SECTION: Information Technology **Number: 10.05.01**
AREA: Information Security

SUBJECT: Information Security Program

I. PURPOSE AND SCOPE

The University of Houston's information resources are vital academic and administrative assets which require appropriate safeguards. Effective information security controls must be employed to appropriately eliminate or mitigate the risks posed by potential threats to the university's information resources. Measures must be taken to protect these resources against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate.

II. POLICY STATEMENT

The University of Houston has a system of internal controls in place to safeguard the security, confidentiality, integrity and availability of its information resources. It is the policy of the university to:

- Protect information resources based on risk against accidental or unauthorized disclosure, modification, or destruction and assure the confidentiality, integrity, and availability of university data;
- Apply appropriate physical and technical safeguards without creating unjustified obstacles to the conduct of the business and research of the university; and
- Comply with applicable state and federal laws and rules governing the security of information resources.

III. DEFINITIONS

A. Information Owner: An information owner is the person responsible for the business use of a collection of information or the business function supported by a system (e.g., the Registrar is the information owner of student records). The information owner may also be responsible for other information resources including personnel, equipment, and information technology that support their business function. The head of a respective college, division, or department may be the information owner, and ownership may be shared by managers of different departments.

B. Information Custodian: An information custodian is a person (or department) providing operational support for an information resource (e.g., server administrators).

C. Information Resource: Procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.

D. User: A user is an individual authorized to access an information resource in accordance with information owner-defined controls and access rules.

IV. INFORMATION SECURITY RESPONSIBILITIES

1. Chief Information Officer

The Chief Information Officer (CIO) serves as the University Information Resource Manager (IRM), as defined by the State of Texas. In this role, the CIO is responsible for the following activities as delegated by the President:

- Protection of university information resources
- Review and approval of information ownership
- Designation of an information security officer
- Approval of the information security program
- Identification of an independent party to review the information security program for effectiveness and compliance with appropriate laws
- Risk management decisions to accept exposure or protect data
- Approval of the business continuity plan

2. Chief Information Security Officer

The Chief Information Security Officer (CISO) is responsible for administering the information security program to ensure the confidentiality, integrity and availability of information resources. The CISO reports to the CIO. Duties of the CISO include:

- Developing and recommending policies and establishing procedures and practices to ensure the security of information resources against unauthorized or accidental modification, destruction or disclosure.
- Documenting and maintaining an up-to-date information security program, which must be approved by the President or designee.
- Monitoring the effectiveness of defined controls for mission critical information.
- Reporting, at least annually, to the President or designee, the status and effectiveness of information resources security controls.
- Performing and documenting a risk assessment of information resources and submitting a security risk management plan based on the assessment to the President or designee for approval.
- Establishing a perimeter protection strategy.
- Issuing exceptions to information security requirements or controls. These exceptions must be justified, documented and communicated as part of the risk assessment process.
- Reporting a summary of security-related events to the Texas Department of Information Resources on a monthly basis.
- Ensuring an information security training and awareness program is implemented and managed appropriately.

3. College/Division Information Security Officer

As defined in MAPP 10.03.06, the College/Division Information Security Officer (C/D-ISO) is responsible for managing the college or division's information security functions in accordance with the established policies and guidelines. This role is often filled by a

director or manager and should report to the C/D-Information Resource Manager (IRM) or directly to the vice president of the division or dean of the college.

4. Information Owner

Information owners are responsible for and authorized to:

- Approve and review access to assigned information resources.
- Approve requests for information from assigned information resources.
- Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures.
- Determine an information resource asset's value and criticality.
- Specify data control requirements and convey them to users and custodians.
- Specify appropriate controls, based on a risk assessment, to protect the information resources from unauthorized modification, deletion, or disclosure. These controls extend to information resources and services outsourced by the university.
- Confirm that controls are in place to ensure the security of data and other assigned information resources.
- Ensuring a backup and recovery plan is developed and implemented by the Information Custodian.
- Approve, justify, document, and be accountable for exceptions to security controls submitted to and approved by the CISO.

5. Information Custodian

Information custodians, including third party entities providing outsourced information resources services, are responsible for:

- Releasing information or allowing access to information only as approved by the information owner.
- Ensuring authenticated access, as designated by the information owner, through an enterprise supported authentication method.
- Implementing the controls specified by the information owner.
- Providing physical, technical, and procedural safeguards for the information resources in accordance with university policies.
- Assisting information owners in evaluating the cost-effectiveness of controls and monitoring.
- Implementing monitoring techniques and procedures for detecting, reporting, and investigating security incidents.

6. User

Users of information resources are responsible for:

- Using information resources only for defined purposes
- Complying with established controls for information resources

- Complying with the requirements of MAPP 10.03.01, Acceptable Use of Information Resources.

- Taking an active role in protecting university data and information resources including compliance with MAPP 10.05.03, Data Classification and Protection and SAM 01.D.06, Protection of Confidential Information.

V. INFORMATION SECURITY CONTROLS

A. Account Management

1. Access to university information resources must be accomplished through the assignment of a unique identifier for each user. Use of shared or departmental accounts is prohibited.

2. User access must be appropriately modified or removed when the user's role or responsibilities within the university change.

3. Access to university information systems and applications will be reviewed regularly to verify users have the appropriate level of access to data.

