found on the Internet as to its accuracy, authority, timeliness, usefulness, or fitness for a particular purpose. Likewise, the University disclaims any control over, or knowledge about, changes in content to the sources for which it has established links, or for the content of sources accessed through secondary links.

The Internet contains much information that is personally, academically, professionally, and culturally enriching. It also provides material that may be factually incorrect, offensive, disturbing to some individuals, and/or illegal. Moreover, the Internet may not be an adequate substitute for many other kinds of information resources which may be limited by copyright or other restrictions to local use.

While the University is committed to serving the general public to the greatest extent possible, it reserves the right to give priority in service to the UMS community (students, faculty, and staff), especially in the case of a high level of demand for limited equipment and materials. This may include limiting the amount of time users may have to use certain information resources and supporting equipment. Moreover, access to some information resources must be limited based on licensing or other contractual agreements with vendors.

Individual Campuses or units may enact additional Acceptable Use Standards that include this Policy at a minimum.

The Campus Information Technology Director will notify the University of Maine System Information Security Office of any significant violation of acceptable use including any violation that may have implications beyond a single campus or may involve loss of private, financial, or medical information.

4.2 INFORMATION CLASSIFICATION

Information shall be classified to indicate the need, priorities, and expected degree of protection when handling the information.

Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme shall be used to define an appropriate set of protection levels and communicate the need for special handling measures.

4.2.1 Classification guidelines

Information shall be classified in terms of its value, legal requirements, sensitivity, and criticality to UMS.

4.2.1 UMS Information shall be classified by the information owner into one of the following three categories:

1. Compliant Data - Information which has specified requirements for the control of confidentiality, availability, or integrity of the data due to statute or contract or other law or agreement. Compliant data is information which requires special protection because the misuse could harm members of the UMS community or compromise the mission of the System and/or any one of the Universities. Compliant data includes, but is not limited to, personally-identifiable information, confidential research information, and information that requires protection under law or agreement such as the Maine Data Act, FERPA (the Family Educational Rights and Privacy Act), GLBA (the Gramm-Leach Bliley Act), HIPAA (the Health Insurance Portability and Accountability Act), FTC “Red Flag Rule”, -by the PCI

(Payment Card Industry) data security standards, and data placed on legal hold in accordance with e-discovery. Examples of Compliant Data include: financial records, health records, student educational records, and any information which could permit a person to attempt to harm or assume the identity of an individual.

2. Business Sensitive – Information that is not the subject of statutory or contractual controls, but where the compromise of the confidentiality, integrity, or availability of the information would result in damage or loss to UMS.
3. Unclassified – Information that does not fall into either of the above categories.

4.2.2 Information labeling and handling

An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by UMS.

4.2.2 Appropriate labeling and handling for information is as follows:

1. Compliant Data -
   - Encrypted or secured at rest, in transit, and anytime it is not in use.
   - Access is controlled according to a documented "need to know" the information.
   - When discussed, the host must verify that all present are entitled to access to the information.
   - When sending Compliant Data to a recipient outside UMS, the sender must be sure that the recipient understands that the data is Compliant Data, and is authorized to receive such data. The information must be protected according to any additional requirements of statute or contract pertaining to the information.
2. Business Sensitive –
   - Must be protected in a system that requires a password to access.
   - Access is controlled according to documented need to know the information.
   - When discussed the host must verify that all present are entitled to access to the information.
   - When transmitting Business Sensitive Data to a recipient outside UMS, the sender must be sure that the recipient understands that the data is Business Sensitive Data, and is authorized to receive such data. The information must be protected according to any additional requirements of statute or contract pertaining to the information.
3. Unclassified –
   - May be made public with management or the information owner's approval.

5 HUMAN RESOURCES SECURITY

5.1 PRIOR TO EMPLOYMENT

Security responsibilities shall be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.

All candidates for employment, contractors and third party users shall be adequately screened, commensurate with the sensitivity of their jobs.

Employees, contractors and third party users of information processing facilities shall sign an agreement on their security roles and responsibilities prior to beginning work.

5.1.1 Roles and responsibilities

Security roles and responsibilities of employees, contractors, and third party users shall be defined and documented in accordance with this information security policy and job requirements.

5.1.1 All position descriptions for full and part time UMS positions shall include a description of the information security roles and responsibilities associated with it.

All contracts and master services agreements shall include a description of the information security roles and responsibilities of the contractor/consultant/temporary as it pertains to UMS information assets included.

5.1.2 Screening

Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

5.1.2 Candidates for specifically designated positions shall successfully pass a background investigation as required for those positions before their hire or position change is considered permanent. In such circumstances, credit or criminal checks may be required depending on the position. Additional checks may be required for positions due to other statutes, regulations, or contracts.

5.1.3 Terms and conditions of employment

As part of their contractual obligation, employees, contractors and third party users shall agree and sign a statement of their and UMS' responsibilities for information security.

5.2 DURING EMPLOYMENT

Management responsibilities shall be defined to ensure that appropriate security practices are observed throughout an individual's employment within UMS.

An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities shall be provided to all employees, contractors, and third party users prior to being given access to minimize possible security risks.

5.2.1 Management responsibilities

Management shall require employees, contractors, and third party users to apply security practices in accordance with established policies and procedures of UMS.

5.2.2 Information security awareness, education, and training

All employees of UMS and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in UMS policies and procedures, as relevant for their job function.

5.2.2 Position-appropriate training will be provided upon hire/contract, and at least annually thereafter, and successful completion of the training program and evaluation is required. This will include general security training for all employees, plus additional training specific to the responsibilities of managers, developers, those with access to Business Sensitive information, and those with access to Compliant Data focusing on the specific statutory or contractual obligations of those with access to the specific information.

Completion of this required training shall be tracked, and supervisors notified of those who have failed to complete the required training.

Awareness programs will deliver reminders and updates at least monthly to all those with access to UMS information.

5.2.3 Disciplinary process

There shall be a formal disciplinary process for employees who have committed a security breach.

5.2.3 Disciplinary action for violations of the Information Security Policy and these supporting standards shall follow normal UMS disciplinary processes, and may result in actions up to and including dismissal.

5.3 TERMINATION OR CHANGE OF EMPLOYMENT

Responsibilities shall be in place to ensure an employee's, contractor's or third party user's exit from UMS is managed, and that the return of all equipment and the removal of all access rights are completed in a timely manner.

