University
of Houston
Clear Lake

Administrative
Policies and
Procedures

Information Security Program Procedural Handbook for Information Custodians (ISPHB04)

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.

Each day, dozens of technology specialists and managers support UHCL's information processing and delivery systems. These individuals, referred to as "Information Custodians", are required to manage the system components that they support in a manner that protects the confidentiality, integrity, and availability of the information to which they have been entrusted. Thus, UHCL has developed an information security program and a set of policies that describe the foundational principles upon which we can develop a consistent set of our own department's and work group's business practices.

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 who implement and/or support UHCL's information technology.

II. Applicability

Anyone who installs, configures, administers, maintains or supports UHCL technology must become familiar with the contents of this document. This document assumes that the reader has read and understands the definitions, roles, policies and procedures contained in the following documents:

- **Information Security Program Description, Roles and Program Policies (ISPOL01)**,
- **Acceptable Use Policy for UHCL Information and Systems (ISPOL02)**
- **Incident Response Policy and Procedures (ISPOL03)**, and
- **Procedural Handbook for All Employees and Contractors (ISPHB01)**.

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. Authorization

In the information security discipline, the term "authorization" can refer to one of two things:

- The process that an Information Owner or Designee follows to give an individual the permission to access the information resources that he or she owns,

- The process that an Information Custodian follows to apply the technology controls that allow an individual to physically and/or logically access information resources in a manner authorized by the Information Owner or Designee.

  Note - This document primarily focuses on the latter use of the term "authorization", and does not delve deeply into the decision making process that Information Owners and Designees must follow when making authorization decisions. That topic is described in depth in ***Section III-D*** *of the* ***Procedural Handbook for Information Owners and Designees (ISPHB03)****.*

Each Information Custodian must ensure that all products and procedures implemented within his or her context support the authorization process as follows:

- Requests to grant an individual access to a UHCL information resource must be documented in a physical or electronic form, and signed by the requesting individual, his or her supervisor, and the appropriate Information Owner(s) and/or Designee(s). An electronic form may be signed and dated using either of the two major digital signature technologies:
  - A digital signature based upon digital certificate technology, or
  - An electronic rendition of the signer's physical signature created using a signature pad or touch screen.

- The "Principle of Least Privilege" must be followed when authorizing access, i.e.,
  - Only information resources deemed as level 3 (public) may be made viewable without the authorization of the appropriate Information Owner(s) and/or Designee(s).

- Access to level 1 (highly sensitive) and level 2 (sensitive) information resources, and update and delete access to level 3 (public) information resources, may only be granted as authorized by the appropriate Information Owner(s) and/or Designee(s).

- No individual may be permitted to access any UHCL information resource in a manner beyond that which has been approved by the appropriate Information Owner(s) and/or Designee(s).

- Authorizing access to specific UHCL information resources by groups of users based upon job function, when it is reasonable to do so, is preferred over authorizing access on a user-by-user basis.

- No one may be granted administrator level privileges to any context without the signed approval of:

  - His or her supervisor,

  - The Information Custodian for that context, and

  - The University's Information Security Officer.

- Each Information Custodian must ensure that all authorization requests and their dispositions are tracked in a physical or automated system. Each record must include the appropriate, authenticated approvals. Acceptable authentication mechanisms include handwritten signatures, digital signatures or a work flow that requires each signer in the process to log on with his or her UHCL login credentials.

B. Securing Data Centers, Server Rooms, and Communications Closets

01. Physical Access Control

- Controls must be put in place to protect University business information against unauthorized physical access.

- All mission critical computer servers and network switches, hubs, routers, firewalls, and other network security devices must be physically secured, either in access restricted data centers, server rooms, or communications closets.

- All servers used to conduct University business must reside in a data center or server room that is approved by the University's Information Security Officer and UCT's Director of Infrastructure.

This includes any server located on- and off-campus (e.g., disaster recovery/business continuity sites.

- Physical access to any UHCL data center, server room, communications closet, or server cabinet must be authorized by the appropriate UCT or departmental data center manager or the University's Information Security Officer.

- Physical access to any of UHCL data center or server room must be controlled using technology that captures the identity of any individuals who enters the protected space and the time of entry. Each individual who is authorized to enter the site must have his or her access device encoded with his or her authorizations. To enter the site, the individual must present his or her identity credential (e.g., card key) to an authenticating device at the entry point by swiping, inserting, tapping, or bringing the card into close proximity.

- Any server that processes information that is classified as level 1 (highly sensitive), must be contained in a locked cabinet within the data center. Only individuals who are assigned to administer a server with level 1 (highly sensitive) data may have access to its associated cabinet key.

- It is strongly recommended that cameras monitor the activity in each data center or server room. Since data center activity is not a continuous process, a video system that is activated by motion detection and emails the captured video clips to an individual assigned to monitor activity is considered the most effective approach.

02. Environmental Controls

Data centers must comply with all applicable fire codes, including the installation of emergency lighting, emergency exit signs with battery backup, fire suppression technology, and an accessible water shut-off valve as applicable.

Data centers must be protected against power outages and environmental hazards such as fire, power issues, excessive heat, high or low humidity, or water damage.

Control mechanisms must be capable of producing alarms if certain thresholds are met, and of providing ongoing reports of environmental readings. The reports should provide status information regarding the following, at a minimum:

- Power, UPS systems, generators
- Temperature
- Humidity

- Water sensors

UCT infrastructure support staff must review control readings at least once daily.

03. Data Center Audit Requirements

The following physical security-related events must be captured in an automated security event log:

- All attempts, both successful and unsuccessful, to enter the data center or server room.
- Environmental controls nearing thresholds set by the appropriate UCT or departmental data center manager and the University's Information Security Officer.
- Video clips of data center and server room activity, if cameras are installed (recommended).

C. Device Management

Computer workstations, servers (physical and virtual), and appliances on any UHCL network must be configured in the following manner to reduce each device's exposure to attack. This section describes the requirements that must be met for all devices, with subsequent sections that list additional requirements for workstations and servers, respectively.

