Information Security Incident Response Procedure

Background

This document and governance structure provides the oversight of and guidance for the required processes for the University of Cincinnati's (UC) security breach response in compliance with applicable federal and state laws, and university policies.

This plan is intended to be scalable. Its use is not necessary for every security incident, as many incidents are small and routine and require only a single responder. It is left to the judgment of the Incident Handler (defined below) or their designee to determine when to convene the Information Security Response Team (ISIRT), however, it will generally be necessary for all "significant" or "high-visibility" incidents (described below). When the ISIRT is convened, this plan document must be consulted, and the elements appropriate to the individual incident must be used.

TABLE OF CONTENTS

SECTION 1: GOVERNANCE

DEFINITION OF ROLES

- **AVP of Information Security** – Serves as the governing authority of for all information security incidents and responsible for communication with IT@UC and university leadership.
- **Incident Handler** - The AVP of Information Security will designate either an individual or a functional position to be responsible for the oversight of the incident investigation. This individual, or their designee, will determine whether to convene the Information Security Incident Response Team (ISIRT) and will communicate the details of the incident to participating teams.
- **Incident Analyst(s)** – Staff members from the IT@UC Office of Information Security (OIS) responsible for the hand-on incident response and report to the Incident Handler.
- **External Entities** – Sometimes, external entities are required to aid in the response for a significant incident. These entities will be contacted on a per-incident basis, and will be involved as deemed appropriate. Examples of external entities are, but not limited to: Internet Service Providers (ISPs), Security Solutions Vendors, consultants and law enforcement (e.g. FBI and DHS).

CHARACTERISTICS OF "SIGNIFICANT" OR "HIGH-VISIBILITY" INCIDENTS

The ISIRT will almost always be convened for all "significant" or "high-visibility" incidents. This is an inherently subjective criterion, so individual judgment is required. However, for the purposes of guidance, some examples of such incidents include, but are not limited to:

- Incidents involving key UC personnel, such as campus leadership and prominent faculty or alumni.
- Incidents for which a press release may or will be issued or media coverage is anticipated.
- Incidents involving 25 or more affected individuals (incidents involving fewer individuals may still be "significant" or "high-visibility," e.g. UC leadership).
- Incidents likely to result in litigation or regulatory investigation.
- Incidents involving criminal activity.
- Any other incident that is likely to involve reputational, regulatory or financial risk to UC of which senior management should be aware.

EMPLOYEE RESPONSIBILITIES

Every faculty and staff member at UC has the responsibility to immediately report suspected or

known information security incidents or breaches of the privacy or security of Restricted data to the IT@UC Office of Information Security. Criminal acts, such as theft, or suspected criminal acts, should also be reported to the UC Police Department (UCPD).

DEPARTMENT RESPONSIBILITIES

All departments and colleges are responsible to maintain, keep up-to-date, and provide to OIS contact information of Data Custodians, IT administrators, and management to be notified in case of an information security incident.

INFORMATION SECURITY INCIDENT RESPONSE TEAM (ISIRT)

The following are the minimum required individuals or functional areas for the ISIRT for every incident for which the ISIRT is convened (smaller incidents will likely be handled by the Information Security staff):

- Incident Handler
- Incident Analyst(s)
- AVP of Information Security (for “high visibility” and “significant” incidents)

The following functions, and any others not listed, may be added to the ISIRT, as appropriate to the incident:

- Information technology system owners and appropriate support personnel
- Director of Privacy
- Office of General Counsel
- Enterprise Risk Management
- Department Leadership of affected unit(s) (Dean, Chair, etc.) or their designee
- Office of the Provost
- Public Information Officer/Public Affairs
- Government Relations/Legislative Liaison
- Human Resources/Academic Personnel
- UCPD and other law enforcement, including FBI, as appropriate
- Office of Internal Audit
- Office of Governmental Relations and Communications
- Export Controls Office
- Office of Emergency Management
- Other executives, as appropriate

RESPONSIBILITIES FOR INCIDENT RESPONSE

- Upon initial determination of a possible security incident, departmental management shall notify OIS immediately.
- The ISIRT is responsible for the execution of all the Sections of this plan that are applicable to the specific incident, and may deviate from this plan, after consultation with the AVP of Information Security, to the extent necessary to respond to the incident.
- As one of their first actions, the Incident Handler shall consult with legal counsel to identify possible conflicts of interest in the investigation. In particular, individuals or teams may not lead investigations within their own areas of responsibility. Counsel should also be consulted regarding possible law enforcement involvement, or the need for forensic investigation.

