University of Houston Clear Lake

Administrative Policy and Procedure Library

Information Security Program Acceptable Use Policy for UHCL Information and Systems (ISPOL02)

Date Issued: November 17, 2016

Last Revision: October 2, 2018

Table of Contents

I. Purpose and Scope 1

II. Applicability 1

III. Policy 2

A. Restrictions on the Use of UHCL Information and Systems 2

01. UHCL Information and Systems must Fully Support the University's Mission 2

02. Incidental Personal Use of UHCL Technology 2

03. Activities Deemed as Inappropriate 3

B. Personal Accountability 4

C. Expectation of Privacy 4

D. Prerequisites for Network Access 5

E. Security Awareness and Training 5

F. Information Sensitivity Awareness 5

G. Providing Information to Others 6

H. Protection of University Information "at Rest" and "in Transit" 6

I. Incident Reporting 8

J. Implementation of New Technology Products and Services 8

IV. Revision Log 9

V. Policy Review Responsibility 9

VI. Approval 9

I. Purpose and Scope

Academic and administrative information resources, either created by or entrusted to the University of Houston-Clear Lake (UHCL), are vital 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 describes how all members of the UHCL community are expected to use UHCL information resources, to set privacy expectations and under what conditions the use of personally-owned computing devices are permitted on the UHCL network.

II. Applicability

Every user of UHCL information resources is required to read, understand, and agree to comply with the policies contained in this document.

This document assumes the reader is familiar with the content of **Information Security Program Description, Roles and Program Policies (ISPOL01)**.

Procedures associated with the policies contained in this document can be found in the document entitled **Procedural Handbook for Employees and Contractors (ISPHB01)**.

III. Policy

A. Restrictions on the Use of UHCL Information and Systems

01. UHCL Information and Systems must Fully Support the University's Mission

UHCL's information resources, computing devices and networks are valuable and unique resources that are intended to be used by authorized users engaged in educational or research pursuits, and in the administrative activities that support the University's academic mission. Unauthorized use is prohibited and subject to Federal, state, civil, and criminal laws.

To ensure that quality, equitable, and cost effective information resources are effectively provided to the educational community, they must be regarded as shared resources by all users who must cooperate as a diverse community with common purposes.

Therefore, it is imperative that users conduct themselves in a responsible, ethical, and polite manner while using these resources. In accordance with the policies of the Texas Department of Information Resources, the University of Houston System, and UHCL, all users are expected to abide by the policies in this document as an Automated Information Systems Agreement of Understanding.

---

02. Incidental Personal Use of UHCL Technology

Incidental personal use of a UHCL computer by a UHCL employee is permitted as long as the activities performed:

- Do not interfere with the performance of his or her professional duties,
- Are of reasonable duration and frequency,
- Do not overburden the system or create additional expense for the University, and
- Comply with all applicable UHCL policies.

E-mail use must be consistent with the policies defined in the following University of Houston's System Administrative Memoranda: **SAM 07.A.07 - Use of Electronic Messaging Services by Employees** and **SAM 07.A.06 – E-mail Retention**.

---

03. Activities Deemed as Inappropriate

The following activities are considered highly inappropriate. As such, performing any of the following activities using a UHCL computing device or the UHCL network may result in disciplinary action up to and including separation of employment, termination of contract, and/or civil or criminal penalties:

- Creating, reproducing, accessing, forwarding, or sharing information in any form that:
  - UHCL is required to protect by law, contract or policy,
  - Violates a federal, state or local law, a software license agreement, or copyright;