Change of responsibilities and employments within UMS shall be managed as the termination of the respective responsibility or employment in line with this section, and any new employments shall be managed as described in section 5.1.

5.3.1 Termination responsibilities

Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.

5.3.1 Notification of UMS and campus IT organizations shall be an explicit step in termination checklists that prescribe termination actions.

UMS and campus IT shall be provided notice of voluntary terminations not less than one week prior to the agreed date of termination.

UMS and campus IT shall be notified of involuntary terminations prior to the employee's notification.

5.3.2 Return of assets

All employees, contractors and third party users shall return all of UMS' assets in their possession upon termination of their employment, contract or agreement.

5.3.3 Removal of access rights

The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed immediately upon termination of their employment, contract or agreement, or adjusted upon change.

5.3.3 Prior to the time and date of employment termination, all UMS userids, and network and application accounts shall be reviewed to determine which userids or accounts shall be terminated.

Should the individual require access to some systems after employment termination, that access must be granted specifically for that purpose in accordance with Section 2.2 and Section 8 as appropriate.

6 PHYSICAL AND ENVIRONMENTAL SECURITY

6.1 SECURE AREAS

Critical or sensitive information processing facilities shall be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They shall be physically protected from unauthorized access, damage, and interference.

The protection provided shall be commensurate with the identified risks.

6.1 This section addresses the risks to information associated with unauthorized physical access to devices that contain Compliant or Business Sensitive information, and the elevated risks of compromise when physical access can be gained to any device by an attacker.

6.1.1 Physical security perimeter

Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.

6.1.1 Physical information processing facilities that contain Compliant Data or Business Sensitive Data shall be secured when not attended by authorized personnel.

6.1.2 Physical entry controls

Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

6.1.2 Physical entry controls shall be applied to any area housing one or more multi-user devices.

Visitor access logs will be maintained at the entrance to any area housing one or more multi-user devices. The entrance and departure of anyone not individually authorized access to that area shall be logged for each visit, and signed for by someone with authorized access. Visitor access logs will be made available for audit upon request of campus IT or UMS ITS, or the CISO.

6.1.3 Securing offices, rooms, and facilities

Physical security for offices, rooms, and facilities shall be designed and applied.

6.1.3 Risk-appropriate physical entry controls shall be implemented for any area housing computing devices that contain Compliant or Business Sensitive Data.

6.1.4 Protecting against external and environmental threats

Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.

6.1.4 A physical risk assessment of all reasonably anticipated threats shall be completed by the owner of any area housing one or more multi-user devices, which contain Compliant or Business Sensitive Data. The physical risk assessment shall be filed and available for inspection upon request of campus or UMS IT or the CISO. No information processing facility, to include individually-sited servers, which contain Compliant or Business Sensitive Data, may be sited in areas that do not have a physical risk assessment in place, and the required remediations completed.

6.1.5 Working in secure areas

Physical protection and guidelines for working in secure areas shall be designed and applied.

6.1.5 No individual shall perform work in a secure area alone without a record.

The use of video, photographic, audio, or other recording equipment in secure areas is prohibited unless specifically authorized by the information processing facility owner for a particular instance or purpose.

6.1.6 Public access, delivery, and loading areas

Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

6.2 EQUIPMENT SECURITY

Equipment shall be protected from physical and environmental threats.

Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This shall also consider equipment siting and disposal. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

6.2.1 Equipment siting and protection

Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

6.2.1 Measures shall be implemented to minimize the risk of theft, environmental hazards or unnecessary access into work areas. When mobile devices are left unattended in unlocked offices or spaces appropriate precautions shall be taken based on the security of the location, the length of time unattended, and data contained on the device. Such measures may include removal from sight, securing in a desk or cabinet, or securing with a cable lock. Computing devices shall be positioned to reduce the risk of Compliant or Business Sensitive Data being viewed by unauthorized individuals.

6.2.2 Supporting utilities

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

6.2.2 All mission critical information processing facilities shall be supported by UPS devices sufficient to meet business continuity requirements.

The necessity of providing redundant power and communications shall be considered to support mission critical functionality. Any information processing facility that supports systems critical to life safety shall have redundant power and communications.

6.2.3 Cabling security

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

6.2.4 Equipment maintenance

Equipment shall be correctly maintained to ensure its continued availability and integrity.

6.2.4 Hardware maintenance agreements with defined service level agreements and/or accessible spare parts shall be maintained for all devices as needed to meet the business continuity needs of UMS.

6.2.5 Security of equipment off-premises

Security shall be applied to off-site equipment taking into account the different risks of working outside UMS' premises.

6.2.5 Fixed UMS information processing facilities located off of UMS property shall be subject to the same physical security requirements as those located on UMS property.

Portable devices should be kept in the personal possession of the owner when possible, and secured or kept out of plain sight when not in the personal possession of the owner.

6.2.6 Secure disposal or re-use of equipment

All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

6.2.6 Storage media shall have all UMS data wiped or securely deleted. Measures taken shall at least be commensurate with the standard for "clearing" as specified in the National Institute of Standards and Technology (NIST) Special Publication SP800-88: Guidelines for Media Sanitization, prior to disposal or reuse.

Software licensed for the device, such as the original operating systems, may be reloaded following sanitization procedures if desired prior to re-use or disposal as appropriate.

6.2.7 Removal of property

Equipment, information or software shall not be taken off-site without prior authorization.

6.2.7 Equipment, information, and software issued for the individual use of an employee may be taken off-site as needed with single verbal management permission. Other UMS-owned equipment may be taken off-site only with specific approval and tracking at the organizational ownership level. For asset management purposes, dates of removal, person authorized, purpose, and date of expected return should be maintained.

7 COMMUNICATIONS AND OPERATIONS MANAGEMENT

7.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES

Responsibilities and procedures for the management and operation of all information processing facilities shall be established. This includes the development of appropriate operating procedures.

Segregation of duties shall be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

7.1.1 Documented operating procedures

Operating procedures shall be documented, maintained, and made available to all users who need them.

7.1.1 Operating procedures shall be developed and maintained by each entity operating one or more multi-user servers that specify the instructions for the detailed execution of each task involved, including but not limited to:

- Processing and handling of information;
- Backup;
- Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

- Process for reporting errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;
- Support contacts in the event of unexpected operational or technical difficulties;
- Special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs;
- System restart and recovery procedures for use in the event of system failure;
- The management of audit-trail and system log information.

7.1.2Change management

Changes to information processing facilities and systems shall be controlled.

