University of Houston Clear Lake

Administrative Policy and Procedure Library

Information Security Program Description, Roles and Program Policies (ISPOL01)

Date Issued: November 17, 2016

Last Revision: October 1, 2018

Table of Contents

I. Purpose and Scope

Academic and administrative information resources, either created by or entrusted to the University of Houston-Clear Lake (UHCL), are vital University business assets that require appropriate safeguards. Effective information security controls must be employed to appropriately eliminate or mitigate the risks posed by potential threats to UHCL information resources. The measures taken must protect these resources against unauthorized access, disclosure, modification, or destruction, whether accidental or deliberate.

This document provides a description of the UHCL Information Security Program including definitions, roles and responsibilities and guiding principles that are intended to serve as the foundation for all information security-related activities.

II. Program Statement

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

- Protect UHCL information resources based upon risk of accidental or unauthorized disclosure, modification, or destruction, and assure the confidentiality, integrity, and availability of UHCL information resources is properly maintained,
- Comply with applicable state and federal laws and rules governing the security of UHCL information resources, and with the terms of any contractual agreements into which UHCL has entered, and
- Apply appropriate physical and technical safeguards that do not create unjustified obstacles that diminish UHCL's ability to conduct its business effectively.

III. Applicability

Each member of the UHCL community who is authorized to access any non-public, University information is required to:

- Read this document,
- Understand his or her role in the overall program,
- Read other policy and procedural documents associated with his or her role,
- Agree to comply with the information security policies as they apply to his or her role, and
- Formally attest to his or her agreement in writing on an annual basis.

IV. Program Objectives

To achieve the goals defined in the above Policy Statement, UHCL must accomplish the following:

- Ensure that every member of the University of Houston-Clear Lake community who has access to any UHCL information resource understands and agrees to support:
  - The purpose and the goals of the UHCL Information Security Program and its definitions, terminology, roles and responsibilities,
  - His or her own role and responsibilities in protecting UHCL information resources, and
  - The information security-related policies that are applicable to his or her role in the program.
- Assess the risk level associated with each piece of information created by or entrusted to UHCL, specifically the risks of its unauthorized disclosure, tampering, and/or destruction.
- Effectively communicate the assessed risk levels to all individuals who come in contact with UHCL information resources, both the users of those resources and those individuals who provide technical or procedural support to the user community.
- Provide products and services necessary to protect each UHCL information resource in a manner commensurate with the resource's risk level.
- Guide those who use or support the use of UHCL information resources in the proper ways of securing the information at each risk level in physical or electronic form, wherever it is located.

- Continually monitor the effectiveness of the controls that are put in place, and respond accordingly.

V. Definitions

A. Information Resource

An information resource is a collection of related data elements and the procedures, software and physical equipment that are implemented, operated and maintained to create, capture, store, retrieve, modify, delete, process, transmit, administer, and/or manage those data elements in support of a specific University business function. For example, a set of related data, procedures, equipment and software used to support the Human Resource's payroll function could collectively be considered an "employee payroll" information resource.

B. Information Context

An information context is any place where information may be found, e.g.

- In centrally managed computer and network environments
  - Servers
  - File storage facilities
  - Databases
  - Traveling across wired and wireless data and voice networks
- In someone's workspace
  - On a personal computer, tablet or smartphone
  - On printed reports
  - On portable storage media, such as CDs, DVDs, and USB tokens
- In someone's memory
- Carried across the air in a conversation between two individuals

Unlike a tangible, physical item, information can be in many locations or contexts at the same time, making it far more complex to protect. As information finds its way into each context, the level of protection that is afforded that information in that context must meet or exceed the security

requirements specified for that information by its owner, otherwise that context becomes the "weak link" in our overall information protection scheme. Once information is exposed, its source really does not matter. Thus,

INFORMATION IS ONLY AS SECURE AS ITS LEAST PROTECTED CONTEXT.

C. Principle of Least Privilege

The term "principle of least privilege" is used to indicate that access privileges to sensitive information resources may be granted only to staff members on a "need to know" basis, and that the level of access granted to each staff member is limited to those privileges necessary for the account holder to perform his or her job function.

