University of Houston Clear Lake

Administrative Policies and Procedures

Information Security Program Procedural Handbook for Employees and Contractors (ISPHB01)

Date Issued: November 17, 2016

Last Revision: October 1, 2018

Table of Contents

I. Purpose and Scope

Every member of the University of Houston-Clear Lake's (UHCL) faculty and staff, and those contracted to provide information-related services shares the responsibility of protecting the information that has been created by or entrusted to UHCL to the best of his or her ability.

Effectively securing UHCL information resources against unauthorized disclosure, tampering, and destruction requires the active participation of every member of the UHCL campus community that is comprehensive and consistent across the campus.

To this end, UHCL has developed an Information Security Program that includes a set of policies that serve as the foundational principles upon which the program is built, and a set of procedural handbooks that provide a comprehensive set of generic, non-vendor-product specific 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.

II. Applicability

This handbook provides procedural guidance that specifically focuses on the daily procedures that are relevant to every user regardless of role or position, so everyone who has access to UHCL information resources should become familiar with its contents.

This document assumes that the reader has read and understands the content of the following documents:

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

III. Procedures

*Note – The data classification levels referred to in this document are described in-depth in the University of Houston's System Administrative Memorandum **SAM 07.A.08 Data Classification and Protection**.*

A. Physically Securing Work Space and Media

Every UHCL employee and contractor is responsible for ensuring that his or her physical workspace is adequately protected so that the security UHCL information resources is not compromised. To this end, actions must be taken to ensure that information held on computing devices and physical media in his or her work space is protected against unauthorized disclosure, tampering, and destruction. Physical media includes but is not limited to printed reports and information stored on removable storage devices, such as DVDs, CDs, and USB tokens.

Protective Measures

- Floor space must be protected to ensure that it is accessible only to authorized individuals.
- Every UHCL employee and contractor expected to understand of the value and risk associated with each UHCL information resource that they access. This knowledge may be obtained from the employee's or contractor's supervisor or by contacting the appropriate Information Owner(s) and/or or Designee(s). Until the information's value and risk is known, it must be assumed that the information is confidential and may not be shared.
- Physical media carrying confidential information must be stored in a locked, tamper and theft resistant container, e.g., a locked drawer, filing cabinet, office, when not in use. Only those who are authorized to access the secured information may have the key to the secured container.
- While reviewing confidential or highly confidential information, measures to prevent unauthorized individuals nearby from viewing that information.
- Physical reports and documents that carry level 1 (highly sensitive) or level 2 (sensitive) information must be shredded before discarding them.
- Any piece of optical media that has been used to store any UHCL level 1 or level 2 information resource must be shredded or otherwise physically destroyed before being discarded.
- Any computer hard drive, solid state drive or other piece of electronic or magnetic media that is being discarded, donated, or repurposed must be wiped using a disk wiping product that has been approved by the University's Information Security Officer. If the media is not being

reused, it must be physically destroyed. The UCT Support Center and Technical Services provide a service to wipe and/or destroy computer hard drives for UHCL equipment that is being discarded or repurposed.

- Data wiping requirements also apply to vendors who may manage equipment used to store or process University data, such as copiers. Contracts with such vendors must include appropriate data wiping procedures.

B. Securing Computers, Tablets, Smartphones, and Other End-User Computing Devices

Every UHCL employee and contractor is responsible for ensuring that his or her computer, tablet, smartphone, or other end-user computing device used to conduct University business does not become a vehicle through which information can be disclosed to unauthorized individuals, altered, or destroyed. To this end, this section is intended to provide the members of the UHCL community with specific actions necessary to strengthen their personal computing environment.

For computing devices that UHCL purchases for use by a UHCL employee or contractor, many of the parameters that are discussed in this section typically are set by the individual's UCT Technical Services representative or his or her departmental technical support person who configures the device.

However, any UHCL employee or contractor who fully or partially administers his or her computing device assumes full responsibility for ensuring that the actions described in this section are carried out to their fullest extent.

01. Properly Configuring Computing Devices

Any device, i.e., computer, tablet, smartphone, or any other computing device that is used to perform University business must be configured in a manner that reduces the risk of UHCL information resources being compromised. When a computing device is initially taken out of the box, there are a number of configuration parameters that must be set, each having some impact in the security of the device.

To ensure that each computing device's security controls and set appropriately, the following actions must be taken:

- The standard "guest" account on any system must be disabled on all systems.

- Where possible, the standard "administrator" account on any system or application should be renamed from its initial default value or it should be disabled and replaced with an account with a different name.

- The standard "guest" and "administrator" accounts' initial default password must be changed as soon as possible after the system is installed.

- On systems where administrative privileges cannot be assigned to individual user accounts, access to the system's standard administrator account must be controlled through a secured, password "lock box" that can be maintained physically, e.g., in a sealed envelope in a secured container, or electronically using "password safe" software that is approved by the Information Security Officer.