7.1.2 Procedures shall be implemented by each entity operating multi-user servers to reduce the risk that a change will cause a system or security failure. Change management procedures should include who is authorized to make what kind of changes, what kind of changes necessitate involvement from stakeholders, testing, back out procedures, and a record of configuration.

7.1.3Segregation of duties

Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of UMS' assets.

7.1.3 Where staff size or composition does not allow a satisfactory separation of duties, documented mitigation procedures shall be developed and followed to limit the exposure of UMS information to misuse. In general, those who execute a task should not be the same as the one who authorizes or audits the task; those who modify systems should not be the same who promote them to production.

7.1.4Separation of development, test, and operational facilities

Development, test, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational system.

7.1.4 Environments that contain Compliant or Business Sensitive Data shall be adequately protected. To protect data, the following measures should be strongly considered:
Testing of new systems or applications, or proposed changes to existing software, should be carried out in other-than-production environments.

Development and test environments may be the same, but must be separate from the production environment.

Maintaining a separate dev/test environment supports the requirements of section 11: business continuity management, as well as the integrity of production data.

7.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT

UMS shall check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.

7.2 It is the responsibility of the UMS contract administrator to any contract for services delivery to ensure that all security related issues meet the requirements of the UMS Information Security Standards. Otherwise the contract cannot be signed without the specific acceptance of the Campus IT and/or the CISO.

7.2.1 Service delivery

It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

7.2.1 It is the responsibility of the UMS party to any third party contract to ensure that all security issues that may pertain to the services provided are included in the terms, conditions, and service level agreements of the contract. The office of the CISO may be consulted for assistance and guidance.

7.2.2 Monitoring and review of third party services

The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.

7.2.2 Review of the security aspects of services provided to UMS by third parties as required by agreement shall be completed annually to ensure that terms and conditions are being met and security events, incidents, and problems are properly managed.

7.2.3 Managing changes to third party services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

7.2.3 It is the responsibility of the UMS contract administrator with input from University Counsel, CISO and/or campus IT to ensure that all security implications of changes or modification to the contract are addressed and managed.

7.3 SYSTEM PLANNING AND ACCEPTANCE

Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance.

Projections of future capacity requirements shall be made, to reduce the risk of system overload. The operational requirements of new systems shall be established, documented, and tested prior to their acceptance and use.

7.3.1 Capacity management

The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

7.3.1 All entities providing mission critical multi-user services shall maintain a 12-month forward looking projection of capacity vs. utilization to anticipate the need for additional capacity in time for effective budgeting and to avoid adverse impact on services delivered.

7.3.2 System acceptance

Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.

7.3.2 No new system or application that processes, stores, or transmits Compliant or Business Sensitive Data shall be promoted to production until information security aspects have been evaluated.

7.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE

Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code.

Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users shall be made aware of the dangers of malicious code. Managers shall, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code.

7.4.1 Controls against malicious code

Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

7.4.1 All servers and single-user devices must have IT-managed anti-malware software, or equivalent protection, installed and running by default.

All single user devices that store, process, or transmit Compliant or Business Sensitive Data devices must have personal firewalls installed, configured, and running by default.

7.4.2Controls against mobile code

Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security standard, and unauthorized mobile code shall be prevented from executing.

7.5 BACK-UP

Routine procedures shall be established to implement the agreed back-up standard and strategy for taking back-up copies of data and rehearsing their timely restoration.

7.5.1 Information back-up

Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup standard.

7.5.1 Multi-user servers that contain Mission Critical data shall be backed up to media stored at a separate location no less than a separate building:

- Incrementally not less than daily, and retained for 15 days.
- Fully not less than weekly, and retained for 45 days.

Test of restore procedures shall be done for all multi-user servers not less than once per year to ensure they meet business continuity requirements.

Single user device that contain original or master copies of Compliant or Business Sensitive data shall be backed up to an encrypted external device or system not less than monthly. If the back-up storage device remains in the possession of the end user, that device must be stored securely in a locked drawer or cabinet.

7.6 NETWORK SECURITY MANAGEMENT

The secure management of networks, which may span organizational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection.

Additional controls may also be required to protect sensitive information passing over public networks.

7.6.1 Network controls

Networks shall be adequately managed and controlled, in order to be protected from threats, and

to maintain security for the systems and applications using the network, including information in transit.

7.6.1 All traffic entering and exiting the UMS network shall be inspected by intrusion detection/prevention systems (IDS/IPS) for known or suspect malicious activity. Traffic entering and exiting a network segment with mission critical multi-user devices that contain Compliant Data contains shall be controlled by a firewall configured to allow only required traffic.

All network devices shall have default passwords changed at a minimum to comply with the password standards where technically possible.
Access to networking devices shall be tightly controlled on a need-to-know basis, audited not less than annually, and monitored for changes.

7.6.2 Security of network services

Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

7.7 MEDIA HANDLING

Media shall be controlled and physically protected.

Appropriate operating procedures shall be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

7.7.1 Management of removable media

There shall be procedures in place for the management of removable media.

7.7.1 Removable media shall be managed according to the requirements for the level of data contained per section 4.

7.7.2 Disposal of media

Media shall be disposed of securely and safely when no longer required, using formal procedures.

7.7.2 When no longer needed, removable media shall have all data made unavailable. Measures taken shall at least be commensurate with the standard for “clearing” as specified in NIST SP800-88.

7.7.3 Information handling procedures

Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.

7.7.3 Consistent with the requirements of section 4 on data classifications and section 7.1 on operation controls, all entities within UMS that manage, administer, or maintain a multi-user server or servers must document regular operational controls for all anticipated instances of handling various information types to protect the information from unauthorized disclosure or misuse.

7.7.4 Security of system documentation

System documentation shall be protected against unauthorized access.

7.7.4 System documentation specific to the implementation within UMS is considered Business Sensitive information, and must be handled accordingly per section 4.

7.8 EXCHANGE OF INFORMATION

Exchanges of information and software between organizations shall be based on a formal exchange standard, carried out in line with exchange agreements, and shall be compliant with any relevant legislation.

Procedures and standards shall be established to protect information and physical media containing information in transit.

7.8.1 Information exchange policies and procedures

Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.

7.8.2 Exchange agreements

Agreements shall be established for the exchange of information and software between UMS and external parties.