    *Note - The policy and procedures related to specific copyright issues defined by the Digital Millennium Copyright Act (DMCA) can be found in the University of Houston's System Administrative Memorandum entitled **SAM 07.A.04 - Digital Millennium Copyright Act**.*
  - May be deemed as discriminatory or offensive to individuals based upon their race, religion, nationality, color, gender, sexual preference, or disability,
  - Is perceived as harassment toward any individual, group, or organization,
  - Serves any commercial purpose including product advertising material,
  - Is related to any form of political lobbying, or
  - Is considered unprofessional or disrespectful;
- Performing any activity that:
  - Involves the intentional running of any software or perform any procedure designed to "hack" into any computing or network device,
  - Damages the integrity of the data or programs stored on any computer or network device,
  - Initiates or continues to proliferate e-mail SPAM, or
  - Disrupts or degrades network resources with the exception of planned vulnerability testing managed by the University's Information Security Officer;
- Using any UHCL-owned or leased computing device and/or the UHCL network, to communicate with individuals who may have compromised a system, with the hope of restoring altered, encrypted, or otherwise destroyed data; or
- Posting messages to social media, chat rooms, mailing lists, and similar services under the identity of an account that UHCL obtained from an external service provider without prior authorization from management.

B. Personal Accountability

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 University information is responsible and held accountable for its use.

UHCL assigns each user a unique computer account that must be used when accessing any UHCL information resource to provide personal accountability for all activities performed. This account may not be shared with anyone else, either within the UHCL community or without.

Each user is expected to create a strong, difficult-to-guess password for his or her computer account to protect it against being used by any other individual or system. Tips for creating strong passwords may be found in Section III-B-04 of the **Procedural Handbook for Employees and Contractors (ISPHB01)**.

To ensure that a computer account is not used by an unauthorized passerby, each user must log off or lock any computer or mobile device that he or she uses to conduct University business when leaving it unattended.

C. Expectation of Privacy

All technology owned or leased by UHCL is intended to be used to conduct University business, and any information held therein is the property of the UHCL. While this policy allows for incidental personal use, there should be no expectation of privacy except as otherwise provided by applicable privacy laws. Thus,

- Computer usage may be subject to security testing and monitoring, and
- Misuse is subject to criminal prosecution.

While there is no expectation of privacy, UHCL, as a courtesy, does not permit anyone to access another individual's files that are stored on his or her University-assigned computer, network folder, or e-mail mailbox without a valid business or legal justification, and the approval of:

- The target person's supervisor,
- The Head of the Human Resources Department,
- The University's Information Security Officer, and
- The Office of the General Counsel.

D. Prerequisites for Network Access

No computing device may be installed on the UHCL wired or authenticated wireless network unless the device complies with the requirements outlined in the **Procedural Handbook for Employees and Contractors (ISPHB01)**.

Whenever any computer incident advisory or other security alert is received regarding a device on any UHCL-managed network, that device will be removed from the network and may not be returned to network service until it has been reimaged.

Manually "cleaning" an infected device without reimaging is strongly discouraged. Returning a manually cleaned device to the network requires the approval of the University's Information Security Officer.

E. Security Awareness and Training

All UHCL employees are required to take and pass an information security training course that meets the criteria established in the Texas Administrative Code, Title 1 (TAC202), the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA).

F. Information Sensitivity Awareness

Anyone with access to UHCL information resources must protect those resources in a manner that is commensurate with its sensitivity. As such, he or she must take the actions necessary to understand the value of the information to which he or she has been granted access, and the risks to the University if the information is disclosed to unauthorized individuals, tampered with, or destroyed. The value and risk associated with each UHCL information resource is obtained from two sources:

- The University of Houston System Administrative Memorandum **SAM 07.A.08 – Data Classification and Protection** defines three sensitivity/risk levels from level 1 (highly sensitive) to level 3 (public) and describes how data elements are classified. It also highlights specific data elements that are protected by law.

- The sensitivity/risk level of data elements that are not specifically named in the above SAM must be obtained from the appropriate Information Owner(s) and/or Designee(s).

Anyone who is unsure of a data element's sensitivity/risk level must assume that it is level 1 until the appropriate level is ascertained.

G. Providing Information to Others

UHCL level 1 or level 2 information resources, as defined in **SAM 07.A.08 – Data Classification and Protection**, may be shared only with individuals who have been authorized to access those resources by the appropriate Information Owner(s) and/or Designee(s).

Anyone who receives a subpoena requesting any UHCL information must forward it to the University of Houston System's Office of the General Counsel immediately.