4. User access must employ the use of a password. The degree of complexity of the password is dependent upon the highest level of data that can be accessed by the user. Passwords must be changed regularly. A strong password must contain each of the following:

   a. At least 8 characters

   b. At least one alphabetic character (upper or lower case, a-z or A-Z)

   c. At least one number (0-9)

   d. At least one special character (!, @, #, $, %, ^, &, (,), *)

B. Elevated Access Privileges

1. Accounts determined as having elevated access privileges are those which meet any of the following criteria:

   a. allow for system administration of an information resource

   b. allow the user to create and control the access of others to an information resource

   c. allow the user the ability to bypass implemented system controls

2. Users must be made aware of any elevated access privileges granted to their accounts. Abuse of such privileges will not be tolerated. Users with elevated access privileges must adhere to the following access requirements:

   a. Accounts with elevated access privileges are designed for use only to perform specific job functions for which the user has been authorized and only for official university business. Users are responsible for ensuring these accounts are not used for tasks not requiring the elevated access privileges, e.g., web browsing, etc. or for personal use.

b. Only the Chief Information Security Officer can authorize an individual's elevated access privileges to perform investigations relating to the potential misuse of information resources by an individual user.

c. Passwords for accounts with elevated access privileges must change when any individual knowing the password leaves the department or University or changes roles within the department; or upon a change in the vendor personnel assigned to University contracts having password access.

d. When special privileges are needed for auditing, software development, software installation, or other defined needs, they:

- Must be authorized by the appropriate department head or owner;
- Must be created with an expiration date when supported; and
- Must be removed and disabled when work is complete.

C. Auditing − Authorized personnel shall be responsible for, and have the ability to, audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information. Appropriate audit trails must be maintained to provide accountability for updates to critical information, hardware, and software and for all changes to automated security or access rules. Depending on the risk assessment of the information resource, a sufficiently complete history of transactions must be maintained to permit an audit of the information resources system by logging and tracking the activities of individuals through the system.

D. Backup and Recovery − Backups must be completed to ensure data and applications are recoverable in case of events such as natural disasters, system disk drive failures, or systems operations errors. The need for backup is commensurate with the criticality level of the data or system, as defined in MAPP 10.05.03, Data Classification and Protection. The information owner must ensure a backup and recovery plan exists and contains the following:

- Procedure for recovering data and applications in case of an unexpected event
- Assignment of responsibility for performing the backup
- Requirements for off-site storage needs
- Physical and network access controls for on-site and off-site storage
- Process to ensure backups are viable and can be recovered (for example, routine testing of backup and recovery procedures)

E. Change Management − The University's Information Resources infrastructure is constantly changing and evolving to support the mission of the University. Computer networks, systems, and applications require planned outages for upgrades, maintenance, and fine-tuning. Change management processes should ensure information resources are protected against improper modification before, during and after system implementation. This includes changes implemented on an emergency basis.

F. Data Classification − All University information must be classified and appropriate safeguards implemented in accordance with MAPP 10.05.03, Data Classification and Protection.

G. Identification/Authentication

1. Each user of information resources must be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification must be authenticated before the information resources system may grant that user access.

2. Information resources systems shall contain authentication controls that comply with documented university risk management decisions.

3. Enterprise authentication sources should be used for authentication whenever possible.

   a. College/Division/Departments developing or implementing software or applications requiring authentication must utilize UIT enterprise authentication sources. Exceptions may be granted with business justification and must be approved by the CISO.

   b. Users should be authenticated by university systems prior to accessing third-party provider sites delivering services whenever possible. University user identification data should not be provided to third party providers for authentication purposes without the approval of the CISO.

H. Perimeter Protection Strategy − The perimeter protection strategy for the University includes implementation and proper configuration of network devices including, but not limited to, firewalls, intrusion detection/prevention systems, and a DMZ (a network boundary between a public and a private network). UIT Security is responsible for ensuring the policies associated with these devices are properly defined, monitored and enforced.

I. Physical Security − Information resources must be physically protected. The level of protection should be based on the criticality of the data contained in the information resource. Physical access to mission critical information resources and resource facilities must be managed to ensure information resources are protected from unlawful or unauthorized access, use, modification or destruction. All information resources must be protected from environmental hazards.

J. Security Awareness and Training − All users of University information resources will participate in Security Awareness and Training regularly. Awareness and training efforts cover applicable state and federal laws, information security best practices, and identification and reporting of information security incidents.

K. Security Incident Handling & Information Disclosure − All security incidents must be reported and investigated in accordance with MAPP 10.05.02, Information Security Incident Reporting and Investigation. Policies related to information disclosure are found in SAM 01.D.06, Protection of Confidential Information.

L. Security Monitoring and Vulnerability Testing − University Information Technology (UIT) Security will monitor the university's security program regularly, to ensure that information resources security controls are current, adhered to and effective. Monitoring activities include, but are not limited to, vulnerability scans of systems and networks, as well as review of:

- Continual automated intrusion detection and prevention logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Data backup recovery logs
- Help desk logs
- Other log and error files

M. Systems development, acquisition, and testing

1. Test environments must be kept either physically or logically separate from production environments. Copies of production data are not to be used for testing unless the data has been authorized for public release or unless all users involved in testing are otherwise authorized access to the data.

2. Information security, security testing, and audit controls must be included in all phases of the system development lifecycle or acquisition process.

3. All security-related information resources changes must be approved by the information owner through a change control process. Approval must occur prior to implementation.

VI. REVIEW AND RESPONSIBILITIES:

Responsible Party: Associate Vice President for Information Technology and Chief Information Officer

Review: Every three years on or before June 1

VII. APPROVAL

Carl Carlucci
Executive Vice President for Administration and Finance

Renu Khator
President

Date of President's Approval: October 19, 2011

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	10/19/2011	Initial version