7.8.2 It is the responsibility of anyone who exchanges Compliant or Business Sensitive Data with any entity outside of UMS to obtain permission from the information owner to do so, and to establish agreements with the outside entity to provide for data protections that are compliant with the UMS policy governing that data.

7.8.3 Physical media in transit

Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond UMS' physical boundaries.

7.8.3 It is the responsibility of anyone who transfers physical media that contains Compliant or Business Sensitive Data outside of UMS' physical boundaries to provide for data protections during the entire time the media exists outside of UMS's physical boundaries that are compliant with the UMS policy governing that data.

7.8.4 Electronic messaging

Information involved in electronic messaging shall be appropriately protected.

7.8.4 Compliant and Business Sensitive Data are subject to the requirements of section 4 during their entire information life cycle, including transmission via electronic messaging systems such as email, instant messaging, text messaging, and other user-to-user technologies.

When sending Compliant or Business Sensitive Data to a recipient outside UMS that is authorized to receive the information, ensure that the recipient is aware of the data classification of the information sent, and the proper controls following receipt. In some instances this may be required every time, In other instances the established relationship may determine the expectation of the classification and handling of the information. It is the responsibility of the sender to be sure of the circumstance.

7.8.5 Business information systems

Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.

It is the responsibility of the UMS entity establishing a connection with other business information systems to ensure that agreements, contracts, or service level agreements are in place with the owner of the other systems that ensures that information protections required in the UMS information security policy and this standard will be met during any interconnected activities. The UMS entity shall consult

with either campus IT, System ITS, or the CISO,

7.9 ELECTRONIC COMMERCE SERVICES

The security implications associated with using electronic commerce services, including on-line transactions, and the requirements for controls, shall be considered. The integrity and availability of information electronically published through publicly available systems shall also be considered.

7.9.1 Electronic commerce

Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

7.9.1 All e-commerce transactions with UMS shall utilize strong encryption, and certificate-based authentication of the UMS server hosting the transaction ensuring the confidentiality and non-repudiation of the transaction while crossing networks. Where possible, certificate-based client side authentication shall be utilized.

7.9.2On-Line Transactions

Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

7.9.2 All on-line transactions with UMS shall utilize strong encryption, and certificate-based authentication of the UMS server hosting the transaction ensuring the confidentiality and non-repudiation of the transaction while crossing networks. Where possible, certificate-based client side authentication shall be utilized.

7.9.3Publicly available information

The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.

7.9.3 Unclassified Information made available via a server represented as part of UMS must provide protections to that information that either authenticates those authorized to change the information, or automatically identifies and notifies the information owner that it has been changed.

7.10 MONITORING.

Systems shall be monitored and information security events shall be recorded. Operator logs and fault logging shall be used to ensure information system problems are identified.
UMS shall comply with all relevant legal requirements applicable to its monitoring and logging activities.

System monitoring shall be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

7.10.1 Audit logging

Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

7.10.1 Security logging, which tracks events such a log-on, log-off, successful and rejected attempts, and changes to configuration, will be enabled on all multi-user devices, and the logs retained for not less than 90 days, or as required by statute or contract.

7.10.2Monitoring system use

Procedures for monitoring use of information processing facilities shall be established and the

results of the monitoring activities reviewed regularly.

7.10.2 The level of monitoring shall be established on all systems containing Compliant or Business Sensitive Data based on a risk assessment, or as required by statute or contract.

7.10.3 Protection of log information

Logging facilities and log information shall be protected against tampering and unauthorized access.

7.10.3 Device logs shall be protected from changes. When possible, device logs shall be stored on a separate log host server that shall be accessible only from servers placing log records there, and from limited monitoring consoles.

7.10.4 Administrator and operator logs

System administrator and system operator activities shall be logged.

7.10.4 Administrator and operator logs shall be stored on a separate log host server that shall be accessible only from servers placing log records there, and limited monitoring consoles. This could be the same log file as identified in 7.10.3.

7.10.5 Fault logging

Faults shall be logged, analyzed, and appropriate action taken.

7.10.5 Faults shall be addressed by a formal problem management process that includes a risk-based response to identified faults.

All faults on mission critical systems with a medium or high effect shall be processed to conclusion, and a record of the action must be retained.

7.10.6 Clock synchronization

The clocks of all relevant information processing systems within UMS shall be synchronized with an agreed accurate time source.

7.10.6 All server and networking device clocks will be synchronized to a standard time distribution from the U.S. Naval Observatory if the device supports this. Devices will be re-synched as needed.

8 ACCESS CONTROL

8.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL

Access to information, information processing facilities, and business processes shall be controlled on the basis of business and security requirements.

Access control rules shall take account of policies for information dissemination and authorization.

8.1.1 Access control policy

An access control standard shall be established, documented, and reviewed based on business and security requirements for access.

8.1.1 Access to Compliant and Business Sensitive Data shall be on a business need-to-know basis only. Both the information owner and the supervisor of the individual to be given access must approve the

access upon granting. A department chair, dean or director may approve for individuals where a supervisor isn't appropriate. Access shall be reviewed periodically and when an individual changes position.

The administrator of systems containing Compliant and Business Sensitive Data shall be responsible for obtaining the proper approvals before granting access via the system, for the annual re-verification of access need process, and for maintaining records available for audit of approvals applicable to their system.

Access shall be automatically locked upon presentation of an incorrect user password more than 5 times in a row where technically feasible. For systems where a lock is not technically feasible, Campus IT will identify those systems to the CISO. The account may be automatically unlocked after no less than one hour. Access may only be re-enabled by resetting the password with proper authentication from the registered user.

8.2 USER ACCESS MANAGEMENT

Formal procedures shall be in place to control the allocation of access rights to information systems and services.

The procedures shall cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention shall be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

8.2.1 User registration

There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

8.2.1 Any entity within UMS that grants or denies access to a multi-user device, must maintain a procedure for controlling access that includes who is authorized to grant access, a record of all users with the conditions and duration of the access granted, and a periodic review of user rights.

8.2.2 Privilege management

The allocation and use of privileges shall be restricted and controlled.

8.2.2 A principle of least privilege shall be maintained, where users are granted the minimum level of access required by their role. Additional privileges will be granted only per 8.1.1 above.

If no appropriate role is defined for a user, no access will be granted without gaining approval from information owners and supervisors for each access privilege granted.

8.2.3 User password management

The allocation of passwords shall be controlled through a formal management process.

8.2.3 Passwords assigned to new accounts, and reset passwords, must meet the requirements for strong passwords per 8.3.1, and must be changed upon the first login.