D. Separation of Duties

The term "separation of duties" refers to a principle of assigning job functions in a manner that provides procedural checks and balances that reduce the risk of any one individual using his or her access privileges to compromise UHCL information resources without detection. Common implementations of the separation of duties principle include:

- The transactions entered by one authorized individual must be monitored by another individual, or
- The entry of certain transactions may require the involvement of two or more individuals.

VI. Information Security Roles and Responsibilities

To be effective, a comprehensive Information Security Program must involve a number of individuals serving in specific roles. The following sections describe the information security-related roles and responsibilities that have been defined by the Texas Department of Information Resources (DIR) for all state agencies.

A. Information Resource Manager

The Information Resource Manager is designated by UHCL's President to have the ultimate responsibility of protecting UHCL information resources. As defined by the State of Texas, the Information Resource Manager is responsible for the following activities as delegated by the President:

- Ensuring that effective controls are in place,
- Reviewing and approving information ownership,
- Designating an Information Security Officer,
- Approving the information security program,
- Identifying an independent party to review the information security program for effectiveness and compliance with appropriate laws,
- Authorizing risk management decisions to accept exposure or protect data,
- Approving UHCL's Disaster Recovery/Business Continuity Plan, and
- Ensuring that appropriate funding is available to implement necessary information security controls.

At the University of Houston-Clear Lake, the role of Information Resource Manager is held by the Executive Director of University Computing and Telecommunications (UCT).

B. Information Security Officer

The Information Security Officer reports to the Information Resource Manager and is responsible for administering the information security program to ensure that the information either created by or entrusted to UHCL, wherever it is located, is protected in a manner that is commensurate with the information's confidentiality, integrity and availability requirements. To this end, the Information Security Officer must maintain up-to-date knowledge of security vulnerabilities, threats and countermeasures by taking advantage of professional development opportunities and collaborating with information security-related organizations that alert participants of current activity.

Additionally, the Information Security Officer must collaborate with and support all members of the UHCL faculty, staff, student body, and other affiliates in their efforts to protect UHCL information resources by:

- Developing, documenting and maintaining an up-to-date information security program that is appropriately funded and is approved by the Information Resource Manager,
- Developing and recommending information security-related policies to the appropriate Shared Governance Committee for review and approval,
- Working with Information Owners and Information Custodians to establish procedures that protect UHCL information resources against unauthorized or accidental disclosure, modification or destruction,
- Monitoring the effectiveness of defined controls,
- Reporting, at least annually, to the President or designee, the status and effectiveness of security controls in place,
- Working with Information Owners to conduct annual risk assessments and submitting a security risk management plan based on the assessment to the President or designee for approval,
- Working with Information Owners and Information Custodians to develop effective technological and procedural strategies for identifying and addressing information risk, and for complying with information security-related legal and contractual obligations,
- Implementing and managing an effective information security awareness and training program for faculty, staff, students and other members of the UHCL community,
- Evaluating the security of proposed departmental and enterprise-wide solutions, and providing effective, business-sensitive alternatives where necessary,
- Coordinating University-wide Information Security Program efforts,
- Managing cross-functional security projects,

- Monitoring compliance with UHCL's information security-related policies and its legal and contractual obligations,
- Ensuring that any identified weaknesses in UHCL's information defenses are promptly and appropriately remediated,
- 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, and
- Coordinating the response to information security-related incidents, red flag alerts and copyright infringement claims as described in the document entitled **Incident Response Policy and Procedures (ISPOL03)**.

C. Information Privacy Officer and Privacy Coordinator

The University's Information Privacy Officer (IPO) is an individual charged with developing the University's privacy policy that explains how the organization handles and protects any personal customer, client, or employee information gathered in its operations. This requires the IPO to maintain a comprehensive and current knowledge of both institutional operations and privacy laws and to work with Information Owners, the Information Security Office and the Office of Communications to ensure that the policy is consistent with the UHCL's objectives. At UHCL, the IPO function described above is performed by the University of Houston System's Office of the General Counsel.

The University of Houston's System Administrative Memorandum **SAM 01.D.06 – Protection of Confidential Information** describes privacy objectives shared by all UH component campuses.

