UNIVERSITY of HOUSTON SYSTEM

INFORMATION SECURITY

GENERAL GUIDELINES & BEST RACTICES FOR MANAGEMENT OF INFORMATION RESOURCES (per SAM 07.A.10, Information Security Program)

INFORMATION SECURITY RESPONSIBILITIES

Information owners are responsible for and authorized to:

- Classify the data under their authority in accordance with SAM 07.A.08, Data Classification and Protection.
- Approve and review access to assigned information resources.
- Approve requests for information from assigned information resources.
- Justify, document, and be accountable for exceptions to security controls submitted to and approved by the UH System CISO or the University ISO.

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

- 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.
- Ensure information is recoverable in accordance with risk management decisions.
- Ensuring authenticated access, as designated by the information owner, through an enterprise supported authentication method such as CougarNet Active Directory.
- Providing physical, technical, and procedural safeguards for the information resources in accordance with UH System and university policies.

INFORMATION SECURITY CONTROLS

Account Management

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

☐ User access is appropriately modified or removed when the user’s role or responsibilities within the UH System or university change.

☐ Access to information systems and applications is reviewed regularly to verify users have the appropriate level of access to data.

☐ User access employs the use of a strong password. Password policy is enforced through device membership via an enterprise supported authentication method, such as CougarNet Active Directory.

Auditing

☐ Audit logging is enabled.

☐ Authorized personnel is responsible for, and has 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 are 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 is maintained to permit an audit of the information resources system by logging and tracking the activities of individuals through the system.

GENERAL GUIDELINES & BEST RACTICES FOR MANAGEMENT OF INFORMATION RESOURCES
(per SAM 07.A.10, Information Security Program)

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 has a backup and recovery plan that 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).

Identification/Authentication

- □ Each user of information resources is assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification is authenticated before the information resources system grants that user access.
- □ Information resources systems contain authentication controls that comply with documented university risk management decisions.
- □ Enterprise authentication sources, such as CougarNet Active Directory, are used for authentication.

Physical Security

- □ Information resources are physically protected. The level of protection is 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 is managed to ensure information resources are protected from unlawful or unauthorized access, use, modification or destruction.
- □ All information resources are protected from environmental hazards.

Security Incident Handling and Information Disclosure

- □ A division/college/department specific Information Resource Plan exists and is consistent with university policies, guidelines, and standards.
- □ All security incidents are 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.

Security Monitoring and Vulnerability Testing

- □ Security monitoring is 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:
  - □ Intrusion detection or prevention logs.
  - □ Firewall or network logs
  - □ Vulnerability scanning or anti-virus logs
  - □ Application or system logs
  - □ Data backup recovery logs