University of Houston Clear Lake

Administrative Policies and Procedures

Information Security Program Procedural Handbook for Line Managers and Supervisors (ISPHB02)

Date Issued: November 17, 2016

Last Revision: October 1, 2018

Table of Contents

I. Purpose and Scope

Every individual who is member of the University of Houston-Clear Lake's (UHCL) faculty and staff, or is contracted to provide information-related services, is responsible for protecting the information created by or entrusted to UHCL to the best of his or her ability.

Line managers and supervisors play a key role in securing UHCL information resources against unauthorized disclosure, tampering, theft, and destruction. Besides being users of information themselves, they establish departmental and work group procedures to ensure that:

- Their teams are staffed with properly vetted individuals,
- The "principle of least privilege" and "separation of duties" are ingrained into their business procedures and practices,
- Access privileges are regularly reviewed to ensure that they remain appropriate, and
- Access privileges no longer needed are removed.

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 a supervisory role.

II. Applicability

Anyone who serves the University in a supervisory role should become familiar with the contents of this document. This document assumes that the reader has read and understands the definitions, roles and policies contained in the following documents:

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

All UHCL employees and contractors also should be familiar with the document entitled **Procedural Handbook for Employees and Contractors (ISPHB01)**.

III. Procedures

A. Personnel Management

To prevent hiring of applicants who do not meet employment eligibility criteria with respect to previous criminal activities or unethical conduct, data processing managers are to direct all applicants for employment to Human Resources if the specific job title requires a background investigation.

---

01. Applicant Screening

Background investigations are required for the following positions:

- Technology related positions:
  - Data Processing Management Positions
  - Systems Programmers
  - Data Base Administrators
  - Computer Operators
  - Technical Support Personnel
  - Programmers/Analysts
- Positions that involve exposure to:
  - Information that UHCL legally is obligated to protect, such as information protected by FERPA, HIPAA, GLBA, and other federal, state and local privacy laws,
  - Information that UHCL contractually is obligated to protect, such as information protected by the University's agreement with the Payment Card Industry (PCI) consortium, and
  - Non-public Information that is associated with the University's strategic direction and financial status.
- Other positions defined as requiring background checks in job descriptions submitted by Administrative and Academic department managers to the University's Human Resources department.

It is the responsibility of the appropriate line manager or supervisor to ensure that each person being hired, appointed or promoted complies with the requirement for a background investigation. A prospective hiree, appointee, or promotee who fails to cooperate in following this procedure must be considered unqualified.

An applicant's references should be checked for at least the past seven years.

Other applicant data, such as date-of-birth, citizenship, home residence, school credentials, and court and financial records, must be verified before a job offer is made.

A photograph must be taken as part of the personnel record.

Employees must sign agreements to cover:

- Ownership and royalty arrangements on business-related inventions by employees.
- Unauthorized disclosure and/or use of the University's commercial and in-house developed proprietary software and the University's information resources by individuals during employment and after they leave the organization.

---

02. Staff Security Awareness Training

Line managers and supervisors are expected to be strong advocates for the University's Information Security Program, and must ensure every employee and contractor on his or her staff understands:

- UHCL's interest in information security and the reasons for it.
- The University's information security policies and procedures applicable to his or her job function,
- His or her direct responsibilities in ensuring the security and integrity of UHCL information resources,
- Violations of these policies and procedures could be serious enough to lead to termination of employment.

---

03. Interaction with Information Owners and Designees

Line managers and supervisors must work with the Information Owner(s) and/or Designee(s) associated with the information that the department uses to understand the value of the information, the risk posed to the University if the information is exposed to unauthorized individuals, tampered with, or destroyed and the measures that need to be taken to protect the information at an appropriate level.

Line managers and supervisors are required to keep staff members informed of the information security requirements associated with the information that they process.