Authentication must be required on anyone requesting a new or reset password before the password is changed.

Stored user passwords must not be visible to or recoverable by help desk or other personnel with the authority to change them. Where possible, stored passwords must not be visible by anyone. This requirement shall not be construed to prohibit key escrow or password recovery procedures for encrypted

hard drives on UMS-owned systems.

All passwords changes, resets, or reassignments shall log the time and date of the event, and the person resetting the password. Help desk tickets may provide a sufficient log.

8.2.4Review of user access rights

Management shall review users' access rights at regular intervals using a formal process.

The system owner or administrator of each multi-user server shall submit a request to each registered user's supervisor at least annually to verify the continued approval for the user's access. A single request may be sent to each supervisor requesting verification of continued access approval for a list of users.

Any user whose continued access is not verified by their supervisor or designee within 30 days shall have their access rights suspended, and shall be notified of same.

8.3 USER RESPONSIBILITIES

The cooperation of authorized users is essential for effective security.

Users shall be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

A clear desk and clear screen policy shall be implemented to reduce the risk of unauthorized access or damage to papers, media, and information processing facilities.

8.3.1 Password use

Users shall be required to follow good security practices in the selection and use of passwords.

8.3.1.1 Users shall not provide their passwords to anyone under any circumstances. Instance where their passwords are requested should be reported to the help desk.

Users shall not use UMS passwords for accounts outside of UMS.

8.3.1.2 Strong Passwords

Strong passwords are the responsibility of each individual who uses services provided by any entity of the University of Maine System.

Passwords shall:

- Be changed immediately from any default password provided with the device or program;
- Be changed immediately after being reset;
- Be at least eight characters long;
- Contain at least one upper and one lower case alphabetic characters (e.g., a-z, A-Z);
- Contain at least one numeric or special character (e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
- Not be a standalone word or common abbreviation in any language, slang, dialect or jargon, etc;
- Not be based on personal information, names of family, etc;
- Be changed annually using a password not previously chosen, unless more frequent changes are required due to contract or statute in your specific environment;
- Not be reused for at least 2 years.

8.3.2 Unattended user equipment

Users shall ensure that unattended equipment has appropriate protection.

8.3.2 Unattended equipment must be protected against loss of information.

PCs and consoles must have password protected screen-savers that automatically lock the screen within 30 minutes of no user activity.

8.3.3Clear desk and clear screen policy

A clear desk standard for papers and removable storage media and a clear screen standard for information processing facilities shall be adopted.

8.3.3 When not in use Compliant or Business Sensitive Data must be secured in a locked container (desk drawer, file cabinet, credenza, etc.) or in a locked room where access is restricted to individuals who have the authority to access that data.

Computer screens should be cleared of Compliant or Business Sensitive Data when the screen is unattended. Simply powering off the display or otherwise blocking it is not sufficient.

8.4 NETWORK ACCESS CONTROL

Access to both internal and external networked services shall be controlled.

User access to networks and network services shall not compromise the security of the network services by ensuring:

a) Appropriate interfaces are in place between UMS' network and networks owned by other organizations, and public networks;
b) Appropriate authentication mechanisms are applied for users and equipment;
c) Control of user access to information services is enforced.

8.4.1 Policy on use of network services

Users shall only be provided with access to the services that they have been specifically authorized to use.

8.4.2 User authentication for external connections

Appropriate authentication methods shall be used to control access by remote users.

8.4.3 Equipment identification in networks

Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.

8.4.4 Remote diagnostic and configuration port protection

Physical and logical access to diagnostic and configuration ports shall be controlled.

8.4.4 Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, should be disabled or removed. Logical access shall be disabled when not in use where possible.

8.4.5Segregation in networks

Groups of information services, users, and information systems shall be segregated on networks.

8.4.5 Multi-user servers that contain Compliant or Business Sensitive Data shall not be logically placed on the same LAN segments as single-user devices, with the exception of single-user devices that are used solely for systems administration purposes.

8.4.6 Network connection control

For shared networks, especially those extending across UMS' boundaries, the capability of users to connect to the network shall be restricted, in line with the access control standard and requirements of the business applications (see 8.1).

8.4.6 All computing devices shall be required to be registered on the UMS network prior to being granted access.

8.4.7 Network routing control

Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control standard of the business applications.

8.5 OPERATING SYSTEM ACCESS CONTROL

Security facilities shall be used to restrict access to operating systems to authorized users. The facilities shall be capable of the following:

a) Authenticating authorized users, in accordance with a defined access control policy;
b) Recording successful and failed system authentication attempts;
c) Recording the use of special system privileges;
d) Issuing alarms when system security policies are breached;
e) Providing appropriate means for authentication;
f) Where appropriate, restricting the connection time of users.

8.5.1 Secure log-on procedures

Access to operating systems shall be controlled by a secure log-on procedure.

8.5.1 The procedure for logging onto a multi-user device operating system shall be designed to minimize the opportunity for unauthorized access. The log-on procedure shall therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance. A log-on procedure shall:

- validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;
- not display the password being entered or consider hiding the password characters by symbols;
- not transmit passwords in clear text over a network.

When possible, the log-on procedure should adhere to the following standard.

- Display a general notice warning that the computer should only be accessed by authorized users.
- Limit the number of unsuccessful log-on attempts allowed, e.g. to five attempts, and consider:
  - Recording unsuccessful and successful attempts;
  - Forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization;
  - Disconnecting data link connections;
  - Sending an alarm message to the system console if the maximum number of log-on attempts is reached;
  - Setting the number of password retries in conjunction with the minimum length of the password and the value of the system being protected;
- Limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on.
- Display the following information on completion of a successful log-on:
  - Date and time of the previous successful log-on;

- Details of any unsuccessful log-on attempts since the last successful log-on.

8.5.2 User identification and authentication

All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

8.5.2 Each userid shall be assigned only to an individual user, and shall not be shared with other users. A single user may have more than one userid assigned to them.

8.5.3 Password management system

Systems for managing passwords shall be interactive and shall ensure quality passwords.

8.5.3 Technical means for enforcing the password policy shall be implemented where possible.

8.5.4 Use of system utilities

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

8.5.5 Session time-out.

Inactive sessions shall shut down after a defined period of inactivity.

8.5.5 For an application that provides access to Compliant Data, inactive session shall be shut down after no more than 90minutes.