- Password composition rules must require the use of a password that is a minimum of eight characters in length and, where possible, include a mix of at least three of the four character types (e.g., upper-case and lower-case alpha, numbers, and symbols).

- Password rules should disable accounts after ten (10) unsuccessful login attempts. The account can be automatically reactivated after fifteen (15) minutes.

- It is strongly recommended that users do their daily work using an account that has user-level privileges, so user accounts should not be added to in the "Administrators" group on the system without the approval of the University's Information Security Officer.

- Level 1 (highly sensitive) information must never be e-mailed unless the contents are encrypted from sender to recipient using an encryption mechanism approved by the University's Information Security Officer.

- Any individual whose role at the University requires the e-mailing of level 2 (sensitive/internal) business information to external entities, should create an e-mail signature line containing the following disclaimer that is appended to each of those messages:

> *The above message may contain confidential information. If you think you have received this message in error, please do not copy or distribute the message, or take any action based upon its content. Further, we ask that you notify us immediately by return e-mail.*

02. Updating Software in a Timely Manner

Malicious individuals can introduce malicious software (malware) into a computing device through system flaws or vulnerabilities in the software that has been installed. Like viruses, the malware they introduce through the software flaw can expose, tamper with, or destroy information resources, can use targeted computers to attack other systems, and can even destroy the computer hardware itself.

To prevent computer hackers from disclosing, altering, or destroying any UHCL information resources or from disrupting UHCL computer services by exploiting vulnerabilities in any piece of installed software, every UHCL employee and contractor is responsible for the following:

- Software updates that are security-related and are considered "critical" or "important" by the vendor must be installed on all computers, tablets, smartphones and other computing devices used to access any UHCL information resource within two weeks of their release.

- For UCT-managed software, the updates are scheduled by UCT's Technical Services. For any software installed on a device that is not managed by UCT, the user is responsible for ensuring that the software is updated within the above parameters.

---

03. Preventing Computer Viruses and Other Malware

By passing a computer virus or other piece of malicious software (malware) to a computing device, a malicious hacker could have the computer perform unauthorized activities without him or her having had any physical access to the device. These activities include but are not limited to automatically accessing and sending confidential information to an external destination, overloading the computer network, attacking other computers, destroying information stored on the device's local, and network-based drives, or even rendering the computer unusable.

Because computer viruses and other forms of malware spread through the sharing of files with other "infected" computers, extreme care must be taken when exchanging files with other individuals, especially those outside the University, via e-mail, Internet web site access, and the exchange of DVDs, USB storage tokens and other portable, electronic media.

The following requirements are intended to prevent computer hackers from disclosing, altering, or destroying UHCL computer-based information and from disrupting UHCL computer service through the spread of computer viruses and/or any other form of malicious software:

- Any computing device that is owned by UHCL or is used to access any UHCL information resource must have anti-virus software installed where such software exists for the technology.

- The anti-virus software that is installed must be configured to:
  - Ensure that the anti-virus software's virus definitions are kept up-to-date on at least a daily basis
  - Actively check software, documents, and files for viruses and other forms of malware whenever the file is opened, and
  - Check all files stored on the device for viruses in a batch mode at least once per week.
- None of the above configuration options may be turned off except under circumstances approved by the University's Information Security Officer.
- In addition to ensuring that anti-virus software is installed and is active on computing devices, every UHCL employee and contractor is expected to avoid performing activities that are known to introduce and/or spread computer viruses and other malware, such as:
  - Not introducing a CD-ROM, DVD, USB storage device of other portable storage device into his or her computing device unless it have been scanned with the most up-to-date anti-virus software.
  - Not opening any e-mail attachment unless he or she knows:
    - Who sent the e-mail,
    - Why the link or attachment has been delivered,
    - What attachment contains, and
    - The attachment is associated with a UHCL business purpose.
  - Avoiding questionable or suspicious web sites and do not click any links on a web site unless he or she is reasonably certain that the link is legitimate.
  - Not opening any file obtained from an outside source without scanning it for viruses and other malware.

04. Maintaining Effective Passwords

Once a system is configured, passwords are the first line of defense in protecting computing devices. When simple easy-to-guess passwords are used, unauthorized individuals can gain access to sensitive information resources without a great deal of effort. Over the past few years, malicious "hackers" have developed automated password-cracking techniques that have enabled virtually anyone to crack a weak password in minutes.