The Privacy Coordinator is tasked with implementing the privacy policy developed by the IPO and ensuring that the details of the organization's privacy policies are effectively communicated to the users of UHCL information resources and to any of the University's constituents who are affected by the policy. Additionally the Privacy Coordinator is expected to work with University Communications in addressing any media and other external inquiries about privacy-related matters.

At UHCL, the Privacy Coordinator role is performed by the University's Information Security Officer.

D. Information Owners and Designees

The UHCL Information Security Program is risk-based, i.e., decisions regarding the types of security controls that are deployed are driven by the risk posed to the University should the confidentiality, integrity, and availability of the information resource be compromised.

For each UHCL information resource, an "Information Owner" must be assigned, an individual who is primarily 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 also may be responsible for other resources including personnel, equipment, and information technology that support their business function. The head of a respective department may be the information owner, and ownership may be shared by managers of different departments.

A list of University's information resources and their associated Information Owners and Designees is maintained by the University's Information Security Officer. This list can be found in the Information Security web site at *(Link TBD)*.

For each of his or her assigned information resources, the Information Owner or Designee is required to:

- Determine the resource's value and its criticality in the manner described by the University of Houston's System Advisory Memo, **SAM 07.A.08 Data Classification and Protection**,
- Assign custody of the resources and provide appropriate authority to implement security controls and procedures,
- Specify data control requirements and convey them to users and custodians,
- Review and authorize access to the resource,
- Specify appropriate control requirements, based on annual risk assessment, to protect resource against unauthorized modification, deletion, or disclosure. These control requirements extend to information resources and services outsourced by the University;
- Confirm that controls are in place to ensure the security of resource.
- Ensure that an effective backup and recovery plan is developed and implemented by each Information Custodian handling the resource.
- Approve, justify, document, and be accountable for exceptions to security controls submitted to and approved by the University's Information Security Officer.
- Perform annual risk assessments in collaboration with the University's Information Security Officer.

It should be noted that it is common for Information Owners to designate day-to-day ownership responsibilities for an information resource to a departmental staff member who may specialize in that

area. Nonetheless, it is important to note the Information Owner is ultimately responsible for all data classification and risk analysis decisions made relating to his or her assigned information resources.

Procedural guidance for the information security-related policies that relate to Information Custodians can be found in the **Procedural Handbook for Information Owners and Designees (ISPHB03)**.

E. Information Custodians

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

An Information Custodian is anyone, employee or contractor, who provides and/or supports the technology and services that users need to achieve UHCL's goals and objectives. The contexts managed by Information Custodians include data centers, servers, workstations, databases, applications, networks, and others.

Each Information Custodian must deploy, maintain, and operate an effective combination of technology controls to keep UHCL information resources safe.

While this role does not require each Information Custodian to understand the business purpose of each UHCL information resource to which he or she is entrusted, he or she must understand the risk level associated with each of those resources by communicating regularly with the appropriate Information Owner(s) and/or Designee(s).

These information contexts may be managed by members of the University Computing and Telecommunications (UCT) department, staff members in departments that support their own systems, or the staff of a vendor to which the University has outsourced its support. Regardless of the support model, all Information Custodians are responsible for the following:

- Providing physical, technical, and procedural safeguards for UHCL information resources in accordance with University policies,
- Implementing controls that meet the security requirements specified by the Information Owner,
- 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,
- Assisting Information Owners and Designees in evaluating the cost-effectiveness of controls and monitoring, and
- Implementing monitoring techniques and procedures for detecting, reporting, and investigating

security incidents.

Procedural guidance for all of the above information security-related policies that relate to Information Custodians can be found in the **Procedural Handbook for Information Custodians (ISPHB04)**.

F. Users

A user is an individual authorized to access an information resource in accordance with information owner-defined controls and access rules. Virtually all UHCL faculty, staff and contractors are users, i.e., their daily work requires that they create, capture, store, retrieve, modify, delete, process, transmit, administer, and/or manage University information across one or more contexts.

Each user is required to establish and maintain a dialog, either directly or through his or her supervisor, with the appropriate Information Owner(s) and/or Designee(s) to understand the security requirements for the UHCL information resources to which he or she has access.