H. Protection of University Information "at Rest" and "in Transit"

With the understanding of sensitivity/risk level of the information that he or she is authorized to access, every member of the UHCL community must take specific actions to ensure that the information to which he or she has access is protected appropriately, both when stored on computing devices, electronic storage media or physical documents (data at rest), or when transmitted across wired and wireless networks, e-mail, FAX, etc. (data in transit).

University of Houston system-wide restrictions are described in the following System Administrative Memoranda (SAM):

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

In addition to the above SAMs, UHCL requires the following:

- Any computer, tablet, smartphone, or other computing device that is used to create, access or exchange any University information, including e-mail, must be configured and operated in a manner that is consistent with the requirements outlined in **Section III-C** in the document entitled **Procedural Handbook for Employees and Contractors (ISPHB01)**.
- Only UHCL-owned or leased computing devices may be used to create or access level 1 (highly sensitive) data, as defined by **SAM 07.A.08 – Data Classification and Protection**.
- Personally owned computing devices may not be used to create or access level 2 (sensitive) University information without the approval of the appropriate Information Owner(s) and/or Designee(s) and the Information Security Officer.
- Hard copy reports, forms, and other documents that contain level 1 or level 2 data must be secured in a locked filing cabinet or other container when not in use.
- The exchange level 1 or level 2 data is only permitted with the approval of the appropriate Information Owner(s) and/or Designee(s), and only on the following networks:

  - The UHCL wired network,
  - The UHCL authenticated wireless network,
  - A network that is secured with UHCL's VPN technology or another secure communication method that is approved by the University's Information Security Officer.

- Electronic mail must not be used to exchange level 1 or level 2 data unless the e-mail message is encrypted end-to-end, from sender to recipient.
- No level 1 or level 2 data may be stored in an application or a file sharing facility hosted in the "cloud" without the approval of:
  - The appropriate Information Owner(s) and/or Designee(s),
  - The University's Information Security Officer and the University of Houston System's Chief Information Security Officer,
  - The University of Houston System's Contracts Administration Department, and
  - The University of Houston System's Office of the General Counsel.
- Before discarding or repurposing any computer, tablet, smartphone, or other computing device that has been used to create or access level 1 or level 2 information, the device's internal drive must be electronically wiped and/or physically destroyed to ensure that any remnants of University data cannot be gleaned from the device.
- Any other piece of removable media (e.g., DVDs, CDs, USB tokens) that has been used to store University data must be physically destroyed before being discarded.
- Any piece of erasable, removable media (e.g., USB tokens) that has been used to store University data must be electronically wiped before being repurposed.
- In all of the above cases, the mechanism used to electronically wipe the data must be approved by the University's Information Security Officer.
- Before discarding any report, form, or other document on physical media, such as paper, microfilm, etc., that contains level 1 or level 2 data, it must be shredded. All documents awaiting shredding must be physically secured in a locked container. Both the shredding method and container must be approved by the University's Information Security Officer.

I. Incident Reporting

It is critical that appropriate authorities are involved as soon as possible when an incident involving a UHCL information resource is suspected. Such incidents include, but are not limited to the following circumstances:

- A UHCL-owned or leased computer, tablet, smartphone, or other computing device, or a personally-owned device that has been used to create or access University information, has been lost or stolen, or is exhibiting behaviors that suggest the device has been compromised.
- The following is observed or suspected:
  - The unauthorized access or modification of a UHCL information resource, computer system, program, network, or piece of networking equipment,
  - The theft or diversion of University funds, computational resources, or other assets,
  - Potential criminal activity, or conflict of interest, or
  - Vandalism or other damage to computer systems, computer programs or data.

Anyone who has been made aware of any such incident must report it immediately, following the procedure described in the document entitled **Incident Response Policy and Procedures (ISPOL03)**. Failure to do so can result in disciplinary action.

J. Implementation of New Technology Products and Services

All University-funded purchases of new computer hardware, software, and services must be reviewed and approved by the University's Information Security Officer. It is strongly recommended that the security review of any proposed solution be performed early in the product selection process to avoid project delays.

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. Policy Review Responsibility

Responsible Parties:

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

Review Period:

- Annually on or before February 28

VI. Approval

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