To ensure that the passwords used by UHCL employees and contractors are strong enough to effectively block unauthorized individuals from accessing any UHCL information resource, the following actions must be taken:

Password Construction

- Passwords must be a minimum of eight characters in length.
- Password must be a minimum of eight characters in length and, where possible, include a mix of at least three of the four character types (e.g., upper-case and lower-case alpha, numbers, and symbols).
- The following are passwords that are easy to crack and **must be avoided:**
  (Note – This list is not exhaustive)
  - A blank password,
  - A password set to its vendor-provided, initial default value,
  - A password equal its corresponding user ID,
  - A password that is a variation of the word "password", e.g., "Password", "passwd", "PassWord", "p@ssw0rd",
  - A password that is set to an obvious sequence, e.g., "12345678", "abcdefgh", "abcd1234", "qwerty",
  - A password that is set to any single word in any dictionary in any language,
  - Any person's name in any language,
  - Any date by itself,
  - Team nicknames or cheers, e.g., "Go Hawks!",
  - A password that is set to a well-known phrase, e.g., "to be or not to be",

- Any of the above with a number of symbol added to the end, and
- Any of the above repeated multiple times or backwards.

Tip for Creating an Easy-to-Remember, Strong Password

Start with a phrase that is easy to remember and use a single character for each word, e.g., the phrase "I am one happy camper at UHCL!" could become the password "Im1hc@UHCL!"

(Note – Please do not use any of the above passwords or any password that is shared in a document as an example. A hacker who has access to this document most certainly would try it to break into the UHCL's systems.)

Password Practices

Passwords must be changed at least once every 120 days at a minimum, even on systems that do not force password changes.

When changing passwords, none of the previous six passwords may be used.

Passwords should not be shared with anyone else under normal circumstances. Anyone who has a compelling business reason for allowing multiple individuals to share login credentials should contact the University's Information Security Officer for assistance through the UCT Support Center at supportcenter@uhcl.edu or via phone at extension 2828.

Passwords should not be written down. However, those who are concerned about forgetting password values could write a password hint or a masked form of the password to make it difficult for someone who might find that piece of paper to figure out the password's value. Password must never be written down with other identifying information, such as its associated user ID or web site. There are tools available that can store password information in an encrypted file that can be unlocked using a single password. For information regarding these "password safe" products, please contact the UCT Support Center at supportcenter@uhcl.edu.

05. Locking Unattended Computing Devices

A computer, tablet, smartphone, or other computing device that is logged in and unlocked when unattended allows anyone who accesses that device to perform activities under the logged in user's identity that can place UHCL information resources at risk, and may even put the logged in user in the unenviable position of having to explain improper activities that might have been performed by the intruder **in his or her name**, e.g., web surfing, e-mail messages sent.

To reduce the likelihood of an unauthorized individual using an already logged in device to compromise any UHCL information resource, any computer, tablet, smartphone, or other computing device that has access to any UHCL information resource must be:

- Logged off or locked when left unattended. Windows computers can be locked by pressing the Ctrl-Alt-Delete keys on the keyboard simultaneously, and then clicking the "Lock Workstation" menu item.
- Configured to engage its password-protected screen saver whenever the workstation is inactive for twenty (20) minutes or more.

Additionally, anyone viewing level 1 (highly sensitive) or level 2 (sensitive) information on his or her computing device must take measures to prevent unauthorized individuals nearby from viewing it.

---

06. Protecting Transportable Technology

Besides having tangible monetary value, transportable computing devices, e.g., laptops, tablets, smartphones, may carry information that may be confidential and whose exposure could post a financial or reputational risk to the University. To ensure that information held on these devices is protected against disclosure:

- Every UHCL employee and contractor who uses a transportable computing device to access any UHCL information resource must secure it against theft and/or unauthorized use.
- It is strongly recommended that transportable computing devices that store or have access to any UHCL level 1 (highly sensitive) or level 2 (sensitive) information resource have software installed that encrypts the information stored on the device to prevent the exposure of confidential information should the device be lost or stolen. Please contact UCT's Support Center at supportcenter@uhcl.edu for information regarding encryption products.
- Any UHCL employee or contractor whose University assigned or personally owned computing device that has been used to access any UHCL information resource is lost or stolen, must immediately contact the University Police Department (281-283-2222) and the UCT Support

Center at supportcenter@uhcl.edu to report the incident. They will ensure that the appropriate members of the incident response team are involved.

07. Securely Disposing or Repurposing Computers, Hard Drives, and other Media

Even when a file is erased, it still remains on the media that stored it until the space that the file occupies is overwritten. The process of overwriting these files is called "disk wiping". To ensure that each computer, hard drive, and other storage medium is consistently and thoroughly wiped before it is discarded, donated or repurposed, the following actions must be taken:

- Before a computer, hard drive, or piece of electronic or magnetic media is discarded, donated, or repurposed, it must be wiped using software that has been approved by the University's Information Security Officer or it must be physically destroyed.
- Optical media that is no longer needed must be physically destroyed. Many modern shredders have the ability to shred CDs and DVDs.
- Because a single overwrite of a storage device can leave traces of the data that has been overwritten on the storage medium, the disk wiping tool used must be configured to overwrite the drive at least three times using methods approved by the University's Information Security Officer.

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 March 31

VI. Approval

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