- As one of their first actions, the Incident Handler shall consult with Enterprise Risk Management to determine whether University of Cincinnati Cyber/Internet Liability & Breach Response Services might provide insurance coverage for the incident, or should be engaged in response.
- The Incident Handler shall ensure that resources are assigned to conduct the investigation, as applicable to the incident. In the event of possible conflicts of interest, those resources must be sufficiently independent to avoid the appearance of a conflict of interest.
- For an electronic incident, OIS shall conduct the forensic investigation.
- The ISIRT is responsible to ensure that, if necessary, evidence is preserved, and each incident is adequately documented. “Adequate” documentation will stand on its own, without requiring further explanation.

SECTION 2: TRIAGE AND SCOPING

OVERVIEW

The triage and scoping phase involves the process of analyzing the information about the situation to determine whether or not a security incident has occurred. This section includes guidance for incident identification, initial reporting, priority-setting based on data and system criticality and sensitivity, required collection and analysis of incident information, information preservation, documentation, and communication.

WHAT IS A SECURITY INCIDENT?

A security incident may involve, but is not limited to, any or all of the following:

- A violation of campus policies and standards
- Unauthorized system or information access
- Loss of information confidentiality
- Loss of system or information availability
- Compromise of system or information integrity
- Denial of service condition against data, network or computer
- Misuse of service, systems or information
- Physical or logical damage to systems, or device theft
- Presence of an unauthorized application, such as malware
- Unauthorized or suspicious network activity

INCIDENT REPORTING

All suspected or confirmed privacy or data security incidents must be reported to OIS in accordance with the Information Security Incident Management and Response Policy. The initial severity level

may be escalated or de-escalated by the information security staff for an electronic incident. All incident reports are to be made as soon as possible after the incident is identified, and with minimum delay for medium to high severity incidents.

INITIAL INCIDENT REPORTS

Initial incident reports must include the following information when describing the incident:

- Date and time of incident discovery
- General description of the incident
- Systems or data at possible risk
- Actions they have taken since incident discovery
- Their contact information
- Any additional relevant information known at the time

INITIAL INCIDENT DOCUMENTATION

Most incidents will not be directly reported to the Incident Handler, but most likely will be processed through local IT support structure or business unit management. If the ISIRT is convened for an incident, the information identified in Figure 1, or as much of the information as is available, must be collected, documented and shared with the ISIRT. When possible, the information will be obtained directly by a member of ISIRT, unless incident circumstance prevent this.

Figure 1
Incident Reporting Elements

Information to Record	Description
References	Assign the next sequentially available OIS incident or investigation number as appropriate
Suggested Severity Level	Low, Medium, High, Critical
Type of Incident	Note all types that apply, including but not limited to 1. Compromised System 2. Compromised User Credentials 3. Network Attacks (DOS, Scanning, Sniffing) 4. Malware (Viruses, Worms, Trojans) 5. Lost Equipment/Theft 6. Physical Break-in 7. Social Engineering (Phishing) 8. Law Enforcement Request 9. Policy Violation 10. General Counsel Request (non-specific) 11. Public Records Request 12. Litigation Hold/Search 13. Copyright Violation 14. Data Breach (physical or electronic) 15. Export Controlled Data Exposure
Incident Timeline	Date/time that the incident was discovered Date/time that the incident was reported Date/time or data range that the incident occurred (if known)
Who or what reported the event	Person or Persons: Contact Information for the Incident Reporter: full name, user ID (6+2), organizational unit/department, title, email address, phone number, and location (mailing address, office room number). Automated System: Name of software package, name of the host where the software is installed, physical location of the host, system owner or department, network address of the host, and MAC address of the host if possible.
Incident Contact Information	List contact information for all parties involved in the incident.
Detailed description of the event	Include as much information as possible such as: Description of the incident (how it was detected, what occurred) Description of the affected resources Description of the affected organizations Estimated technical impact of the incident (i.e. data deleted, system crashed, application unavailable) Summary of response actions performed Other organizations contacted Cause of the incident if known (misconfigured app, unpatched host, etc.) List of evidence gathered Total hours spent on incident handling and/or additional non-labor costs involved in handling (estimate) Incident Handler Comments
Identification of the host(s)	Source of the Incident: List of sources Host name/IP Address Target of the Attack: Host Name/IP Address (note: Target of the attack should not be listed for incidents involving protected health information or sensitive student information)
Incident Handling Action Log	Include: actions taken, when, by whom
Physical Security Controls	If there is limited physical access to the computer, document the physical security controls that limit access (ask the person reporting the event to describe what they have to do to access the computer).

INCIDENT CLASSIFICATION

All incidents that are processed by the ISIRT shall be classified by the ISIRT. Incident classification informs those involved of the severity and impact of the incident, and ensures that the incident receives the appropriate level of attention. Classification also ensures that the incident is reported to management in a timely manner.

