SECTION: Information Technology **NUMBER: 07.A.10**

AREA: Computing Services

SUBJECT: Information Security Program

1. PURPOSE

Information resources of the University of Houston System (UH System) 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.

2. POLICY

The UH System has internal controls in place to safeguard the security, confidentiality, integrity and availability of its information resources. It is the policy of the UH System to:

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

3. DEFINITIONS

3.1. Information Owner: An information owner is the person(s) with statutory or operational authority and responsibility 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 head of a respective college, division, or department may be the information owner, and ownership may be shared by managers of different departments.

3.2. Information Custodian: An information custodian is a department, agency, or third-party service provider responsible for implementing the information owner-defined controls and access to an information resource (e.g., server administrators).

3.3. Information Resource: As defined in Texas Government Code §2054.003(7), procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

3.4. User: An individual, process or automated application authorized to access an information resource in accordance with federal and state law, UH System and university policy, and information owner procedures and rules.

4. INFORMATION SECURITY RESPONSIBILITIES

4.1. Chief Information Officer

The Chief Information Officer (CIO) of the UH System and each university serve as the agency Information Resource Managers (IRM), as defined by the State of Texas. In this role, the CIOs are responsible for the following activities as delegated by the Chancellor and Presidents:

A. Review and approval of information ownership;

B. Endorsement of the information security program;

C. Risk management decisions to accept exposure or protect data; and

D. Approval of the business continuity plan.

4.2. Chief Information Security Officer

The UH System Chief Information Security Officer (CISO), along with Information Security Officers (ISO) designated for each university, are responsible for administering the information security program to ensure the confidentiality, integrity and availability of information resources. Duties of the CISO/ISOs include:

A. Developing and maintaining an institution-wide information security plan as required by Texas Government Code, Section 2054.133.

B. Developing and maintaining information security policies and procedures to ensure the security of information resources against unauthorized or accidental modification, destruction or disclosure and the identification of information security risks.

C. Working with business and technical resources to ensure controls are utilized to address information security risks.

D. Training and overseeing personnel with significant responsibilities for information security.

E. Providing guidance and assistance to senior UH System and university officials, information owners, information custodians and end users concerning their responsibilities related to information security.

F. Ensuring annual information security risk assessments are performed and documented by information owners.

G. Coordinating the review of data security requirements specifications, and, if applicable, third-party risk assessment of any new applications or services that receive, maintain, and/or share confidential data.

H. Reporting, at least annually, to the Chancellor, President or designee, the status and effectiveness of information security controls.

I. Issuing exceptions to information security requirements or controls. These exceptions must be justified, documented and communicated as part of the risk assessment process.

J. Ensuring a summary of security-related events is reported to the Texas Department of Information Resources on a monthly basis.

K. Ensuring an information security training and awareness program is implemented and managed appropriately.

L. Addressing security incidents in accordance with applicable law and UHS and university policies, guidelines and procedures.

4.3. College/Division Information Security Officer

When defined per university, 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.

4.4. Information Owner

Information owners are responsible for and authorized to:

A. Classify the data under their authority in accordance with SAM 07.A.08, Data Classification and Protection.

B. Approve and review access to assigned information resources.

C. Approve requests for information from assigned information resources.

D. Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures.

E. Coordinate information security control requirements with the System CISO or university ISO.

F. Participate in risk assessments initiated by the UH System CISO, university ISO, or designee.

G. Justify, document, and be accountable for exceptions to security controls submitted to and approved by the UH System CISO or the university ISO.

4.5. Information Custodian

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

A. Implementing controls required to protect information and information resources based on the classification and risks specified by the information owner or as specified by UH System and university information security policies, procedures and standards.

B. Providing owners with information to evaluate the cost-effectiveness of controls and monitoring.

C. Adhering to monitoring techniques and procedures for detecting, reporting and investigating information security incidents.

D. Provide the necessary information to enable appropriate information security training to employees.

E. Ensure information is recoverable in accordance with risk management decisions.

F. Releasing information or allowing access to information only as approved by the information owner.

G. Ensuring authenticated access, as designated by the information owner, through an enterprise supported authentication method.

H. Providing physical, technical, and procedural safeguards for the information resources in accordance with UH System and university policies.

4.6. User

Users of information resources are responsible for:

A. Using information resources only for defined purposes.

B. Formally acknowledging compliance with established information security controls and UH System and university policies to prevent unauthorized or accidental disclosure, modification or destruction of information resources.

C. Complying with the requirements of university policies regarding acceptable use of information resources.

D. Taking an active role in protecting UH System and university data and information resources including compliance with SAM 07.A.08, Data Classification and Protection and SAM 01.D.06, Protection of Confidential Information.