All users must read, understand, and agree to comply with the policies contained in the **Acceptable Use Policy for UHCL Information and Systems (ISPOL02)** document that includes:

- Using UHCL information resources only for defined purposes
- Complying with established controls for protecting UHCL information resources and applicable University of Houston System Administrative Memoranda (SAMs), e.g.,
  - **SAM 07.A.08, Data Classification and Protection** and
  - **SAM 01.D.06 - Protection of Confidential Information**
- Taking an active role in protecting UHCL information resources.

Procedural guidance for the information security-related policies that are applicable to all UHCL employees and contractors can be found in the **Procedural Handbook for Employees and Contractors (ISPHB01)**.

G. Line Managers and Supervisors

The terms line manager and supervisor refer to any individual who manages UHCL employees or contractors who have access to any UHCL information resource.

In addition to understanding the information security requirements of the user role, individuals who manage UHCL employees and contractors are responsible for ensuring that:

- Job functions are defined clearly to ensure that required background checks are performed as part of the hiring process where necessary,
- Access privileges that are requested for staff members adhere to the "principle of least privilege", as described in the "Definitions" section of this document,
- "Separation of duties", as described in the "Definitions" section of this document, is properly enforced among staff members,
- Their staff members have taken information security awareness training and understand their role in protecting the UHCL information resources used by the department, and
- Their staff members are aware of the risks associated with the UHCL information resources that they are authorized to access.

Procedural guidance for the information security-related policies that relate to line managers and supervisors can be found in the **Procedural Handbook for Line Managers and Supervisors (ISPHB02)**.

VII. Program Policies

Line managers and supervisors are responsible for ensuring that the operation of their department or team effectively supports the Information Security Program. Thus, each line manager and supervisor must manage his or her team (employees and contractors) in a manner consistent with the following policies.

A. Classification of University Information

Data classification is the act of assigning a sensitivity/risk level to an information resource based upon its requirement for confidentiality, integrity, and availability.

To ensure that each UHCL information resource is protected appropriately, the resource must be classified, and measures must be taken to ensure that everyone who is authorized to access the resource is aware of its sensitivity level, and the actions that must be taken to secure it.

The University of Houston System has defined for all of its component campuses three sensitivity levels from Level 1 data (most sensitive) to Level 3 data (least sensitive). Details regarding the classification process and the three sensitivity levels can be found in the University of Houston's System Administrative Memorandum, entitled **SAM 07.A.08 Data Classification and Protection**.

B. Identity and Access Management

01. Accountability and Account Management

All information gathered and maintained by UHCL for the purpose of conducting University business is considered institutional information. Any individual who creates, captures, stores, retrieves, modifies, deletes, processes, transmits, administers, and/or manages any UHCL information resource is responsible and held accountable for its use.

UHCL information resources may only be accessed by individuals who have been authorized to do so by the appropriate Information Owner(s) and/or Designee(s). To this end, each user must be assigned a uniquely-named computer account that may be used only by the individual to which it has been assigned and that must be used whenever that individual accesses any UHCL information resource to provide personal accountability for the activities performed.

The use of shared, group or departmental accounts requires the approval of the University's Information Security Officer.

If an account holder leaves the University his or her computer accounts and access privileges must be immediately disabled. When an account holder's job function changes, the access privileges associated with his or her account must be modified to be consistent with his or her new role.

Access privileges for each UHCL information resource must be reviewed by the appropriate Information Owner(s) and/or Designee(s) regularly to verify that each user has the appropriate level of access to that resource. Quarterly reviews are recommended.

---

02. Elevated Access Privileges

Accounts with elevated access privileges are those meeting any of the following criteria:

- They allow for system administration of an information resource
- They allow the user to create and control the access of others to an information resource
- They allow the user the ability to bypass implemented system controls

Accounts with elevated access privileges are intended to be used when performing the specific job functions for which the user has been authorized and only for official University business. UHCL strongly discourages the use of accounts with elevated access privileges for tasks that do not require such privileges, e.g., web browsing, e-mail, personal use, since such action increases the risk of compromise.