8.5.6 Limitation of connection time

Restrictions on connection times shall be used to provide additional security for high-risk applications.

8.5.6 Connection time of any single session to an application that provides access to Compliant Data shall be limited to no more than 12 hours. Users who need access for periods of more than 12 hours will make special arrangements with campus IT or System ITS.

8.6 APPLICATION AND INFORMATION ACCESS CONTROL

Security facilities shall be used to restrict access to and within application systems.

Logical access to application software and information shall be restricted to authorized users. Application systems shall:

a) Control user access to information and application system functions, in accordance with a defined access control policy;
b) Provide protection from unauthorized access by any utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls;
c) Not compromise other systems with which information resources are shared.

8.6.1 Information access restriction

Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control standard.

8.6.2 Sensitive system isolation

Sensitive systems shall have a dedicated (isolated) computing environment.

8.6.2 Multi-user systems containing Compliant Data shall be on isolated LAN segments which are appropriately controlled commensurate with the risk assessment.

8.7 MOBILE COMPUTING AND TELEWORKING

The protection required shall be commensurate with the risks these specific ways of working

cause. When using mobile computing the risks of working in an unprotected environment shall be considered and appropriate protection applied. In the case of teleworking UMS shall apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

8.7.1 Mobile computing and communications

A formal standard shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

8.7.1 Mobile computing devices shall be required to provide the required protections to each classification of information that it may contain to be authorized for use.

All new UMS-issued laptop, notebook, netbook, and tablet devices that will or may store or process Compliant or Business Sensitive Data shall be deployed with authentication and encryption capabilities installed and activated.

8.7.2 Teleworking

A standard, operational plans and procedures shall be developed and implemented for teleworking activities.

8.7.2 Employees who telecommute or telework shall be required to maintain the same controls over UMS information and systems under their control that process, store, or transmit UMS information as if office based.

9 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

9.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements shall be identified and agreed prior to the development and/or implementation of information systems.

All security requirements shall be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system. Security requirements analysis and specification

Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.

9.2 CORRECT PROCESSING IN APPLICATIONS

Appropriate controls shall be designed into applications, including user developed applications to ensure correct processing. These controls shall include the validation of input data, internal processing and output data.

Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls shall be determined on the basis of security requirements and risk assessment.

9.2.1 Input data validation

Data input to applications shall be validated to ensure that this data is correct and appropriate.

9.2.2 Control of internal processing

Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

9.2.3 Message integrity

Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.

9.2.4 Output data validation

Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

9.3 CRYPTOGRAPHIC CONTROLS

A standard shall be developed on the use of cryptographic controls. Key management shall be in place to support the use of cryptographic techniques.

9.3.1 Policy on the use of cryptographic controls

A standard on the use of cryptographic controls for protection of information shall be developed and implemented.

9.3.1 The use of cryptography for the protection of Compliant Data is specified in section 4. The encryption used for this must be AES256 or an equal or stronger equivalent.

Where specific statutes or contracts require stronger algorithms, those requirements shall prevail.

9.3.2Key management

Key management shall be in place to support UMS' use of cryptographic techniques.

9.3.2 Departments or employees utilizing public key cryptography are responsible for maintaining the security their private keys, and of the public key infrastructure under their control.

9.4 SECURITY OF SYSTEM FILES

Access to system files and program source code shall be controlled, and IT projects and support activities conducted in a secure manner. Care shall be taken to avoid exposure of sensitive data in test environments.

9.4.1 Control of operational software

There shall be procedures in place to control the installation of software on operational systems.

9.4.1 The installation of software on multi-user servers containing Compliant or Business Sensitive Data shall be subject to the formal change management procedures and segregation of duties requirements of this standard.

9.4.2Protection of system test data

Test data shall be selected carefully, and protected and controlled.

9.4.2 Compliant Data shall not be used in the development or test environments. Records that contain Compliant Data elements may be used if the Compliant Data is first masked or altered so that the original value is not recoverable.

9.4.3 Access control to program source code

Access to program source code shall be restricted.

9.4.3 For programs that process Compliant or Business Sensitive Data, initial implementation as well as applied updates and modifications must be produced from specifically authorized and trusted program source libraries and personnel.

9.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

Project and support environments shall be strictly controlled.

Managers responsible for application systems shall also be responsible for the security of the project or support environment. They shall ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

9.5.1 Change control procedures

The implementation of changes shall be controlled by the use of formal change control procedures.

9.5.2 Technical review of applications after operating system changes

When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

9.5.3 Restrictions on changes to software packages

Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.

9.5.3 Modification to software packages that process compliant or business sensitive data shall be authorized by the vendor if required, and conform with change management procedures prior to being modified.

9.5.4 Information leakage

Opportunities for information leakage shall be prevented.

9.5.4 A risk assessment of leak vectors for the life cycle of Compliant or Business Sensitive Data by owners and administrators shall lead to a risk management decision for proper controls.

9.5.5 Outsourced software development.

Outsourced software development shall be supervised and monitored by UMS.

9.5.5 Outsourced developed software shall complete a full user acceptance test prior to being placed into production.

9.6 TECHNICAL VULNERABILITY MANAGEMENT

Technical vulnerability management shall be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations shall include operating systems, and any other applications in use.

9.6.1 Control of technical vulnerabilities

Timely information about technical vulnerabilities of information systems being used shall be obtained, UMS' exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

9.6.1 It is the responsibility of the department or employee who owns or administers a multi-user device to track vulnerabilities in all hardware and software associated with the multi-user device and review of manufacturer and other vulnerability distribution lists and other sources as needed, and to assess, and remediate as necessary, high-impact vulnerabilities within 2 weeks and medium vulnerabilities within 2 months, The tracking of these remediations shall be via the change management process. If remediation is not preformed within the prescribed periods, the CISO, in consultation with the owner/administrator of the system, will make a determination of the risk, and as a result, the device may be removed from the network.

10 INFORMATION SECURITY INCIDENT MANAGEMENT

10.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES

Formal event reporting and escalation procedures shall be in place. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of UMS assets. They shall be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

10.1.1 Reporting information security events

Information security events shall be reported through appropriate management channels as quickly as possible.

10.1.1 Campus IT and UMS ITS Help Desk facilities will support the reporting of information security events by users, ensuring immediate escalation to the applicable Campus or IT organization, and will track incidents to closure.

10.1.1.1 Computer Security Incident Response

Each campus IT organization shall develop and implement a computer security incident response plan that is approved by the CISO and the campus administration that will include conditions for escalation to the System office, and be an annex to their campus and crisis management plan.