01. All devices

- Anyone who installs, configures, and/or supports any computing device that is used to access any UHCL information resource must:
  - Maintain up-to-date knowledge of the latest information security threats and countermeasures, and
  - Be familiar with recognized information security guidelines and best practices from recognized standards agencies, such as the National Institute of Standards and Technology (NIST), the Texas Division of Information Resources (DIR), vendors, and expert web sites.
- Hardware inventories must be maintained and reviewed on a regular basis to ensure that hardware address and other related information is accurate. Audits of all computer

workstations residing on any UHCL network may be performed at any time to ensure that each connected device is compliant.

- Each device must be configured with all unnecessary services disabled.
- Where possible, each workstation and server must be added to one of UHCL's domains so it can be managed by group policy.
- Every computer must be configured with a password-protected screen saver that automatically locks the device after a maximum of twenty (20) minutes of inactivity, and requires the user to reenter his or her password to regain access.
- Security-related updates for any piece of software that is installed on any computing device must be applied in a reasonable time period after the update is released as follows:
  - The time period must be approved by the University's Information Security Officer and must take into consideration the severity of the vulnerability, the likelihood of an imminent exploit, and any conditions in UHCL's technology environment that could mitigate or exacerbate the risk.
  - As a general rule, operating system updates that the vendor classifies as "critical" or "important" should be applied within one week after their release. Critical or important updates to third party application software and support software, such as Java, should be applied within one month.
  - Vendor updates that are intended to address information security-related vulnerabilities that are not considered "critical" or "important" should be applied as soon as it is feasible to do so.
  - If a conflict arises between a software update and any application software that precludes the roll-out of a critical update, the Information Custodian for the affected contexts should work with the University's Information Security Officer to develop a risk mitigation strategy for protecting the context against a possible exploit.
- Where the technology exists, each workstation and server must have anti-virus/anti-malware software installed that is configured to:
  - Update its virus and malware signatures at least once per day.
  - Run in active mode where all applications and documents are scanned for viruses and malware every time they are loaded into computer memory.
  - Scan the server's hard drive on a weekly basis at a minimum.

- No software may be installed on any UHCL computing device without a valid business justification approved by the University's Information Security Officer.

- Only commercial software that is supported by its vendor, "open source" software that has an active support community and application software developed and supported in-house may be run on any UHCL computing device. Any system, networking, database, application software, or any other software product, that is no longer supported by its vendor must be upgraded or replaced by the time the support ceases.

- Each computing device that is capable of keeping an audit trail must be configured to capture in a security event log all logon and logoff activity, and all activity performed using an account with administrative privileges.

- Having a standard device image for each platform is strongly recommended, where feasible.

- Where possible, domain accounts should be used instead of computer accounts that are locally administered on the computing device. If it is necessary to use a locally administered account to access a UHCL information resource, all password composition, expiration and account lockout rules defined in **Section III-D** of this document entitled "**Identification and Authentication (I/A)**" must be enforced on the computing device.

- All UHCL computing and networking devices must display the following warning message prior to logon, where possible:

> *The University of Houston-Clear Lake*
> *Legal notice as required by the State of Texas*
>
> \- -
>
> *Texas Administrative Code (Title 1, Part 10, Chapter 202) requires the display of the following notice pertaining to systems use within Texas Higher Education entities:*
>
> A. *Unauthorized use is prohibited*
>
> B. *Usage may be subject to security testing and monitoring*
>
> C. *Misuse is subject to criminal prosecution*
>
> D. *No expectation of privacy except as otherwise provided by applicable privacy law*

- Where possible, systems must be configured to:
  - Display the user's last login date and time upon successful login.

  - Not allow a user to open more than one session on any server under the same computer account.

- All technology managers must maintain up-to-date knowledge of security vulnerabilities, threats and countermeasures associated with the platforms they support by taking advantage of professional development opportunities and collaborating with information security-related organizations that alert participants of current activity.

02. Workstations

In addition to the above requirements, each UHCL desktop computer, laptop, tablet, smartphone or other computing device must:

- Be connected to a domain managed by University Computing and Telecommunications (UCT).

- Have its software firewall turned on and configured to limit the types of inbound communications sessions permitted from external devices to those necessary to conduct University business.

- Only run software and software versions approved by the University's Information Security Officer.

- Not be used for normal day-to-day work with an administrator-level account without the approval of the University's Information Security Officer.

- The individual to whom a UHCL computing device is assigned is responsible for taking measures to ensure that the device is protected against loss or theft.

  - The storage on any transportable computing device (i.e., a laptop, tablet or smartphone) that has been used to conduct University business, including those devices used to review e-mail, must be encrypted. The encryption of the hard drive of any desktop system that is not physically secured is encouraged.

  - Where possible, is configured in a manner that allows the device to be tracked and remotely wiped if lost or stolen.

03. Servers

For the purpose of this document, a server is a computing device that provides services to user workstations and other servers. The term "server" refers to a variety of devices including web servers, application servers, database servers, file servers, domain controllers, network servers, appliances, etc. In addition to the requirements listed for all devices, UHCL servers are subject to the following:

- All UHCL servers must be physically secured in a data center or server room protected by monitored, approved physical access control technology.
- The maintenance schedule for all of the University's servers must be documented and followed.
- Any UHCL server that houses level 1 (highly sensitive) data must also be secured in a locked cabinet within the secured data center or server room to further manage access to the device. Only individuals whose job function requires them to access the device physically should have access to the server cabinet key.
- Only those individuals who are responsible for installing, maintaining, administering or operating software on a UHCL server may be granted administrative access to the device.
- Servers should be installed using either a standard image or hardening script that ensures that the controls that are applied are consistent and complete.
- Each UHCL server and each UHCL web application must be tested with an approved vulnerability analysis tool:
  - Before it is made available for service,
  - Any time a non-trivial change is made to its configuration, and
  - At least once a quarter.
- The University's Information Security Officer is responsible for:
  - Coordinating the efforts of the technical support staff intended to remediate the deficiencies detected by the vulnerability analysis testing.
  - Working with Information Custodians to select appropriate vulnerability analysis tools.
  - Keeping management informed of major vulnerabilities uncovered and the status of the remediation efforts.

04. Virtual Server Technology

All virtualization software used on a UHCL server must be approved by the University's Information Security Officer.