The incident classification table, Figure 2, provides several incident factors to assist in proper incident classification. Depending on the nature of the incident, some of the incident criteria represented in the table may not be present in a particular incident. Moreover, if an incident contains characteristics in several different severity columns, the severity of an incident must reflect the highest category.
Incident classification is a dynamic process. Incident severity may change one or more times as incident details emerge over time during the investigation process.

Figure 2
Incident Classification Table

Incident Factors	Incident Severity Characteristics		
	Low	Medium	High
Criticality – Application	Internal systems and applications	Internal or external systems and applications	Internal or external systems and applications
Criticality – Infrastructure (As defined in the Critical System Inventory)	User system	Non-critical enterprise system	Critical enterprise system
Criticality – Infrastructure	No	Limited Scope	Campus-wide impact
Impact – User/System	Affects few people or few systems	Department-wide impact	Campus-wide impact
Impact – Public	None	Potential impact	Definite impact
Countermeasures	Solutions are readily available	Weak countermeasures	No countermeasures
Encryption	Robust encryption algorithm, and key control	Weak algorithm and/or key controls	No encryption, or easily defeated encryption
Resolution Procedures	Available and well-defined	Resolution procedure not well-defined, bypass available	No resolution procedures or bypass available
Information Sensitivity	Affects an individual researcher, employee or unit	Affects an individual college or department	University-wide, statewide or national impact
Research Intellectual Property	Initial datasets	Research working papers and completed datasets	Publishable research
Protected Information (Personally- Identifiable Information or Protected Health Information)	None	Possible	Definite

CONTAINMENT STRATEGY

A containment strategy must be implemented that will limit the damage to university resources. The containment strategy must include contact information for various campus organizations and personnel who may be involved in incident response. Containment may involve a combination of technical controls, such as network and system disconnects, as well as media and communications to the public and to staff, depending upon the scope of the breach.

PRESERVATION OF EVIDENCE

Consideration should be given to preserving evidence during the Triage and Scoping Phase, particularly if it becomes apparent that the incident involves criminal activity. Containment, however, takes precedence over preservation while the incident is active. Proper preservation of evidence requires establishment of chain of custody procedures prior to an incident. Any electronic evidence should be properly tracked in a documented and repeatable process.

INCIDENT DOCUMENTATION

The importance of adequate and sufficiently-detailed documentation cannot be over-emphasized, especially if regulatory investigation(s) or lawsuit(s) arise as a result of the incident. Very serious consideration must be given to dedicating a single, full-time resource to adequately document the decisions that are made, and the actions taken, particularly for larger incidents. It is especially important to begin this type of documentation as soon as the need for the ISIRT is identified, so that documentation is performed dynamically during the incident.

IDENTIFY AND ENGAGE RELEVANT EXPERTISE

Identifying and engaging groups and individuals with relevant expertise is critical to accurately triage an incident and determine its scope. In large or complex cases, the ISIRT should consider bringing in a third party, such as an external organization to assist in the triage and scoping effort. In order to comply with terms of liability insurance, the insurance carrier may conduct a forensic investigation and participate in the incident response activities. Cooperation with the insurance carrier is required under the terms and conditions of the insurance policy.

In incidents where the level of severity or data impacted warrants, the ISIRT should consider engaging individuals and groups with appropriate subject matter expertise as described in the Information Security Incident Escalation Guideline. Incident Handler, or their designee, will establish contact with designated departments and/or individuals after an initial assessment and classification of the incident has been performed by the ISIRT.

COMMUNICATION/DISCLOSURE STRATEGY

Proper handling of internal and external communications is critical in the initial phases of incident response. It is quite possible that an initially small incident could grow into a large multi-site incident. It is also quite possible that a suspected incident could be determined to be unfounded.

Improper handling of communications could lead to embarrassment to the university in the event of a false positive, or could tip off any malicious attackers to cover their tracks, thus exposing the university to more risk.
Communication of incidents should be handled on a need-to-know basis, especially early on. The ISIRT will engage the IT@UC Public Information Office and Office of Governmental Relations and

Communications to facilitate incident appropriate communication strategies. All communications about the incident external to the ISIRT should be properly documented by the responsible department and conducted through a central point.
Legal counsel should be consulted to determine whether the investigation will proceed under the direction of counsel and attorney-client privilege. If so, counsel will establish particular procedures for communication and documentation.

If there is an impermissible use or disclosure of Protected Health Information (PHI) belonging to a UC HIPAA covered unit, a breach assessment will be conducted.

If it is determined that a breach has occurred, notification will be made to the individuals, Health and Human Services, and if applicable, the media, in accordance with UC HIPAA policy.

SECTION 3: EXECUTION

PREPARATION

The ISIRT should collect and review the incident documentation and event reports. This information should first be verified as being factual (information may have been misreported or incorrectly documented). The ISIRT should assign the incident severity, or re-consider its appropriateness if already assigned. The ISIRT should determine who outside of the ISIRT needs to be notified of the incident as per the Information Security Incident Escalation Guideline and make those notifications. Information should be restricted on a need-to-know basis.