Following the receipt of a report of a potential breach involving Compliant Data on a multi-user system, the office of the CISO must be notified by the owning campus IT organization. Notification shall be made to the office of the CISO within 2 hours for multi-user systems and within 4 hours for single user systems unless the involvement of Compliant Data can be ruled out within that time frame. Should a breach of Compliant Data be confirmed on a multi-user or single user system, the CISO must be notified immediately.

Following the receipt of a report of a potential breach involving Business Sensitive Data or Unclassified Data, the office of the CISO must be notified by the owning campus IT organization within 24 hours

unless the involvement of Business Sensitive Data or Unclassified Data can be ruled out or resolved within that time frame.

10.1.1.2 Non IT-Related Security Incident Response

Following the receipt of a report of a potential breach involving Compliant Data, the CISO must be notified by the Campus within 1 hour unless the involvement of Compliant Data can be ruled out within that time frame. Should a breach of Compliant Data be confirmed, the CISO must be notified immediately.

Following the receipt of a report of a potential breach involving Business Sensitive Data or Unclassified Data, the CISO must be notified by the Campus within 8 hours unless the involvement of Business Sensitive Data or Unclassified Data can be ruled out or resolved within that time frame.

Weekly reports of any reported weaknesses and incidents and the actions taken to close them will be provided to the office of the CISO.

10.1.2 Reporting security weaknesses

All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

10.1.2 UMS Help Desk facilities will support the reporting of information security weaknesses by users, ensuring immediate escalation to the applicable campus or System IT organization, and will track these reports to closure. It is the responsibility of the campus or System IT organization to execute the corrective actions of reported weaknesses. Monthly reports of any reported weaknesses and the actions taken to close them will be provided to the CISO.

10.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

Responsibilities and procedures shall be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement shall be applied to the response to, monitoring, evaluating, and overall management of information security incidents.

Where evidence is required, it shall be collected to ensure compliance with legal requirements.

10.2.1 Responsibilities and procedures

Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.

10.2.1 Management responsibilities will be conveyed to all supervisors during annual security and awareness training.

10.2.2Learning from information security incidents

There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

10.2.2 An after-action report, or post-mortem report will be developed by the campus or System IT organization responsible for closing incident or weakness reports, and delivered to the CISO.

10.2.3Collection of evidence

Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

10.2.3 The campus police department, or local law enforcement where sworn campus police are not available, shall be utilized to ensure proper procedures in evidence collection, chain of custody, storage, and delivery whenever an incident may involve a violation of law such as illegal entry.

11 BUSINESS CONTINUITY MANAGEMENT

11.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

A business continuity management process shall be implemented to minimize the impact on UMS and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process shall identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

The consequences of disasters, security failures, loss of service, and service availability shall be subject to a business impact analysis. Business continuity plans shall be developed and implemented to ensure timely resumption of essential operations. Information security shall be an integral part of the overall business continuity process, and other management processes within UMS.

Business continuity management shall include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

11.1.1 Including information security in the business continuity management process

A managed process shall be developed and maintained for business continuity throughout UMS that addresses the information security requirements needed for UMS' business continuity.

11.1.1 Each business unit or division in UMS shall develop a business continuity plan to address how their organizations function can be continued and what security requirements they would have in the absence of assets upon which they currently rely.

11.1.2Business continuity and risk assessment

Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

11.1.2 Each business unit or division in UMS shall perform a business impact analysis as part of the development of their business continuity plan to identify types of events that may impact their roles, the likelihood of the event, and the impact it would have. The security of the information utilized by the supervisors department shall be part of the business impact analysis.

11.1.3Developing and implementing continuity plans including information security

Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

11.1.4Business continuity planning framework

A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

11.1.5 Testing, maintaining and re-assessing business continuity plans

Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

11.1.5 Each plan shall be tested not less than every two years.

12 COMPLIANCE

12.1 COMPLIANCE WITH LEGAL REQUIREMENTS

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements.

Advice on specific legal requirements shall be sought from UMS' legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).

12.1.1 Identification of applicable legislation

All relevant statutory, regulatory, and contractual requirements and UMS' approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and UMS.

12.1.2 Intellectual property rights (IPR)

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

12.1.2 No software products that require a license shall be used on UMS-owned devices without proper licensure.

All intellectual property rights specified by UMS policy, statute, contract, or applicable agreement shall be fully observed as they are consistent with applicable law.

12.1.3 Protection of organizational records

Important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

12.1.3 UMS records will be handled in accordance with the Records Retention Administrative Practice Letter (APL) IV-D found at http://www.maine.edu/pdf/IV-DRecordRetentionPractices.pdf.

12.1.4 Data protection and privacy of personal information

Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

12.1.5 Prevention of misuse of information processing facilities

Users shall be deterred from using information processing facilities for unauthorized purposes.

12.1.5 Misuse of UMS assets shall be addressed using normal UMS disciplinary processes. Misuse of Compliant or Business Sensitive Data, or the equipment on which it resides, shall be considered a breach of the Information Security Policy, and dealt with accordingly.

12.1.6Regulation of cryptographic controls

Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

12.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE

The security of information systems shall be regularly reviewed.

Such reviews shall be performed against the appropriate security policies and the technical platforms and information systems shall be audited for compliance with applicable security implementation standards and documented security controls.

12.2.1 Compliance with security policies and standards

Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

12.2.2 Technical compliance checking

Information systems shall be regularly checked for compliance with security implementation standards.

12.2.2 It is the responsibility of the department or employee who owns or administers a multi-user device to ensure continued compliance of that information processing facility with these information security policies and standards.

It is the responsibility of the office of the CISO to audit the continued compliance throughout UMS.

12.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS

There shall be controls to safeguard operational systems and audit tools during information systems audits.

Protection is also required to safeguard the integrity and prevent misuse of audit tools.

12.3.1 Information systems audit controls

Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.

12.3.2 Protection of information systems audit tools

Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

GLOSSARY

Asset
Anything that has value to the organization. An asset is subject to this policy and these standards if the asset is either owned by UMS; or has been entrusted to UMS with a statutory, contractual, or other understanding that the asset will be protected by UMS while under their control.

Bailment
The transfer of possession but not ownership of personal property (as goods) for a limited time or specified purpose (as transportation) such that the individual or business entity taking possession is liable to some extent for loss or damage to the property.