Obtaining elevated access privileges requires the proper business justification and must be authorized by the appropriate department head, the Information Owner of any resource to which the requestor will obtain elevated access, and the University's Information Security Officer.

Elevated privileges must be created with an expiration date when supported, and such privileges must be removed or disabled when work is complete. Accounts that require elevated privileges on an ongoing basis must be reviewed regularly by the appropriate Information Owner or Designee to determine if the privilege level is still required.

Users must be made aware of the specific elevated access privileges that have been granted to their accounts. Abuse of such privileges may result in disciplinary action.

---

03. Identification and Authentication

When accessing a UHCL information resource, each user must identify himself or herself with his or her assigned computer identifier except for situations where the risk analysis performed by the Information Owner demonstrates no need for individual user accountability.

Where required, the user's identity must be verified or "authenticated" before the user can access the resource. Authentication controls must be consistent with documented risk management decisions made by the Information Owner or Designee.

Enterprise authentication sources, i.e., domain accounts as opposed to accounts managed on the local device, should be used for authentication where possible. Departments developing or implementing software or applications requiring authentication must utilize UCT enterprise authentication services. Exceptions may be granted with business justification and the approval of the University's Information Security Officer.

When designing technology solutions, whether hosted on-site or in an off-campus data center, it is strongly recommended that users authenticate against UHCL's central authentication services rather than having them maintain a different set of credentials for the hosted system. However, under no circumstances shall any individual, department or work group send UHCL authentication credentials, i.e., a file of user identifiers and passwords or password hashes, to an externally hosted service without the approval of the Information Security Officer.

The use of two-factor authentication solutions, such as those using any combination of passwords/PINs, tokens, certificates or biometrics, is strongly encouraged, especially for administrator-level accounts and accounts with access to level 1 data as defined by **SAM 07.A.08 Data Classification and Protection**.

The authentication controls must at a minimum use a password that complies with UHCL's password standard, i.e.

- A password must be at least eight (8) characters in length
- Each password must include:
  - 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 (!, @, #, $, %, ^, &, (,), *)

Passwords must be changed regularly, at least every ninety (90) days and should not match any of the previous six passwords used for the account.

Password composition and expiration rules must be reviewed on an annual basis to ensure that the University complies with industry best practices.

04. Access Privilege Management

Access privileges must be assigned in a manner consistent with the "principle of least privilege," as described in the "Definitions" section of this document.

It is strongly recommended that access privileges to UHCL information resources be granted to job function-related account groups rather than assigning access privileges on an individual account basis.

Access to each UHCL information resource must be reviewed regularly by its Information Owner or Designee to verify that each user does not have access privileges beyond those required to perform his or her current job function.

05. Separation of Duties

When assigning responsibilities to his or her staff members, each line manager or supervisor must enforce "separation of duties", as described in the "Definitions" section of this document, i.e., any individual who performs privileged transactions against any UHCL information resource must not be responsible for monitoring his or her own activity. Additionally, transactions deemed as high risk should require the involvement of multiple individuals.

06. Termination of privileges

If an account holder leaves the University his or her access privileges must be immediately disabled, and ID cards, physical keys, etc. are immediately returned.

Whenever an account holder's job function changes, the account holder's access privileges must be re-evaluated and modified to be consistent with his or her new role.

C. Staff Awareness

All UHCL employees must participate in the University of Houston System's annual security awareness training to better understand information risk, actions that can mitigate that risk, and the UHCL's legal and contractual obligations regarding the security of UHCL information resources.

The annual training program includes the following topics:

- Awareness of the University's Information Security Program, information security policies and procedures, and their responsibilities to protect UHCL information resources against unauthorized disclosure, misuse, theft or destruction.
- An understanding of day-to-day procedures for handling sensitive data and applications, conducting security checks, and maintaining the confidentiality, integrity, and availability of UHCL information and systems.
- Logical access controls to UHCL information resources.
- Physical access controls to secured facilities, including escort policies.
- Proper handling of physical and information-related threats.

For each piece of University information to which he or she has access, each UHCL employee or contractor must be aware of and understand the sensitivity level that has been assigned by its Information Owner. This information may be provided directly from the appropriate Information Owner or Designee, or from the employee's line manager or supervisor.