Access to any virtual hypervisor must be tightly controlled and only available to support staff who have been tasked with managing the virtual environment.

The following hypervisor security events must be logged and reviewed daily at a minimum:

- Attempts to log into the hypervisor,
- Account creation and maintenance,
- Management of access privileges,
- Virtual machine (VM) creation,
- The installation of software on a VM, and
- User log offs.

---

05. Device Audit Requirements

Computer workstations and servers must be set up to capture audit log entries for the following events at a minimum:

- All user logons and logoffs,
- All unsuccessful attempts to access any resource,
- Administrative activities performed,
- History of software updates applied,
- Incidents when software updates failed,
- Suspected virus activity, and
- Communications traffic blocked by hardware and software firewalls.

While the logging of successful attempts to access information resources can have a significant impact on system performance, it is recommended that successful attempts to UHCL information resources carrying the greatest risk be captured as resources permit. Such decisions should be made in conjunction with the appropriate Information Owner(s) and/or Designee(s).

06. Vulnerability Management

Each Information Custodian, working in conjunction with the University's Information Security Officer, must ensure that the security of his or her managed technology components is reviewed regularly to determine whether security controls are current, effective, and configured appropriately. To accomplish this, these individuals must be diligent in maintaining an up-to-date awareness of the latest threats and vulnerabilities by subscribing to industry recognized security alert services.

Random visual inspections of configuration data should be performed quarterly. Where possible, testing should be performed using automated server and application testing tools to ensure that each UHCL technology component is configured and maintained in a manner that effectively minimizes risk, and that application software does not include any potential “back doors” that would allow a malicious entity to compromise UHCL information resources.

07. Change Management

UHCL's technology infrastructure is constantly changing and evolving to better support the University's mission. Except in cases where emergency maintenance is needed to restore service, any outages necessary to upgrade, maintain, or fine-tune computer systems, networks, databases and applications must be planned, scheduled and appropriately conveyed to affected stakeholders.

Change management processes must be documented and must ensure that UHCL information resources are protected against unauthorized modification before, during and after system implementation. This includes changes implemented on an emergency basis.

Change management procedures must support “separation of duties” where possible, e.g., individuals who develop software, prepare technologies for implementation, and/or test technologies should not be the individuals who move the solution into production.

A three tiered approach that includes individual development/test, quality assurance (QA) and production environments is strongly recommended.

Development/test environments must be physically or logically separate from QA and production environments.

The University's Information Security Officer should be briefed on all planned and emergency system and application changes to determine the impact of the modification on the security of the system. If it is determined that a proposed change does negatively impact security, a remediation action plan must be developed, documented, and approved by the University's Information Security Officer and the appropriate Information Owner(s) and/or Designee(s).

Copies of level 1 (highly sensitive) data must not be used for testing unless:

- The appropriate Information Owner(s) and/or Designee(s) have authorized the use of production data for testing,
- All level 1 (highly sensitive) data is masked or obfuscated before it is copied onto the development system in a manner that precludes the determination of the original values,
- All users involved in testing are already authorized to access the production data, and
- All access controls configured in the test environment are consistent with the access controls in the production environment.

08. Discarding or Repurposing Devices

For the purpose of this section, the term "repurposing" refers to the reassignment of the computing device to serve in a different on-campus or off-campus capacity, such as a device being transferred to another UHCL department or work group, being donated to another organization, etc. The actions below are recommended, but not required when the device is reassigned to a different person performing the same job function as the previous assignee.

Before discarding or repurposing any computing or networking device that has been used to access, process, or transmit UHCL information resources, its internal drive must be electronically wiped and/or physically destroyed to ensure that any remnants of UHCL data cannot be gleaned from the device.

Any piece of removable media that has been used to store a UHCL information resource must be physically destroyed before discarding or repurposing. Where the technology permits, the media must be electronically wiped.

D. Identification and Authentication (I/A)

All information gathered and maintained 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.

The term "identification and authentication" refers to the tools and methods used to determine and confirm the identity of an individual who is requesting access to a system or resource.

01. User Account Management

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,

- Every individual whose job function requires him or her to access UHCL information resources must have a unique computer account assigned that only he or she uses.

- Every computer account holder must use his or her assigned account whenever he or she accesses a UHCL information resource to provide personal accountability for activities.

- Departmental or work group accounts that are intended to receive e-mail messages that can be acted upon by members of a defined group are permitted, but one individual of the group must be identified as the account owner who "owns" the account, i.e., who is responsible for managing the account password and for maintaining and managing access privileges associated with the account's resources. The account owner, and a designee if the account owner is unavailable, are the only individuals who should be able to log into a system with the group account's credentials. Other members of the group may access the account's resources, but only using their own account credentials in the manner defined by the account owner.

- The use of shared accounts, i.e., having multiple users sharing a common computer account, is strongly discouraged. However, if there is a compelling business justification for such an account, it may be created with the approval of the University's Information Security Officer.

- If an account holder leaves the University, all access privileges to UHCL information resources that have not been identified as exceptions by the appropriate Information Owner(s) and/or Designee(s) must be disabled immediately. For example, a retiree may still be granted access to personal employment information while his or her other privileges are revoked. The account for each student who has left the University continues to have access to e-mail for a period of one year plus one semester.

- When an account holder’s job function changes, the access privileges associated with his or her account must be modified immediately to be consistent with his or her new role.

- Any domain computer account that has been inactive for sixty days must be disabled or deleted.

- Any domain account with administrator-level privileges that has been inactive for over thirty days must be disabled or deleted.

- Access privileges to UHCL information resources must be reviewed semi-annually by the appropriate Information Owner(s) and/or Designee(s) to ensure that each user has been granted a level of access that is consistent with his or her current job function.

02. Default Account Management

Security-related events that occur on UHCL systems, networks, databases, applications, etc., must be tracked by user account, where possible. Thus, the use of built-in default accounts and other shared accounts is not permitted without the approval of the University’s Information Security Officer. To ensure accountability:

- The initial default passwords for the standard “guest” and “administrator” accounts must be changed as soon as possible after the system is installed.

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

- If the system permits the standard “administrator” account to be renamed, it should be renamed to a user name whose purpose is less obvious.

