Information Security Policy

3/14/2011

Version 1.0

The University of Maine System
Information Security Policy

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.

1.1.2 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.

2.1.4 Authorization process for information processing facilities

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

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.

2.1.6 Contact with authorities

Appropriate contacts with relevant authorities shall be maintained.

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.

2.1.8 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.

2.2 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.

2.2.2 Addressing security when dealing with customers

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

2.2.3 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.

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.

3.2 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.

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.

4.1.2 Ownership of assets

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

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.

4.2 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.

4.2.2 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.

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.

5.1.2 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.

5.1.3 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.

5.2.3 Disciplinary process

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

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.

5.3.2 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.

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.

6.1.1 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.

6.1.2 Physical entry controls

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

6.1.3 Securing offices, rooms, and facilities

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

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.

6.1.5 Working in secure areas

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

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.

6.2.2 Supporting utilities

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

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.

6.2.5 Security of equipment off-premises

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

6.2.6 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.

6.2.7 Removal of property

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

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.

7.1.2 Change management

Changes to information processing facilities and systems shall be controlled.

7.1.3 Segregation of duties

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

7.1.4 Separation 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.

7.2 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.

7.2.1 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.

7.2.2 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.

7.2.3 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.

7.3 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.

7.3.2 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.

7.4 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.

7.4.2 Controls 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.

7.6 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.

7.6.2 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.

7.7.2 Disposal of media

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

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.

7.7.4 Security of system documentation

System documentation shall be protected against unauthorized access.

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.

7.8.3 Physical media in transit

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

7.8.4 Electronic messaging

Information involved in electronic messaging shall be appropriately protected.

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.

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.

7.9.2 On-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.

7.9.3 Publicly available information

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

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.

7.10.2 Monitoring system use

Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.

7.10.3 Protection of log information

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

7.10.4 Administrator and operator logs

System administrator and system operator activities shall be logged.

7.10.5 Fault logging

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

7.10.6 Clock synchronization

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

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.

8.2 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.

8.2.2 Privilege management

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

8.2.3 User password management

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

8.2.4 Review of user access rights

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

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.

8.3.2 Unattended user equipment

Users shall ensure that unattended equipment has appropriate protection.

8.3.3 Clear 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.

8.4 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.

8.4.5 Segregation in networks

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

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).

8.4.7 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.

8.5.2 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.

8.5.3 Password management system

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

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.

8.5.6 Limitation of connection time

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

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.

8.7 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.

8.7.2 Teleworking

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

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.

9.1.1 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.

9.3.2 Key management

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

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.

9.4.2 Protection of system test data

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

9.4.3 Access control to program source code

Access to program source code shall be restricted.

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.

9.5.4 Information leakage

Opportunities for information leakage shall be prevented.

9.5.5 Outsourced software development.

Outsourced software development shall be supervised and monitored by UMS.

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.

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.

10.1.2 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.

10.2 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.

10.2.2 Learning 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.

10.2.3 Collection 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).

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.

11.1.2 Business 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.

11.1.3 Developing 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.

11.1.4 Business 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.

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.

12.1.3 Protection of organizational records

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

12.1.4 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.

12.1.6 Regulation 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.

12.3 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.

--- END ---