To meet certain compliance requirements, additional security awareness training may be required.

D. Risk Assessments

The UHCL Information Security Program is risk-based, i.e., decisions regarding the types of security controls that are deployed are driven by the risk posed to the University if the confidentiality, integrity, and availability of the information resource is compromised.

To ensure the controls that UHCL has in place are effective against current threats, risk assessments must be performed annually by each Information Owner or his or her Designee in conjunction with the University's Information Security Officer to highlight any risks that may be associated with the UHCL information resources that they "own" so that the appropriate level of security controls may be applied.

E. Management of Technology

Each UHCL information resource stored on or passing through technology deployed at UHCL must be secured to a level appropriate for its value and the risk it poses to the University as defined by **SAM 07.A.08 – Data Classification and Protection** and by its Information Owner or Designee.

For security to be effective, each Information Owner and Designee must work together with University's Information Security Officer and Information Custodian throughout the system implementation/ development lifecycle from its earliest planning stages through implementation and ongoing operation.

With a complete understanding of the information risks involved, Information Custodians must apply controls in the manner prescribed in the following documents:

- **SAM 07.A.08 – Data Classification and Protection**
- **SAM 01-D-06 – Protection of Confidential Information**, and
- **Procedural Handbook for Information Custodians (ISPHB04)**.

F. Record Retention and the Elimination of Obsolete Data

Staff members must always ensure that University records are preserved in accordance with UHCL's record retention schedule. The schedule can be found at the following web site (ADD LINK).

Once data in any context has reached its retention limits and is deemed by its Information Owner or Designee as obsolete, the data must be destroyed in an appropriate manner that makes the information permanently inaccessible. This includes:

- The shredding of physical media, such as paper, microfilm, etc.,
- Physical destruction of removable media, such as DVDs, CDs and USB storage devices, and
- Electronic wiping of hard drives and solid state storage using software approved by the University's Information Security Officer.

G. Data Discovery and Access to Personal Files

On occasion, UHCL receives requests from the University of Houston System's Office of the General Counsel to provide the data that is stored either in an individual's e-mail mailbox, on his or her assigned personal computing device, or in his or her assigned file server space. Such data discovery requests may only be made by the Office of the General Counsel.

Additionally, there are occasions where a line manager or supervisor requires access to the e-mail or files of a staff member who:

- Has left the University,
- Is inaccessible for an extended period of time, or
- Is suspected of performing unauthorized activity.

In the latter case, no one may access another individual's UHCL mailbox unless he or she has obtained the approval of either:

- The account holder, or
- All of the following four individuals:
  - The account holder's supervisor,
  - The University's Information Security Officer,
  - The Head of the Human Resource Department, and
  - The Office of the General Counsel.

Any individual who requires access to the mailbox or stored data of another member of the UHCL community must submit a form contains standard language describing how the requestor must protect of the privacy of the account holder. The privacy language on any such form must be approved by the University of Houston System's Office of the General Counsel.

In addition to signing the form indicating that the requestor has read, understands and agrees to comply with the privacy terms, he or she must provide the following information:

- The reason for the request,
- The topics that are of interest,
- The type of data required, e.g., e-mail, files,
- The starting and ending date for any e-mail messages being requested.
  Note – for e-mail the ending date could be in the future.

Once the form has been approved and signed by all required parties, the appropriate support staff can configure the access controls to satisfy the request.

The University's Information Security Officer must maintain a file of all approved requests.

VIII. Program Planning and Maintenance

A. Program Planning and Maintenance

The University's Information Security Officer is required to develop an annual security plan that is shared with the University's Information Resource Manager and the President for their approval. This plan must be consistent with and support UHCL's mission, goals, and objectives at large, and must include the following:

- An evaluation of the University's current security posture,
- Proposed plans for addressing weaknesses in UHCL's information defenses,
- The cost of and justification for the proposed remediation efforts, and
- The progress that has been made toward the completion of the approved plans.

While informing UHCL's executive management on a regular basis is an ongoing activity, there should be a formal review and discussion of the information security program on an annual basis at the end of the spring semester.