- If the system permits the assignment of administrative privileges to individual computer accounts, the standard “administrator” account must be disabled once the individual privileged accounts are configured. In this case, each individual who is tasked with performing administrator duties on a system must use a unique administrator level account that has been assigned specifically to him or her for this purpose.

- If the system requires the standard administrator” account to be used to perform system maintenance, access to the system’s standard “administrator” account’s password must be controlled through a secure 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 University’s Information Security Officer.

03. Authentication Requirements

To access UHCL information resources, each user must have his or her identity verified or "authenticated" before the user may access the resource using an authentication mechanism that is consistent with the documented risk management decisions made by the appropriate Information Owner(s) and/or Designee(s).

Each user must self-identify with his or her assigned computer identity when accessing UHCL information resources except when the risk analysis performed by the appropriate Information Owner(s) and/or Designee(s) indicates no need for individual user accountability.

The authentication mechanism used to access any UHCL information resource must comply with the following:

- Enterprise authentication sources, i.e., domain accounts as opposed to accounts managed on the local device, must be used for authentication where possible.
  - Departments developing or implementing software or applications requiring authentication must utilize UCT enterprise authentication services.
  - When designing technology solutions that are hosted by an off-campus data center, it is strongly recommended that users authenticate against UHCL's central authentication services rather than having the hosted system perform the authentication function.
  - Exceptions may be granted with business justification and the approval of the University's Information Security Officer.
- Under no circumstances shall UHCL send authentication credentials, i.e., a file of user identifiers and passwords or password hashes, to an externally hosted service without the approval of the University's Information Security Officer.
- Access to UHCL information resources, except "view-only" access to information resources that have been classified by their Information Owner(s) and/or Designee(s) as level 3 (public) data, must be authenticated using an authentication mechanism that has been approved by the University's Information Security Officer. These methods include the following, either singly or in combination:
  - A password that meets the UHCL password standard,
  - An approved smart token, e.g., an RSA SecurID token,
  - An authorized digital certificate,
  - An approved biometric mechanism, e.g., fingerprint scan, retina scan, voice recognition.

- 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 (highly sensitive) data.

- Before an individual may access any level 1 (highly sensitive) or level 2 (sensitive) UHCL information resource in any of UHCL's technology-based contexts from an external network or from the UHCL public wireless network, he or she must open a session with and authenticate to the UHCL Virtual Private Network (VPN) service before a connection to the target system or application may be made.

04. Password Rules

Systems that use passwords for authentication must be configured with the following password restrictions, where possible:

- Both system and application passwords may be stored only in a "one-way encrypted format" where a password cannot be decrypted without knowing the password itself. For applications, the one-way encryption formula used must be approved by the University's Information Security Officer.

- The initial password and any reset password must be pre-expired, requiring the user to change his or her password immediately upon logon.

- Passwords must not be displayed or echoed in clear text.

- Password rules must be configured to prevent the entry of the most common, easy-to-guess passwords.

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

- The passwords for UHCL faculty, staff, contractor, and service accounts must expire after one hundred twenty (120) days after being set or changed, and should not match any of the previous six passwords used for the account.

- After a user has failed to log into a context five consecutive times, the system must be set up to take specific measures to evade a potential brute force attack. These measures may involve:
    - The engagement of automated evasion technology built into the operating system, or
    - The disabling of the account for at least twenty (20) minutes, or until a UCT Support Center representative or an administrator unlocks the account.
- Before a member of the Support Center staff or an administrator resets the password for any individual, that individual must verify his or her identity. Some acceptable methods of verification include:
    - Physically presenting his or her UHCL ID card,
    - Calling from his or her authorized work phone and providing appropriate authenticating information that UHCL has on file for that individual,
    - The successful use of the UHCL password reset tool, and
    - Accurate responses to security questions.
- Password composition and expiration rules should be reviewed by the University's Information Security Officer and Information Resource Manager (IRM) on an annual basis to ensure that the University complies with industry best practices.

05. Granting Elevated Privileges to an Account

Accounts determined as having elevated access privileges are those that allow the user to administer an information resource, to create and control the access of others to an information resource, or to bypass user-level system controls.

Requests to obtain elevated access privileges for a computer account must be supported by a compelling business justification for such privileges and must be approved by the University's Information Security Officer. If the elevated access privileges enable the user to access UHCL information resources that he or she has not been authorized to access, the appropriate Information Owner(s) and/or Designee(s) must also approve the request.

If granted, these accounts are subject to the following:

- The computer account user must be informed of the increased risks of using an account with elevated privileges.

- The account may only be used when performing specific job functions for which the user has been authorized and only for official University business.

- Computer accounts with elevated privileges should not be used for day-to-day tasks, such as sending and receiving e-mail, web browsing, etc., since any malicious software that can be delivered would execute with elevated privileges as well. For this reason, it is recommended that the elevated privileges be assigned to a secondary local or domain account that is used only when privileged tasks are being performed, instead of the requestor's domain account.

- The authorization of elevated privileges must include an expiration date. The elevated privileges must be removed or disabled on the expiration date or when the work that prompted the access has been completed, whichever is earlier.

- Each user must be made aware of the specific elevated access privileges that have been granted to his or her account.

- Abuse of elevated privileges may result in disciplinary action.

06. I/A Audit Requirements

Authentication systems must be configured to capture, in a security event log, user login and logoff activity, both successful and unsuccessful, at a minimum.

E. Access Control

This section refers to the tools and methods used to establish and enforce the rules that govern whether access to specific UHCL information resources should be permitted or denied based upon:

- The identity of the requestor, as determined when the individual logged in,

- The resource being requested, and

- The type of access being requested, e.g., view, add, update, delete, control.

Some access control systems also can allow or deny access to information resources based upon the additional criteria, such as the device originating the access request, the day of the week, the time of day, and the current date. In high risk scenarios, such expanded controls should be considered in conjunction with the appropriate Information Owner(s) and/or Designee(s).

01. Access Control General Requirements

Any access to UHCL information resources classified as level 1 (highly sensitive) or Level 2 (sensitive), and update access to any UHCL information resource must be managed in a manner consistent with the following principles:

- All privileges granted to users of UHCL information resources must be authorized by the appropriate Information Owner(s) and/or Designee(s).