---

04. Separation of Duties

The University and all of its departments must enforce separation of duties and appropriate checks and balances in their daily operations to ensure that information is protected against intentional and accidental actions that put our information at risk. This involves the following:

- Operational and system development functions must be performed by different individuals from those who perform monitoring functions.
- Application software that is developed in-house may not be moved to the production systems by members of the application's development team. Rather, the application software must be moved by a "change manager", i.e., an individual not on the development team who is assigned to move software from development to production. That change manager could be a developer from another project team.
- In cases of a production emergency, a developer could move updated software to the production environment with the approval of the University's Information Security Officer. However, the software must go through the regular change management process as soon as the situation stabilizes.
- There should be cross training of operations staff to provide depth and backup, and to reduce individual dependence.
- Application developers must not be able to update or execute software in the production environment except in emergency situations approved by the University's Information Security Officer.
- Server managers should not be able to make changes to production application or system software libraries, to execute any jobs or programs that have not been scheduled through established procedures, or to execute (outside of standard production processing) data or software-modifying system utilities without proper authorization and dual control.

- Individuals whose job function involves the entry of financial and other forms of sensitive data into the University's systems should not prepare source documents for input or audit his or her own data-related activities.

---

05. Termination of Employment or Employee Reassignment

When an employee or contractor no longer serves in the same job function, either through reassignment or termination, it is the responsibility of the employee's or contractor's manager or supervisor to ensure that he or she no longer can access any UHCL information resources associated with his or her prior position.

- Line managers and supervisors must ensure that all identities and access privileges, both access to physical facilities and logical access to UHCL systems and information, for any employee who is leaving the University are revoked before he or she leaves the premises.

- Department heads should develop a formal employee exit interview process.

Note - UHCL would like to maintain a stable work force with a minimum level of staff losses. Facts and opinions stated during an exit interview may be of material value toward that objective.

- Departments should maintain a termination checklist to ensure that no access capabilities remain for the terminated employee.

- It is the responsibility of the line manager or supervisor to advise the departing employee that he or she cannot continue to use University of Houston-Clear Lake data processing facilities, data, or equipment.

- All UHCL property, including computer and communications equipment, keys, identification cards, programs, data, and documentation, must be returned to the terminating employee's manager or supervisor who is responsible for ensuring that each item is forwarded to its appropriate destination. A property issuance and return record should be created that includes issuance and return dates, and the authorized issuer's signature for each item specified. Typically, the record will include keys, identification cards, badges, passwords, etc. In special instances, computer and communications equipment also may have been issued to employees for use in off-site locations.

- Situations requiring the immediate revocation of access or processing authorization must be resolved directly with the University's Information Security Officer.

B. Vendor Management

The University's information security policies apply not only to UHCL employees and contractors in-house, but also to individuals who provide contracted services to the University externally. Thus, line managers, supervisors, and the individuals who negotiate contracts with the vendors must ensure that the contract terms are consistent with the University's policies and procedures and are vetted by the University of Houston's General Counsel.

This requires that line managers and supervisors who lead projects that use third-party services, either on- or off-campus, perform the following:

- When assembling contract terms, the line manager or supervisor must involve the University's Information Security Officer early in the project to ensure that the contract terms meet or exceed UHCL's policy requirements. The University's Information Security will work with the University of Houston System's Chief Information Security Officer and the Office of the General Counsel to ensure that the contract terms effectively protect UHCL's interests.

- For contractors who will be working on-site with University supplied computers, the primary focus must be the vendor's personnel practices which must be consistent with those specified for UHCL employees.

- For cases in which UHCL information resources will be hosted at an off-campus vendor site, the contract must specify:

    - The sensitivity of the information involved,

    - UHCL's information security expectations for the vendor's operating environment, any third parties involved in processing the data, and any data transmissions among UHCL and any of the external parties involved,

    - How data will be handled and/or destroyed if or when the agreement is terminated,

    - A mechanism for assuring compliance.

    Note - It is strongly recommended that the vendor's practices are subject to annual audits against universally accepted standard frameworks, such as ISO 27001, SSAE16, COBIT, and that UHCL is provided with the executive summary to ensure that each vendor is in compliance.

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