University of Houston Clear Lake

**Administrative Policy and Procedure Library**

# *Information Security Program Incident Response Policy and Procedures (ISPOL03)*

**Date Issued: November 17, 2016**

**Last Revision: October 1, 2018**

# Table of Contents

# I. Purpose and Scope

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

This document describes the policies, procedures, and roles of members of the UHCL community when UHCL information resources are suspected of being disclosed to unauthorized individuals, when computer or personal activities raise "red flags" about possible malicious activity, and when copyright infringement claims are received.

# II. Applicability

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

This document assumes the reader already has read and understands the content of the following Information Security Program documents:

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

# III. Policies and Procedures

## A. Response to a Potential Data Breach

### 01. Potential Data Breach Response Policy

*Terminology*

The term "data breach" refers to the possible disclosure of data that is the result of situations that include, but are not limited to:

- A computer, tablet, smartphone, or piece of portable media being lost or stolen,
- A computing device exhibiting suspicious behaviors and a member of the technology support staff determining that it has been compromised, or
- Level 1 or level 2 data, as defined by the University of Houston's System Administrative Memorandum **SAM 07.A.08 – Data Classification and Protection**, potentially being accessed by an unauthorized individual or entity.

*Actions must be taken to ensure an effective partnership with law enforcement*

UHCL requires that all actions taken in response to a reported incident consider how the University will interact with the appropriate law enforcement authorities and other organizations that may be involved in the breach.

For cases of suspected criminal activity, the UHCL Police Department must be engaged immediately to initiate an investigation and/or contact external law enforcement agencies, as necessary.

Additionally, it is critical that all forensic activities used to investigate the potential security breach are executed in a manner that satisfies federal, state, and local requirements for the proper handling of evidence, since any procedural error could interfere with any potential prosecution of a prospective offender.

*Response must be collaborative*

UHCL's response must be a collaborative effort with representation from a number of UHCL and University of Houston System departments, as appropriate. The following table lists the individuals, and groups that may be called upon when a potential data breach that occurs:

| Participant | Role |
|---|---|
| The individual whose device was lost, stolen, or compromised | Report the incident to the UCT Support Center and provide background information about the device and any data it may have stored. |
| UCT Support Center | Engage the University's Information Security Officer and UHCL Police Department if potential criminal activity is suspected. |
| The University's Information Security Officer | Convene the incident response team and coordinate incident response activities, track progress, maintain a complete log of incident response activities, and keep senior management informed. |
| UHCL Police Department | Perform local investigations and coordinate with external law enforcement agencies, as necessary. |
| The University's Information Resource Manager to support efforts | Provide investigative resources as needed, and ensure that any deficiencies that may have facilitated the breach are remediated promptly. |
| The Information Owner(s) and/or Designee(s) associated with the potentially exposed data | Determine whether or not any information that may be exposed is protected and requires the notification of affected parties. |
| The University of Houston System's Chief Information Security Officer | Provide expertise and procedural guidance. |
| The University of Houston System's Office of the General Counsel | Provide legal guidance and notification text. |
| The manager of the University department or work group whose device was lost, stolen, or compromised | Contribute to the notification process and to possibly send notices to affected parties under his or her signature. |

*All incident response activities must be documented by the University's Information Security Officer*

Incident documentation must include:

- A description of the incident,
- The individuals involved,
- The systems and other technologies involved,
- The investigative steps that have been taken,
- The results of those actions,
- Whether or not notifications were required and sent,

- The final disposition of the incident, and
- A description of any weaknesses in the UHCL environment that facilitated the incident and recommended remediation efforts.

### *Incident response procedures must be tested on an annual basis*

All incident response data compromise scenarios must go through at least a tabletop exercise to ensure that all potentially involved parties fully understand their roles and responsibilities within the incident response context.

---

## 02. Potential Data Breach Response Procedure

### *Step 1 - Determine if a data breach might have occurred*

If the computing device was lost or stolen:

- Any member of the UHCL faculty or staff, or contractor who has lost or has had stolen a computer, tablet, smartphone, or other computing device that has been used to store, process or transmit University data lost or stolen, or who suspects that a UHCL information resource has been exposed as a result of a system compromise or a procedural error, must report the incident immediately to the UCT Support Center at extension 2828 or via e-mail at supportcenter@uhcl.edu. The Support Center will direct the individual reporting the loss or theft to fill out a standard incident form with pertinent information regarding the case. Once completed, the individual should submit the form directly to the University's Information Security Officer.

- Any student who has lost or has had stolen a University-owned laptop, tablet, smartphone, or other computing device that he or she has borrowed from the University's loaner program, must report the incident immediately to the staff at the University location that provided the student with the device. The staff member receiving the report will gather all pertinent information related to the incident from the student and enter it into the standard incident form. The form should be forwarded to the University's Information Security Officer and the UHCL Police Department.