- No access privileges may be altered without being properly authorized by the appropriate Information Owner(s) and/or Designee(s) in the manner specified in **Section III-D** of the **Procedural Handbook for Information Owners and Designees (ISPHB03)**.

- The access privileges being requested must adhere to the "principle of least privilege", i.e., only the minimum privileges necessary for the account holder to perform his or her job function may be granted.

- Where possible, access privileges to specific UHCL information resources should not be granted to individual users. Rather, user groups representing common job functions with common information resource needs should be set up with appropriate access privileges granted. Then, as users assume or leave those job functions, they merely can be added to or deleted from the appropriate group to obtain their access privileges.

- Access privileges to UHCL information resources must be reviewed semi-annually by the appropriate Information Owner(s) and/or Designee(s) to ensure that each user has the proper level of access for his or her current job function.

02. System Access Control Requirements

To prevent access controls from being bypassed, the following actions must be taken:

- No UHCL system may be configured to "trust" any non-UHCL-owned device or domain without the documented approval of the University's Information Security Officer.

- Only support personnel authorized by the appropriate Information Custodian are permitted to load or update software on any device in a centrally managed context.

- Access controls for system and application software in production and quality assurance (QA) environments must not be updated by anyone other than authorized administrators and change management personnel.

- Only database or system administrators who have been authorized by the Information Custodian of that system, may access database files directly through operating system commands.

- All servers that provide central technology services to the campus must be built to a pre-defined, standard configuration that is consistent with industry "best practices" for information security on that platform.

- The standard configuration for any device on the perimeter of the UHCL wired or authenticated wireless network or within a UHCL "de-militarized zone (DMZ)", such as firewalls, domain name servers, routers, proxy servers, web servers, e-mail servers, etc., must comply with industry "best practices" for system "hardening".

F. Network Management

This section focuses on the implementation of network technologies, including the UHCL wired, public and authenticated wireless networks, and the UHCL Virtual Private Network (VPN).

01. Network Management General Requirements

- Since many networking devices are built upon standard server platforms, they are subject to the requirements described in **Section III-C** of this document, entitled "**Device Management**."

- By default, each device that connects to any UHCL network must be assigned a non-routable IP address as defined by the Internet Engineering Task Force's RFC1918 unless there is a compelling business reason for using a routable address. All requests to assign a routable address to a device must be approved by the University's Information Security Officer.

- Any device that is used to access a level 1 (highly sensitive) or level 2 (sensitive) UHCL information resource must either be authenticated by its network hardware address (a.k.a. "MAC address") or must be connected to the UHCL Virtual Private Network (VPN). Once the connection to the UHCL information resource is made, the user also must authenticate to the system upon which the resource resides.

- Only Doman Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP) servers that are authorized by the University's Information Security Officer (ISO) are permitted on the network

- Each Domain Name Service (DNS) server must be configured, where technologically feasible, to utilize DNS security extensions that verify the authenticity of external DNS devices with which it communicates.

02. Firewall and Router Administration

Technically, firewalls and routers can be used interchangeably to block undesirable network traffic from reaching its intended target systems, but firewalls provide the additional benefit over routers of having a highly specialized and intuitive user interface to facilitate administration. Thus, firewalls are the preferred method of screening network traffic over routers with access lists. However, in cases where a router is used in a firewall capacity, all of the requirements listed below would apply equally for the router implementation.

Definitions

Computer and mobile devices are categorized using the following criteria:

- "Untrusted device" – A computer or mobile device that is connected to the Internet via an external network provider or to the UHCL public wireless network that is not using UHCL Virtual Private Network (VPN) technology approved by the University's Information Security Officer.

- "Internal workstation" - A computer or mobile device that is connected to the UHCL wired network or authenticated wireless network, or an untrusted device that uses the UHCL Virtual Private Network (VPN).

- "Outward-facing server" – A computer server or appliance located in the UHCL data center that must be accessible by untrusted devices. Outward-facing servers are typically web and standalone application servers.

- "Trusted application server" – A computer server or appliance located in the UHCL data center that provides processing or database services to corresponding outward-facing servers.

- "Core technology server" – A computer server that provides essential central technology services to UHCL users, systems and applications, i.e., directory services, authentication services, network services, e-mail.

Outward-facing, trusted application and core technology servers must be protected by up-to-date firewall technology that is approved by the University's Information Security Officer. While it is possible to configure network routers to function as firewalls, they should be used in this capacity only under limited circumstances with the approval of the University's Information Security Officer.

Every UHCL server must be protected by up-to-date, firewall technology that is approved by the University's Information Security Officer.

Firewall Configuration

Firewall technology is subject to the following requirements:

- Each UHCL firewall must be secured physically either in the data center or in a communications closet with authenticated physical access.
- Firewall technology may be a self-contained appliance or a software package that must be installed on a "hardened" platform, i.e., one whose operating software is consistent with security industry "best practices".
- The firewall must permit or block each requested communication session based upon the IP address of the source device, the IP address of the destination device, and the destination port. In cases for which a consistent source address is unavailable, an authenticated user ID may substitute for the source address.
- Firewalls must support "IP address spoofing detection", i.e., the ability to detect discrepancies between the IP address listed as the source of a communications packet and the physical port used to enter the firewall.
- Firewalls must be configured to BLOCK:
    - Any connection that is not explicitly defined,
    - Any connection to the firewall itself, except connections originating from the firewall's authorized management devices,
    - Any network management protocol, such as SNMP, that originates from a device connected to either an external network or the UHCL public wireless network,
    - Any connection from a device whose network address is inconsistent with its physical location, i.e., a source IP address that enters the firewall from an unexpected network segment.

Firewall Business Rule Administration

- All firewall rule additions and updates must be documented and approved by the University's Information Security Officer.

- Firewall rules must be configured to allow only communication sessions that have been explicitly authorized by the University's Information Security Officer. All other interactions must be denied by default.

- Firewall rules must permit access only to specific target devices and only to specific ports on the target device that are required to conduct University business. No firewall rule may grant access to all ports on any device on any UHCL network.