If the incident requires computer forensic analysis, arrangements must be made to gain access to the data and devices involved in the incident. The primary objective is to maintain and restore business continuity.

CONTAINMENT

The ISIRT must communicate with system owners and departments for incident containment. Individual departments are responsible to engage sufficient staff with appropriate technical skills to do an effective job of containment.

The ISIRT must assess whether to disrupt services to internal or external customers. Decisions of this nature must be made in consultation with the appropriate senior leadership and an evaluation of whether the systems impact critical services.

ANALYSIS: DATA & SYSTEMS

Assess the cause and type of breach**.** Depending on the documentation provided to the ISIRT, it

should either validate or determine what types of data are involved, based on the university Data Protection Policy. The cause of the breach is determined by technical analysis and investigation, as described below.

FORENSIC ANALYSIS

Forensic analysis entails a technical examination of evidence, preservation of that evidence, preservation of the chain-of-custody of the evidence, documentation of observations, and analysis drawn from logical conclusions based on the evidence, absent opinion or conjecture. When conducting a forensic analysis, the analyst must adhere to the following principles:

- Analysis must be an unbiased examination of the evidence submitted.
- Chain of custody and evidence integrity is maintained thought the whole process of investigation.
- Forensic analysis does not pronounce or imply guilt. The purpose is to determine whether indicators exist that can tie the suspect hardware or identity to the incident under investigation.
- Report only verifiable information.
- Be precise. Statements such as “numerous,” “many,” “multiple hundreds,” etc. should be avoided. Specifically state the finding, as well as the precise locations of information.
- Identify the evidence being analyzed as thoroughly as possible.

SECTION 4: REMEDIATION AND POST-INCIDENT REVIEW

RESPONSIBILITIES

The ISIRT communicates the need for remediation to system owners and responsible departments. Teams responsible for remediation will communicate status and results to ISIRT at scheduled intervals.
Based findings or an assessment of incident size and complexity, the ISIRT may convenes one or more Post-Incident Review Teams (PIRTs). PIRTs will typically be converged only for large incidents, although exceptions may be made for complex or sensitive incidents.

- The ISIRT and PIRTs document and review findings from incident investigation, containment and resolution activities.
- ISIRT and PIRTs analyze conditions in the IT environment local to the incident, including technical, policy, and organizational aspects. Scope of review includes circumstances and activities before the incident as well as during the response.
- The ISIRT and PIRTs prepare an action plan for recommended changes to improve the university environment going forward.

- PIRTs document lessons learned, including aspects that were good as well as those which were problematic.

TECHNICAL ACTIONS

Specific technical review activities should include:

- Review whether remediation of affected local system(s) is complete.
  - Vulnerable hardware or software has been hardened against any break-ins, future attacks, or other security issues (e.g. installed patches, updated versions, replaced vulnerable sections of code).
- Conduct a root-cause analysis.
- Assess whether security vulnerabilities can be adequately remediated by making changes within the current environment or a new/replacement environment should be created.
- Take needed actions to restore essential systems to functioning status, either in the original or a repaired environment, or determine that the activities must cease or be suspended until a different or rebuilt environment can be created.
- Identify any areas where different technical measures would have prevented the breach or improved results in this environment. Also identify what technical measures worked well.
- Share lessons learned with appropriate contacts.

POLICY AND ORGANIZATION

Analyze sufficiency of policies and procedures, efficacy of organizational structure, and accountability of those who were involved, or should have been involved, in risk mitigation and in the response. Include internal and external environments and individuals who are staff, management and organizational leaders.

RECOMMENDATIONS AND NEXT STEPS

The ISIRT assesses findings and recommendations of the PIRT(s), and then issues a report of the incident and its response to the AVP of Information Security, including findings and recommendations.

DEFINITIONS

Denial of Service (DoS) - is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service (DDoS) is where the attack source is more than one–and often thousands of-unique IP addresses.

Enterprise system - the overall combination of computer hardware and software that the university uses to organize and run its operations. Enterprise systems provide core services used across the institution and on which other applications or business processes often are dependent.

ISIRT – Information Security Incident Response Team. Team responsible for assessment and investigation of a security incident involving university technology or data assets.

Malware - software that is intended to damage or disable computers and computer systems.

Phishing - is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, or other communication channels.

Social Engineering - is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

User system – combination of hardware or software that is used by single or multiple individuals to perform their daily duties.

CONTACT INFORMATION

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

RELATED LINKS

Data Governance & Classification
Information Security Incident Management and Response Policy
Information Security Incident Response Escalation Guideline

HISTORY

Issued: 01/23/2019