Computing Device
Anything that stores, processes, or transmits information

Control
A means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
NOTE Control is also used as a synonym for safeguard or countermeasure.

Criticality Rating
A measure of the impact of a compromise of the confidentiality, integrity, or availability of an information asset. The criticality rating of any asset is equal to the highest criticality rating of any subordinate or contained asset. See the "Calculating a Criticality Rating" section on the UMS Information Security website.

Customer
In this document, "customer" refers to anyone who receives goods or services from UMS in a capacity other than as an employee. For the purposed of this document, this includes students.

Device, Computing
Any electronic equipment or article that can process or transmit information, including but not limited to PCs, servers, tablets, PDA's, telephones, cell phones, smart-phones, WiFi access points, routers, switches, firewalls, network traffic management or monitoring equipment.

Device, Mobile
Any computing device that is designed to be used in regularly changing locations, or other than in a fixed location. Mobile devices would include, but not be limited to, cell phones; smart phones; laptop, notebook, palmtop, and tablet computers.

Device, Multi-user
Any computing device that is designed and used to support more than one user in an environment where each user is supported by a separate environment or account, either simultaneously or with only a single user at a time, such as a server. For the purposes of this document, a multi-user device refers to a server class machine and does not refer to an individual computing device which is intended to support one user at a time (such as a PC with multiple log in accounts).

Device, Single-user
Any computing device that is used to support a single user, such as a PC. A single user device may be capable of being used as a multi-user device, but it is used to support a single user.

Enhanced Access Controls
Enhanced access controls are those beyond a simple userid and single password. This may include multifactor authentication, multiple or multi-level passwords (e.g. one password to log in, a second password to write or modify information), physical proximity to the device, or access limited to specific devices).

Guideline
A description that clarifies what should be done and how, to achieve the objectives set out in policies.

Incident
A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

Information
Information in this document, information refers to information that is either wholly or partially owned by UMS, or that has been entrusted to UMS with the expectation that the information will enjoy protections of confidentiality, integrity, or availability by statute, contract, or other agreement. .

Information Asset
Anything that stores, processes, transmits, or is information. A computing device or the information itself.

Information Owner
Also may be known as the information custodian: the person primarily responsible for the protection of the confidentiality, availability, and integrity of the information in question. The information owner determines who may have access to information, and under what circumstances. They may delegate the administration of managing access, but not the responsibility.

Information Processing Facilities
Any information processing system, service, or infrastructure; or the physical locations housing them. This includes but is not limited to computing devices, single and multi-user devices, and mobile devices and the rooms that house them.

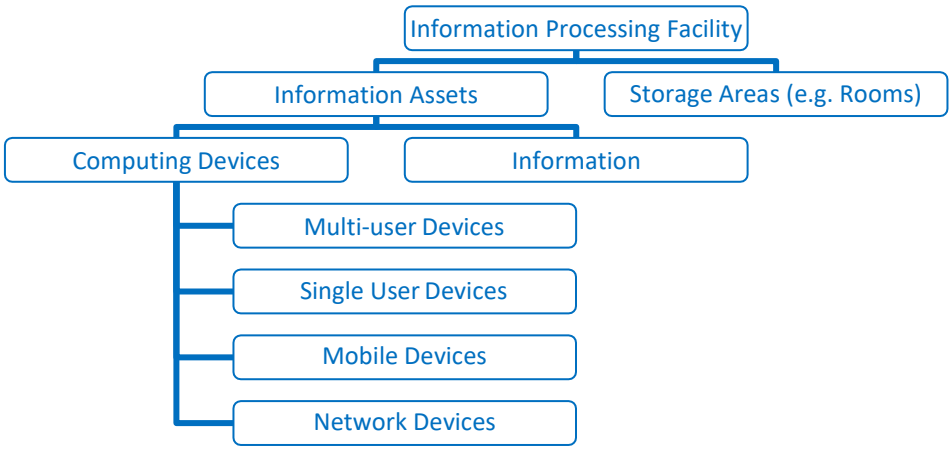
Information Security
Information Security is the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional; although Information Security often involves electronic data, hard copy (written or printed) and verbally transmitted information require appropriate safeguards. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information Security Event
An information security event is an identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

Information Security Incident
An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising or adversely impacting business operations and threatening information security.

Information Nomenclature Hierarchy
Equipment items that store, process, or transmit information are called computing devices. Single user devices, multi user devices, and mobile devices together are called computing devices. Information and computing devices together are called an information asset.

Information assets together with the places that they are kept (rooms, data centers, file cabinets, etc) are called an information processing facility.



Mission Critical
Any asset whose compromise would significantly and adversely impact the ability of the University to deliver core services.

Mobile Code
Mobile code is software which transfers between computers and then executes automatically without explicit user interaction. Examples include: JavaScript, VBScript, Java applets, ActiveX controls and Flash animations.

Network Service
A service installed on the network to ensure security and to provide shared resources. Examples of network services are firewalls, intrusion detection systems, authentication servers and directory services.

Policy
The overall intention and direction as formally expressed by management.

Risk
The combination of the probability of an event and its consequence.

Risk Analysis
The systematic use of information to identify sources and to estimate the risk.

Risk Assessment
The overall process of risk analysis and risk evaluation.

Risk Evaluation
The process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk Management
The coordinated activities to direct and control an organization with regard to risk. NOTE: Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.

Risk Treatment
The process of selection and implementation of measures to modify risk.

Third Party
A person or entity or organization that is recognized as being independent of the parties involved, as concerns the issue in question.

Threat
A potential cause of an unwanted incident, which may result in harm to a system or organization.

UMS
In the context of the standards, "UMS" is the University of Maine System and all of its campuses and subordinate components.

Vulnerability
A weakness of an asset or group of assets that can be exploited by one or more threats.

Vulnerability Impact Level
Vulnerability impact is calculated using the NIST Common Vulnerability Scoring System found at http://nvd.nist.gov/cvss.cfm. This system quantitatively scores vulnerability impact on a scale of 0.0-10.0, with vulnerabilities then qualitatively rated by the score:

- CVSS base score between 7.0 and 10.0 = HIGH
- CVSS base score between 4.0 and 6.9 = MEDIUM
- CVSS base score between 0.0 and 3.9 = LOW

Some vulnerability scanners also report a "critical" impact level for some vulnerabilities, but for purposes of this document a "critical" vulnerability impact will be considered as "high".

--- END ---