- At least five firewall "zones" must be configured, at least one for each device type described in "**Definitions**" at the beginning of this section. All traffic between any two zones must pass through the firewall.

  - An untrusted device may open a communication session only with an outward-facing server.

  - All devices except untrusted devices may open a communication session with a core technology server, but only using ports that are associated with the services the target device is intended to provide. Core technology servers may open outbound communication sessions as needed.

  - No device is permitted to open a communication session with an internal workstation or a trusted server without a documented business justification approved by the University's Information Security Officer.

  - While multiple unrelated trusted servers may share the same trusted zone, it is recommended that any trusted application server that processes level 1 (highly sensitive) data be placed in its own trusted server zone segregated from other trusted servers, where feasible.

- No untrusted device may establish a communications session with any device on a UHCL network that stores level 1 (highly sensitive) or level 2 (sensitive) data.

- No device may establish a communications session with any device that stores or processes level 1 (highly sensitive) data without passing through the firewall, except for application and database servers that are part of the same three-tiered implementation (i.e., web, application, and database server).

03. Intrusion Prevention Systems

All network traffic originating between untrusted devices and internal devices, outward-facing servers, trusted application servers, and core technology servers must pass through an up-to-date intrusion prevention system (IPS) that is approved by the University's Information Security Officer.

The IPS systems deployed must adhere to the following:

- Each IPS must, at a minimum, test for all network attack patterns that are delivered with the product. Network support staff and the University's Information Security Officer must determine the activities that the intrusion prevention system must block.
- Each IPS must be configured to update its malware signatures at least daily.
- Each IPS must capture all network activity that is consistent with known attack patterns in a security event log.

04. Network Audit Requirements

Routers, firewalls, and intrusion detection/prevention systems must be configured to capture the following events in a security event log:

- Communication sessions that were blocked by the device.
- Communication sessions that were successfully opened with a device that collects, stores, processes or transmits level 1 (highly sensitive) data.
- All administrative activity performed on the device.

G. Database Management

When database technology is used, the application and database software must be configured in a manner that ensures accountability for each database transaction performed. Central management of the databases by University Computing and Telecommunications (UCT) database administration staff is strongly encouraged.

Ideally from a security standpoint, a database should support one application system. However, from a practical standpoint, a database can be shared across multiple applications as long as each application uses its own schema. It is strongly recommended that databases containing level 1 (highly sensitive) data not be shared across applications where feasible so.

Each database may only house data associated with one segment of the development lifecycle, i.e., one database for the development/test environment, one for quality assurance (QA), and one production.

Level 1 (highly sensitive) production data elements should not be used for development or testing unless it is masked or “obfuscated” in a manner that cannot be reversed.

H. Web Server Management

Central management of the web servers by University Computing and Telecommunications (UCT) database administration staff is strongly encouraged, especially any web application that provides access to level 1 (highly sensitive) or level 2 (sensitive) data.

Only authorized server management personnel may be granted administrator-level privileges to the device and its operating software, e.g., operating system, networking software, web server, database software, file storage system, etc.

Each web application must have at least one individual assigned from office or department that either commissioned or purchased the application to serve as the “application owner”. Application owners typically perform application administrative tasks, such as granting privileges to the application, managing content, reviewing usage statistics, etc.

I. E-Mail Server Management

UHCL's centrally managed e-mail service must be configured with supported, up-to-date SPAM filtering and anti-virus/anti-malware software. Filtering must be performed on both inbound and outbound messages to ensure that UHCL is neither receiving nor propagating SPAM.

Both the SPAM filtering and all modifications to the SPAM filtering rules must be approved by the University's Information Security Officer.

J. Cryptography

Cryptography is a technology that provides enhanced protection for information resources in the following areas:

- Confidentiality, i.e., the need of an information resource to remain private,
- Integrity, i.e., its need to have its accuracy assured, and
- Non-repudiation, i.e., its need to preclude a sender from denying that he or she sent the document, or to preclude a recipient from denying that he or she received it.

01. Encryption Management

The University of Houston System's policy requires the encryption of level 1 (highly sensitive) data, and recommends encryption for level 2 (sensitive) data.

Any encryption solution deployed must be approved the University's Information Security Officer.

When the sensitivity of a UHCL information resource warrants the use of encryption, the following standards must be applied, where possible:

- There are two types of encryption system in the marketplace: symmetric encryption ("shared key") systems that use a single encryption key to encrypt and decrypt data, and asymmetric encryption ("public key") systems that use two corresponding encryption keys – one to encrypt the data and the other to decrypt it.
- Currently, the Advanced Encryption Standard is the preferred shared key encryption system. PGP, GPG, and RSA are the preferred public key encryption software. RSA is the acceptable mechanism for exchanging encryption keys using an asymmetric approach.

- Both shared key and public key systems are acceptable solutions to protect the confidentiality of information being stored or transmitted. Public key systems are geared more toward protecting person to person communications among the members of a group. Shared key systems are used more widely for protecting a communications channel carrying data between two sites.

- When a public key encryption system is deployed, it is most effective to manage the encryption keys centrally. However, for small applications involving the exchange encrypted data among small numbers of participants, the management of encryption keys may be managed on the user's local systems.

- The encryption keys used with symmetric systems must use a key length of 256 bits or more unless the computer running the software is being used at an international destination whose import laws restrict encryption key lengths.

- Encryption keys used with asymmetric systems should use a key length of 2048 bits or more.

- If traveling outside of the United States, please consult the University's Information Security Officer to ensure that the encryption software stored on your computer complies with United States export law, and with any import laws of your destination countries.

- All symmetric encryption keys and the private key of any asymmetric key pair must be treated as level 1 (highly sensitive) information.

- Access to central key generation workstations must be restricted both physically, e.g., in a locked room accessible via card key or biometric authentication, and logically, e.g., available only to authorized key administration personnel.

02. Data Integrity Verification Management

Each Information Custodian must ensure that all products and procedures implemented within their contexts support the data integrity function as follows:

- Any UHCL information resource for which its Information Owner or Designee indicates that its data integrity must be confirmed should be protected using hash values.

- Products that implement the "SHA-256" algorithms for calculating and verifying hash values are strongly recommended.