  *Note: The standard incident form can be found at the following web site: http://www.uhcl.edu/computing/information-security/procedures/stolenlost.*

- For cases of possible criminal activity, the Information Security Officer will involve the UHCL Police Department, if the individual who reported the incident has not done so already. The UHCL Police Department will work with any external agencies, when necessary.

- In all cases of loss or theft, the appropriate manager of the department whose device inventory is affected by the incident and Property Management also must be notified.

- The University's Information Security Officer will work with the individual involved in the incident to determine if it held any level 1 or level 2 data as defined by **SAM 07.A.08 Data Classification and Protection** that may have been exposed. If a backup copy of the lost or stolen device's hard drive is available, the backup copy must be restored onto another computer and scanned for level 1 and level 2 data using scanning software approved by the Information Security Officer. If there is no backup copy, the University's Information Security Officer will interview the device user to determine what data might have been on the device.

- If it is determined that the device contains level 1 or level 2 data, the University's Information Security Officer will direct the appropriate support staff to remotely wipe the device lost or stolen device, if possible.

If a computer is still in the University's possession but is exhibiting suspicious behavior:

- The member of the support staff who maintains the device, either a member of the UCT Technical Services team, the Academic Computing team, or the departmental staff member tasked with supporting the device, should triage the device to determine if the device is being impacted by application, system, or network performance problems.

- The support staff member will notify the University's Information Security Officer about the results of his or her triage effort. If the cause of the suspicious activity is determined to not be a system compromise (e.g., a hardware failure, software "bug"), the incident can be closed.

- If the suspicious activity is deemed to be the result of malicious activity, the Information Security Officer will work with the technology support staff to determine the risk level of the information stored on or accessible through the device. This process involves:

    - Shutting the system down,

    - Making a "forensic copy" of the system's hard drive on read-only media, and

    - Storing the forensic copy in a secure storage facility to preserve the "chain of evidence".

    - Scanning the hard drive for level 1 and level 2 data using scanning software approved by the University's Information Security Officer.

    - The University's Information Security Officer also will work with the individual whose device was compromised to determine what types of data typically was stored on the device.

In all other cases, such as the inadvertent electronic or manual transfer of level 1 or level 2 data to an unauthorized individual:

- The Support Center will forward the information about the reported incident to the Information Security Officer.

- The Information Security Officer will review the information presented and will work with the individual who made the data available to determine whether or not level 1 or level 2 data was involved.

*Step 2 – Respond to the possible disclosure of level 1 or level 2 data*

For any of the above cases, if there is no evidence of level 1 or level 2 data being exposed to unauthorized individuals, the University's Information Security Officer will close the case and document the disposition.

If it is possible that level 1 or level 2 data has been exposed, the Information Security Officer will take the following actions:

- Notify the University's Information Resource Manager and the University of Houston System's Chief Information Security Officer of the potential data breach,
- Contact and work with the appropriate Information Owner(s) and/or Designee(s), and the University of Houston System's Office of the General Counsel to confirm the risk level of the data and whether or not the suspected breach requires the University to notify any affected parties. If so, this group will work with the manager of the department in which the possible breach occurred to develop the notification text and to determine under whose signature the notice will be sent,
- Keep senior management informed about the potential data breach, the associated risks and the status of the actions being taken,
- Work with the appropriate Information Custodians to determine how UHCL can mitigate any risk associated with the incident,
- Inform any external organizations that may have been affected by the potential breach,
- Coordinate the risk mitigation efforts, and
- Document all of the activities performed throughout the investigation.

## B. Response to a Red Flag Alert

UHCL must ensure that each staff member understands his or her responsibilities as they relate to the detection of and response to potential "Red Flag Rule" violations described in the University of Houston's System Administrative Memorandum **SAM 01.C.14 – Identity Theft**.

## C. Response to a Copyright Infringement Claim

UHCL takes copyright infringement matters very seriously, and is committed to investigate each infringement claim thoroughly and to address all verified claims diligently.

The University of Houston System has developed the following System Administrative Memorandum for handling copyright infringement cases in **SAM 07.A.04 – Digital Millennium Copyright Act**.

To address such issues, the University's Information Security Officer is responsible for:

- Following up on all Digital Millennium Copyright Act copyright infringement notices promptly,
- Working with technology staff to determine the individual(s) involved in the alleged infringement activities,
- Contacting each identified individual and his or her dean or manager to:
    - Inform them about the copyright infringement claim,
    - Request that the activities cease immediately, and
    - Remind the identified individual that such activities may be subject to a loss of network privileges and/or other disciplinary action at the offender's dean or manager discretion.
- Documenting the disposition of each incident.

# 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<br>b) Updated name of UHCL President<br>c) Added a requirement to test incident response procedures at least annually |
| 3 | 10/01/2018 | Replaced Glen Houston with Anthony Scaturro in the list of approvers |

# V. Policy Review Responsibility

*Responsible Parties:*

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

*Review Period:*

- Annually on or before January 31

# VI. Approval

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