University of Houston Clear Lake

Administrative Policies and Procedures

Information Security Program Procedural Handbook for Information Owners and Designees (ISPHB03)

Date Issued: November 17, 2016

Last Revision: October 1, 2018

Table of Contents

I. Purpose and Scope

All members of the University of Houston-Clear Lake's (UHCL) faculty and staff, and those contracted to provide information-related services, share the responsibility of protecting the information created by or entrusted to the University to the best of his or her ability.

The University's Information Security Program is risk-based, i.e., the decisions made regarding how information is to be protected is based upon the value of each information resource and the risk to the University if the information resource were to be disclosed to unauthorized individuals, tampered with, or destroyed.

The key to having an effective risk-based information security program is ensuring that the value and risk of each information resource is evaluated by the most appropriate manager in the University who is known as the "Information Owner". For example, the Information Owner for staff information would be the head of Human Resources, the Information Owner for student information would be the Registrar, etc. The Information Owner not only evaluates value and risk of his or her assigned resources, but also makes decisions regarding who should and should not have access to the resource and how that information is permitted to be used.

As Information Owners are responsible for managing a wide variety of data elements, it is common for an Information Owner to designate one or more individuals on staff to make information value and risk decisions on the Information Owner's behalf. However, no matter how many Designees are assigned, the Information Owner is ultimately responsible for all of the information-related decisions that the Designees make.

The documents in this "Procedural Handbook" series have been developed to provide a comprehensive set of generic business procedures that can be used either "as is" or can be tailored by each business area to handle procedural variations driven by specific vendor products. This specific handbook provides procedural guidance for performing information security-related tasks that are relevant to individuals in an Information Owner or Designee role.

II. Applicability

Anyone who serves the University as an Information Owner or Designee should become familiar with the contents of this document. This document assumes that the reader has read and understands the contents of the following program and policy documents:

- **Information Security Program Description, Roles and Program Policies (ISPOL01)**,
- **Acceptable Use Policy for UHCL Information and Systems (ISPOL02)**.

As a UHCL employee or contractor, each Information Owner or Designee also should be familiar with the handbook for all users of UHCL information and systems:

- **Procedural Handbook for Employees and Contractors (ISPHB01)**.

III. Procedures

A. The Information Security Officer's Role in Information Ownership

The University's Information Security Officer must ensure that the Information Owner of each information resource that has been created by or entrusted to UHCL is identified, and that effective mechanisms are in place to disseminate ownership information throughout the University.

The University's Information Security Officer also is expected to assist each Information Owner and Designee is their data classification and risk assessment efforts, and to ensure that mechanisms are in place to ensure that data classification decisions are effectively communicated to the users of UHCL information resources.

B. Information Ownership

The Information Owner for an information resource evaluates its value and risk, makes decisions regarding what roles or individuals should and should not have access to the resource, and how that information is permitted to be used.

When selecting an appropriate Information Owner for an information resource, the person selected should be the head of the department that is most associated with that resource and that has the most comprehensive understanding of the legal and contractual obligations associated with that resource.

It is inappropriate to assign information ownership responsibilities for business-related information to the Information Technology staff. Members of the Information Technology staff typically do not have sufficient familiarity with University business-related information to be able to determine its value and only could speculate about the damage that would be caused if a specific information resource under their care is compromised. Additionally, there are many locations where information can be held outside of the Information Technology group's control.

Although the Information Technology team does not own business-related information, they are Information Owners of all of the information used to manage the computers and networks under their control, such as audit trails, computer performance statistics, etc.

As owning departments are responsible for a wide variety of data elements, it is common for an Information Owner to designate one or more individuals on staff to make information value and risk decisions on the Information Owner's behalf. It is important to note that the Information Owner ultimately is responsible for the decisions made by any of his or her Designees.

C. Data Classification

Each Information Owner is required to determine the value/risk (sensitivity) level associated with each of his or her information resources by evaluating three characteristics:

- Its need to be kept private (confidentiality),
- Its need to have its accuracy guaranteed (integrity), and
- Its need to be available readily (availability).

Knowing the sensitivity of an information resource informs UHCL staff the extent to which the resource needs to be protected and highlights resources that require special attention. Not understanding the sensitivity of the information resources being handled could result in the inadvertent exposure of sensitive information and/or a significant financial and/or reputational loss for the University.

The campuses of the University of Houston System have deployed a data classification scheme that assigns one of the following three levels to each information resource, based upon the three information sensitivity characteristics described above. There are three sensitivity levels that have been defined by the University of Houston System from level 1 (most sensitive) to level 3 (public).