03. Non-Repudiation Management

When considering digital signature technology, keep in mind that there are two distinct mechanisms in the marketplace that have been referred to as “digital signatures”:

- The first type of digital signature is a digitized rendition of the individual’s actual hand written signature that is created by having the individual write his or her signature using an electronic stylus or his or her finger on a touch sensitive pad.
- The more common type of digital signature is built upon asymmetric “public key” encryption and hashing technologies. For a detailed overview of this form of digital signature and encryption/decryption technology, please refer to the following page in the University’s Information Security Office web site: https://www.uhcl.edu/computing/information-security/tips-best-practices/encryption.

Unfortunately, while one digital signature may be appropriate for one business process, it may not be appropriate for another. Therefore, it is important to contact the University’s Information Security Officer who will work with the University of Houston’s Office of the General Counsel to ensure that the approach you are taking is appropriate.

- When required, encryption-based digital signatures must be created using asymmetric encryption and hashing technology approved by the University’s Information Security Officer.
- Documents requiring digital signatures must be stored on non-modifiable media and must be accompanied by the appropriate public key and date/time stamp.
- All signed documents must be retained as long as we are legally required to do so. In cases for which no specific retention period is mandated, the Information Owner or Designee for that resource must decide how long the document should be kept.

04. Cryptography Audit Requirements

The following cryptography-related events must be captured in a security event log:

- All unsuccessful attempts to decrypt a protected UHCL information resource
- Optionally, all successful attempts to decrypt a protected UHCL information resource.
- All failed hash value verifications
- All digital signature verification failures.

K. Application Development and Implementation

In-house developed, open source and purchased application software that is installed at UHCL must be securely designed and implemented. Additionally, in-house developed software must be protected against accidental or intentional modifications that could expose UHCL information resources to unauthorized individuals, alter the information on file, or disrupt service. The goal of this section is to ensure that the above goals are effectively met.

01. Software Design

The design of any application software, whether in-house developed, open source or purchased, must be reviewed by the University's Information Security Officer during the design phase, and again right before the application begins system or QA testing.

Web application software that is intended to exchange level 1 (highly sensitive) or level 2 (sensitive) data with off-campus, non-VPN users must be organized using a multi-tiered approach made up of:

- One or more outward facing servers (i.e., web server) that manage the user interaction, and
- One or more internal trusted servers process the application's transactions and store the data.

Client-server application servers must be installed on internal trusted servers that are not accessible by untrusted devices, i.e., computers, tablets, smartphones and other computing devices that are connected to an external Internet Service Provider (ISP) or to the UHCL public wireless network.

Application software program code that has been developed in-house must go through a code review by an individual who is well-versed in the programming languages used and who was not involved in writing the code being reviewed. Code reviews should be performed before software is moved into the quality assurance (QA) or production environments.

02. Management of In-House Developed Application Program Code

Application source code must be managed by a source code management system approved by the University's Information Security Officer. Both the products chosen and their implementation must be consistent with the following:

- The system must be able to enforce "separation of duties" between developers and those involved in moving applications from the development environment to the quality assurance environment to the production environment.

- The change management software must be used to control and track modifications made to application software through its full development lifecycle.

- For each application, an individual who was not involved in the coding of the application will be assigned to serve as the "Change Manager" for the application.

- Access controls within the development, QA, and production environments, and within the change management software must be configured in the following manner:

    - An application developer may only be granted update or delete privileges for the application code that he or she supports.

    - Application software code may not be altered directly in the QA and production environments. Rather, it must be updated in the development change management system and moved to the QA and production environments. Configuration changes for third-party software may be applied directly to the production environment after appropriate testing in the development and/or QA environment has been performed.

    - The Change Manager will have read-only access to the application software stored in the change management system.

    - Only Change Managers will have privileges to move application software to the QA and production environments.

- An application change history must be maintained within the application documentation.

03. In-House Application Development Audit Requirements

The following system integrity-related events must be captured in a security event log:

- The change management software must be able to capture the following, where possible:

    - Each time an individual logs into and logs out of the change management system.

    - All modifications to any of the applications managed by the change management system.

- All attempts to add, modify, or delete resources within the Quality Assurance and Production environments must be captured in a security event log.

L. Backups and Disaster Recovery/Business Continuity Planning

A sound backup and recovery system helps to ensure that data and applications are recoverable in case information is tampered with or destroyed by natural disasters, disk drive failures, malicious software, system compromises, human error, etc. A data backup plan must be defined and operational for all mission critical systems.

01. Backup Media Security

- Any system that stores information considered by its Information Owner or Designee as being mission critical must be backed up daily to two backup systems: one on-site and one off-site.

- Off-site storage arrangements must be subject to contractual terms that have been approved by the University of Houston System's Office of the General Counsel. These terms must include, at a minimum, an indication of the sensitivity of the information being stored, UHCL's information security requirements for data-at-rest and data-in-transit, the verification of the vendor's compliance with UHCL's requirements, and actions to be performed at contract termination.

- Whether on-site or off-site, backup media must be stored in a location that is accessible only to authorized individuals.

- The transport of physical media must be performed by a contracted, bonded courier.

- Backup storage media should be encrypted, where possible.

- Backup storage media must be labeled accurately and annual exercises must be scheduled and conducted to ensure that the backup storage can be used effectively to restore operations to the required level.

- Backup media must be destroyed or the data that it holds must be "wiped" when the information that it holds is no longer needed. The data wiping software used must be approved by the University's Information Security Officer.

02. Disaster Recovery/Business Continuity Plan (DR/BCP)

For each mission-critical UHCL information resource, the University's Information Security Officer, the Information Owner or Designee, and appropriate Technology Managers must develop and maintain an effective Disaster Recovery/Business Continuity Plan (DR/BCP) that will allow mission-critical functions to continue if services are lost due to environmental or physical disasters, power outages, equipment failures, system compromises, human error, etc.

Each DR/BCP must be approved by the University's Information Security Officer who will:

- Integrate all DR/BCPs for each of the mission-critical information resources,
- Ensure that information- and technology-related plans are consistent with the comprehensive, University-wide plan maintained by the Director of Emergency Management, and
- File the combined DR/BCP with the UHCL Office of Emergency Management.