The Information Security Office is responsible for estimating and monitoring all expenses associated with the implementation of the information security program.

However, because information security technology is often a component of a larger non-security-related solution, purchases of technology associated with the information security program plan will be made by the operating unit within whose realm the technology most appropriately resides. For example, the cost of security software that supplements a piece of networking hardware would be purchased from funds budgeted by the network support area of UCT.

B. Maintenance of the Policy and Procedure Library

Information Security Office's web site hosts the Information Security Program's policy and procedure documentation. To access these documents, please visit http://www.uhcl.edu/computing/information-security/policies.

01. Document Types

The Information Security Program Document Library contains five types of documents:

(Note – in the Doc Code column, "n" represents a numeric digit and "a" represents an alphabetic character.)

Doc Code	Document Class	Description
SAM *nn.a.nn*	University of Houston System Administrative Memorandum	A policy mandated across all UH System component campuses
ISPOL*nn*	UHCL developed policy	A set of definitions, roles, principles and directives established by an organization to define its goals, to protect its interests, and to direct and limit any related actions taken by its members. Policies must be approved by an appropriate Shared Governance Committee
ISPHB*nn*	UHCL procedural handbook	A generic description of tools, configuration settings, tasks, workflows, etc., that can implement UHCL's policies, either used "as is" or tailored for a specific department, work group or product.
ISPRC*nn*	UHCL detailed procedure	A set of detailed instructions for implementing a specific vendor product, such as Active Directory.
ISSTD*nn*	UHCL standard	Requirements, specifications, characteristics and, in some cases, specific products that can be used across an organization to fulfill a business need.
ISGDL*nn*	UHCL guideline	A recommended course of action that allows some discretion or leeway in its interpretation, implementation or use.

02. Current Catalogue and Target Audiences

Currently, the Information Security Program Documentation Library contains seven documents as listed below. This table also indicates each document's target audiences:

Document Name	Audience					
	Employees and Contractors	Managers and Supervisors	Information Owners and Designees	Information Custodians	Students	Visitors
Information Security Program Description, Roles and Program Policies (ISPOL01)	✔	✔	✔	✔		
Acceptable Use Policy for UHCL Information and Systems (ISPOL02)	✔	✔	✔	✔		
Incident Response Policy and Procedures (ISPOL03)	✔	✔	✔	✔		
Acceptable Use Policy for UHCL Public Computers and Networks (ISPOL04)					✔	✔
Procedural Handbook for All Employees and Contractors (ISPHB01)	✔	✔	✔	✔		
Procedural Handbook for Line Managers and Supervisors (ISPHB02)		✔				
Procedural Handbook for Information Owners and Designees (ISPHB03)			✔			
Procedural Handbook for Information Custodians (ISPHB04)				✔		

C. Policy Review Process

Once a year, each policy associated with the University's Information Security Program must be reviewed by a team comprised of individuals representing the constituencies for whom the policy is most relevant to ensure that it remains comprehensive, relevant and consistent with UHCL's mission, goals and objectives. To ensure that each policy is given an appropriate level of attention, the evaluations will be distributed throughout the year. The policy review schedule is presented in the following table:

Information Security Program Document Name	Review Due Date
Information Security Program Description, Roles and Program Policies (ISPOL01)	January 31
Acceptable Use Policy for UHCL Information and Systems (ISPOL02)	February 28
Incident Response Policy and Procedures (ISPOL03)	January 31
Acceptable Use Policy for UHCL Public Computers and Networks (ISPOL04)	February 28

Each policy review committee is chaired by the University's Information Security Officer who is responsible for:

- Keeping a record of the committee's policy-related discussions,
- Working with the University of Houston System's Office of the General Counsel to ensure that the policy content and language are appropriate,
- Incorporating all agreed upon modifications into the policy content, and
- Providing status information to the University's President and Information Resource Manager.

Additionally, once the policies are revised, the Information Security Officer will work with the appropriate target audiences to update the procedural handbooks as necessary.

IX. 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

X. Policy Review Responsibility

Responsible Parties:

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

Review Period:

- Annually on or before January 31

XI. Approval

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