Details regarding each value/risk level can be found in the following University of Houston System Administrative Memoranda:

- **SAM 07.A-08 – Data Classification and Protection**
- **SAM 01.D.06 – Protection of Confidential Information**

D. Information Authorization

In addition to classifying their assigned information resources, each Information Owner or Designee must authorize the use of any of his or her level 1 or level 2 information resources as defined in **SAM 07.A.08 – Data Classification and Protection**.

All authorization requests submitted to the Information Owner or Designee must be made in writing and must include:

- The name and signature of the requestor,
- The name of the information resource,
- The type(s) of access being requested (e.g., view, add, edit/modify, delete), and
- The name and signature of the requestor's supervisor,
- The date that access was authorized,
- The authorization's expiration date, if applicable.

Note – Authorization forms may be signed either physically or electronically.

Authorization requests that are approved must be signed by the appropriate Information Owner or Designee before being submitted to the Information Custodian(s) who manage(s) the context(s) where the information is stored.

Access may be authorized on an individual basis or by functional role. UHCL strongly recommends authorizing access by functional role rather than on an individual basis since it significantly simplifies the provisioning and deprovisioning of access privileges.

When authorizing access to level 1 and level 2 resources, the "principle of least privilege" must be applied, i.e.,

- Except for information resources classified as level 3 data (public), an individual or job role should be permitted to access only the specific information resources that are needed to perform specific job duties, and
- An individual or job role may not be given access to any information resource in a manner beyond that required to perform specific job duties. For example, an individual who is only required to view an information resource must not be given access to update it.

E. Keeping Staff Informed about Information Sensitivity

As part of the authorization process, each Information Owner or Designee must ensure that each individual who is granted access to any of his or her assigned information resources is aware of its sensitivity, what uses are and are not permitted, and with whom the information resources may be shared. For accountability purposes, the information sensitivity level should be conveyed in writing.

F. Annual Risk Assessment

On an annual basis, an information risk assessment must be performed as follows:

- The University's Information Security Officer will work with each Information Owner or Designee to reassess the value/risk associated with their information resources.
- For each information resource, once the reassessment is made, the Information Security Officer will work with the Information Context Managers to review the security of each of their applications and systems that use the resource to ensure that the information is being protected appropriately.
- If the security requirements defined for the resource's sensitivity level are not met, the Information Security Officer will work with the appropriate Information Custodian to remediate any deficiencies.
- The Information Security Officer will summarize the results of the risk assessment and status of the remediation efforts for the University's Executive Management.

G. Illustration of the Information Owner / Information Custodian Interaction

The following example describes the Information Owner / Information Custodian model:

- The Human Resources Department decides to implement a system to purchase an applicant tracking system. The individual who recommends the purchase (Sponsor) contacts the Information Security Officer to ensure that the system meets security and compliance standards.
- The Sponsor and the University's Information Security Officer determine who will be the Information Owner. In this case, that choice is straightforward – the Head of Human Resources.
- The Information Owner may assign ownership duties to one or more Designees in his or her department, or may choose to perform these duties himself or herself.
- The Information Owner or assigned Designee logically groups the system's data elements by sensitivity and defines the specific security requirements for each logical group.
- The Sponsor calls a meeting with the University's Information Security Officer and appropriate Information Custodians who, in this case, would be UHCL Technology Managers. These Technology Managers could include, as necessary:
    - Data center manager
    - Server manager
    - Network manager
    - Database manager
    - Backup media manager
    - Technical services manager
    - Application development manager
    - Others, as identified

All of the Information Custodians must be part of the discussion as early on in the project as possible.

The Information Owner and Information Custodians need to discuss a variety of security and non-security-related topics, such as:

- Infrastructure requirements
- Networking requirements
- Storage technology and sizing requirements
- Backup requirements
- Information security requirements for each information collection, e.g.,
    - What roles should be allowed to access information
    - What types of access are permitted for each role
    - The need for encryption
    - Audit and compliance requirements

The Sponsor is responsible for ensuring that an effective project management approach is being performed to ensure that each participating technology area is fully aware of the functionality expectations and time line for procuring and implementing the solution.

IV. Revision Log

Revision Number	Approval Date	Description of Changes
1	07/12/2016	Initial version
2	12/11/2017	a) Updated of all document links to be consistent with UHCL's new website b) Updated name of UHCL President
3	10/01/2018	Replaced Glen Houston with Anthony Scaturro in the list of approvers

V. Procedural Handbook Review Responsibility

Responsible Parties:

- Associate VP for Information Resources
- Information Resource Manager
- Information Security Officer

Review Period:

- Annually on or before April 30

VI. Approval

- Anthony J. Scaturro
  Information Security Officer
- Ira K. Blake
  President