Each DR/BCP should contain the following:

- Roles and responsibilities,
- Procedures for performing backups and managing backup data on- and off-site,
- Backup storage requirements,
- Procedures for recovering each UHCL information resource and its priority relative to other resources,
- Physical and network access controls for on-site and off-site storage to protect the information against loss, theft, damage, unauthorized exposure, modification or destruction, etc., and
- Routine testing procedures to ensure backups are viable and can be recovered.

UHCL must have a contractual arrangement in place with a backup site in case an extended outage occurs. The contract with the backup data center vendor must clearly state the sensitivity of the information being processed and UHCL's security and service level expectations, and must be approved by the University of Houston System's Office of the General Counsel.

Choosing a backup site consider factors that reduce the risk of both sites being incapable of restarting operations, such as the physical distance between the two data centers, power grids, etc.

The DR/BCP must include procedures for transferring control to the backup site and returning service back to the UHCL data center. Both procedures must be tested at least annually.

M. Security of Transportable Storage Media

As is the case for laptops, tablets, smartphones, and other transportable computing devices used to store or process UHCL information resources, the protection of transportable storage media (e.g., portable drives, USB tokens) that contain UHCL information is the responsibility of the person to whom the device is assigned.

Level 1 (highly sensitive) information may not be stored on a transportable storage device in an unencrypted form. The use of self-encrypting storage media is recommended over the manual encryption of the data prior to being storage on the device.

Transportable storage media must be physically secured in a locked drawer or cabinet when not in use. Keys must not be left in the lock when no one is present.

N. Security Event Log Monitoring

Audit trails or “security event logs” must be maintained to:

- Provide accountability for updates to critical information, hardware and software, and for all changes to the security configuration or access rules, and

- Enable UHCL to detect possible malicious activity from devices both inside UHCL and entering UHCL through the Internet.

- Build an effective history of computer activity that can enable UHCL to track activity associated with specific source and target devices, computer accounts, etc.

The University’s Information Security Officer is responsible for ensuring that the security event logs associated with devices that store, process or transmit UHCL information resources provide sufficient information and are monitored at least daily to detect any activity that could lead to the unauthorized disclosure, modification, or destruction of UHCL information resources.

01. Security Monitor Role and Responsibilities

A security event log monitoring program must be in place to detect suspicious activity on UHCL systems, networks, databases, and applications. Any security event log monitoring program must include the following:

- "Separation of Duties" - No individual may be assigned the task of reviewing a security event logs for the purpose of detecting inappropriate activities for any system for which he or she:
  - Has administrative privileges, or
  - Reports to any person who has administrative privileges.
- Security event logs must be reviewed at least once per day for events described in the sections below. To reduce the amount of time between the initiation of malicious activity and its detection by the security monitor, the implementation of security information and event management (SIEM) software that is capable of detecting suspicious activity in "real time" and of immediately notifying appropriate personnel is strongly recommended.

02. Security Event Log Configuration

The following actions must be taken to ensure that security events are not lost due to improperly configured resource constraints:

- Procedures must ensure that the storage space reserved on the system for event log data is sufficient to store at least one month's worth of log data.
- All devices that generate log data must have their system time clocks synchronized using a trusted time service.

03. Security Events to be Captured

The following events must be captured in the security event log, where possible:

- User logons and logoffs,
- Unsuccessful attempts to access systems, files, services, and other resources,
- Successful attempts to access level 1 (highly sensitive) resources,
- Actions taken by administrators,
- Attempts to clear the event logs,

- System start-ups and shut-downs,
- Service start-ups and shut-downs,
- Detected viruses or other forms of malicious software,
- Unsuccessful attempts to decrypt resources,
- Data, system, and application integrity-check failures, and
- Digital signature verification failures.

---

04. Security Event Data Elements to be Captured

For each auditable event, the following data elements should be captured in the security event log, where possible:

- The date and time of the event, using a recognized, centrally managed time service,
- The host name and/or network address of the device that reported the event,
- The user ID that was logged into that device at the time, if any,
- The host name and/or address of the device from which the action was attempted,
- The action that was performed or attempted,
- The host name and/or network address of the resource that was the target of the action,
- The computer account that was the target of the action, if applicable,
- Whether the action was successful or unsuccessful, and
- Event specific information not covered above, as available.

---

05. Security Event Log Monitoring Requirements

At a minimum, the security-related events in both system and application generated security event logs must be reviewed at least once every twenty-four hours. At a minimum, daily monitoring tasks must include review of:

- Known hacking patterns encountered, including but not limited to:
    - Denial of service (DOS) and distributed denial of service (DDOS) attacks,
    - Attempts to test for the availability of system services, e.g., port scans.
    - Instances of more than ten (10) unsuccessful attempts to log into a system or application,
    - Unsuccessful attempts to change a password,
    - Unsuccessful attempts to access UHCL information resources, and
    - Unsuccessful attempts to execute functions associated with administrators.
- All administrative activity,
- Detection of malicious software, and
- Inappropriate use of system and network resources.

06. Protection of Security Event Log Data

To ensure that security event logs are not lost or modified, the following actions must be taken:

- Where possible, audited events must be captured to one or more centrally-managed servers that is/are secured in a manner that precludes the modification and/or deletion of log records by anyone except security event log monitoring personnel.
- Any attempt to clear log files, to modify and/or delete log records, or to change the logging configuration in any way must be logged.
- At a minimum, security event logs must be maintained online for thirty (30) days and offline for one (1) year. Some systems may require a longer retention period for their security event logs to satisfy the Information Owner’s risk objectives and UHCL’s legal and contractual obligations.

O. Incident Handling, Cyber Response and Forensics

Any member of the technical support staff who suspects that a UHCL information resource may have been disclosed to unauthorized individuals due to a system compromise, loss or theft, must contact the UCT Support Center at extension 2828 or **supportcenter@uhcl.edu** either directly or through his or her supervisor.

Once it is confirmed that a UHCL information resource may have been exposed or is currently at risk, the UCT Support Center will contact the University's Information Security Officer who will initiate the information response procedure that is described in the document entitled **Incident Response Policies and Procedures (ISPOL03)**.

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