5. INFORMATION SECURITY CONTROLS

5.1. Account Management

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

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

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

5.1.4. 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.

The following password controls must be implemented in accordance with risk management decisions:

A. Password expiration

B. Password history

C. Password lockout timeframe

D. Password complexity – A strong password must contain each of the following:

- At least eight (8) characters
- At least one alphabetic character (upper or lower case, a-z or A-Z)
- At least one number (0-9)
- At least one special character (!, @, #, %, ^, &, (,), *)

5.2. Elevated Access Privileges

5.2.1. 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; or

C. Allow the user the ability to bypass implemented system controls.

5.2.2. 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 UH System or 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 UH System CISO or university ISO 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, changes roles within the department, or terminates employment; or upon a change in the vendor personnel assigned to UH System or university contracts having password access; and

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.

5.2.3. Reviews of elevated access privileges to ensure the appropriateness of system elevated access should be performed at least annually. When inappropriate elevated access is identified, immediate action should be taken to remove the access. Documentation of reviews, including any action taken in response to inappropriate access, should be retained for at least three years in compliance with SAM 03.H.01, Records Retention.

5.3. 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 Level 1 data as defined by SAM 07.A.08, Data Classification and Protection. 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.

5.4. 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 classification level of the data or system, as defined in SAM 07.A.08, Data Classification and Protection. The information owner must ensure a backup and recovery plan exists and contains the following:

A. Procedure for recovering data and applications in case of an unexpected event;

B. Assignment of responsibility for performing the backup;

C. Requirements for off-site storage needs;

D. Physical and network access controls for on-site and off-site storage; and

E. Process to ensure backups are viable and can be recovered (for example, routine testing of backup and recovery procedures).

5.5. 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 be in place to ensure information resources are protected against improper modification before, during and after system implementation. This includes changes implemented on an emergency basis.

5.6. Data Classification

All UH System and university information must be classified and appropriate safeguards implemented in accordance with SAM 07.A.08, Data Classification and Protection.

5.7. Identification/Authentication

A. 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.

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

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

1. Colleges/Divisions/Departments developing or implementing software or applications requiring authentication must utilize university enterprise authentication sources. Exceptions may be granted with business justification and must be approved by the System CISO or university ISO.

2. 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 System CISO or university ISO.

5.8. Internet Websites/Mobile Applications

Internet websites or mobile applications that process confidential information, as defined as Level 1 Data in SAM 07.A.08, Data Classification and Protection, must be reviewed and approved by the University ISO prior to deployment. The following information will be required for the review:

A. The architecture of the website or application;

B. The authentication mechanism for the website or application; and

C. The administrator level access to data included in the website or application.

In addition, the Internet website or mobile application will be subject to a vulnerability and penetration test performed by the UHS Information Security department.

5.9. Physical Security

Information resources must be physically protected. The level of protection should be based on the classification of the data, as defined in SAM 07.A.08, Data Classification and Protection, contained in (at rest) or passing through (in transit) 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.

5.10. Security Awareness and Training

All users of UH System and 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.

5.11. Security Incident handling and Information Disclosure

All security incidents must be reported and investigated in accordance with SAM 07.A.11, Information Security Incident Reporting and Investigation. Policies related to information disclosure are found in SAM 01.D.06, Protection of Confidential Information. Suspected security incidents involving sensitive personal information shall be handled according to the guidelines located on the Office of General Counsel website: http://www.uh.edu/legal-affairs/general-counsel/protection-and-confidential-information/Security%20Incident%20Response%20Guidelines.pdf.

5.12. Security Monitoring and Vulnerability Testing

Security monitoring will be performed regularly to ensure 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;
- Network scanning logs;
- Application logs;
- Data backup recovery logs;
- Help desk logs; and
- Other logs and error files.

5.13. Systems Development, Acquisition, and Testing

A. 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.

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

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

D. All newly-developed systems must undergo a vulnerability scan performed by the UHS Information Security department prior to being released for production.

6. REVIEW AND RESPONSIBILITY

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

Review: Every five years on or before June 1

7. APPROVAL

Approved: Jim McShan
Senior Vice Chancellor for Administration and Finance

Renu Khator
Chancellor

Date: February 8, 2019

8. REFERENCES

System Administrative Memorandum (SAM) 01.D.06 – Protection of Confidential Information

SAM 03.H.01 – Records Retention

SAM 07.A.08 – Data Classification and Protection

SAM 07.A.11 – Information Security Incident Reporting and Investigation

Texas Government Code, Section 2054.003 (7)

Texas Government Code, Section 2054.133

Title 1, Texas Administrative Code, Chapter 202

REVISION LOG

Revision Number	Approval Date	Description of Changes
1	02/08/2019	Initial version (formerly MAPP 10.05.01)