Data Security Incident Response Guide

UNIVERSITY OF CENTRAL ARKANSAS

1.1. Purpose

The Security Incident Response Team (IRT) has been established to provide a quick, effective and orderly response to security incidents such as virus infections, hacking activity, break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications.

The Incident Response Guide identifies and describes the roles and responsibilities of the IRT. The Incident Response Team is responsible for preparing and putting the plan into action. At a minimum, the response guide is intended to:

- Assess the nature and scope of an event or incident. Including but not limited to situation where information systems and personal information have been accessed or misused.

- Take appropriate steps to contain and control the event or incident to minimize further threats, including unauthorized access to, or use of, sensitive information.

- Ensure timely notification to appropriate federal regulatory agencies when UCA becomes aware of an incident involving unauthorized access to, or use of, sensitive information.

- Prevent or minimize disruption of UCA's critical services

1.2. Scope

The guidance contained in this document is generally focused at UCA's key Incident Response Teams and job roles, e.g. security teams, technical specialists, building support personnel and communications staff. However, the guidance is applicable to all employees, contractors, and others who process, store, transmit, or have access to IT information, infrastructure and computing resources, at all levels of sensitivity, whether owned and operated by UCA or operated on behalf of UCA. The IRT's mission is to prevent a loss of information assets, profits, or public confidence by providing an immediate, effective and skillful response to any unexpected event involving personal information, computer systems, networks or databases.

1.3. Distribution

This classification applies to information which cannot be considered PUBLIC due to the nature of the information, but is not of a sensitive nature that would require encryption (e.g., electronic distribution of the ISP), for this type of information, encryption is preferred but not required. Disclosure of RESTRICTED information requires a Non-Disclosure Agreement on file.

1.4. Criteria Used to Identify a Security Event

The identification of a potential or actual event can be made by a variety of parties, either internal or external to UCA (e.g. vendors, employees, regulatory agencies, etc.). An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a Web page, a user sending electronic mail, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, and include any security-related incident that may severely impact UCA's ability to continue normal operations such as:

- Information System failures and denial of service
- Identity theft
- Misuse and/or unauthorized use of system privileges
- Execution of malicious code that destroys data
- Disclosures of protected health information
- Incapacitation of key UCA facilities and/or infrastructure
- Breaches of confidentiality and integrity
- Other situations as defined by the Office of the President and the IRT

All events do not necessarily qualify as incidents. Section 4.4 "Using Problem Reporting" provides the guidance for determining when an event qualifies as an incident.
Regardless of the source or Priority of the event, it is essential that the incident is reported, logged and tracked through the use of the IT Help Desk Ticketing System (TDX) and UCA Information Security Team. This ensures that escalation and auditing processes occur as required.

1.5. Authority

The UCA IT Organization is tasked with the mission of developing policies and standards for providing adequate security for all UCA operations and assets.
The UCA Security Incident Response Team is authorized to take the appropriate steps necessary to contain, mitigate and resolve security incidents. The Information Security Director is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost effective manner and reporting findings to management and the appropriate authorities as necessary. UCA's Chief Information Officer serves as the IRT Coordinator.

1.6. Update Methodology

This document will be reviewed annually, and updated on an as needed basis.

2.1. Incident Response Team Membership Requirements

All UCA employees, from end users of UCA's networks to the executive management team, have responsibilities related to the security of UCA systems. Likewise, individuals contracted by UCA, by virtue of that employment, assume responsibility for the security of UCA systems.
Each of the following areas is required to have a primary and an alternate member identified as assignable to the Security Incident Response Team (IRT).

- IT Security
- Physical Security
- Finance
- Privacy
- Network Architecture
- Operating System Architecture
- Internal Audit
- Legal
- Corporate Communications and Public Relations
- Human Resources

2.2. General Responsibilities

In the course of everyday activities, employees and/or contractors may be the first to discover a situation that could adversely impact UCA. Both employees and contractors are tasked with:
- Securing UCA's critical information and systems in their possession or in the possession of their workgroups.
- Remaining apprised of security policy and procedures, as well as the common threats/vulnerabilities to UCA's processes.
- Participate in UCA sponsored security training and awareness programs.
- Reporting unusual behavior which may precede or indicate a security incident in progress.
- Report events and potential events as soon as possible to the UCA IT Information Security Director.

2.3. UCA Leaders

UCA leaders are responsible for ensuring that their employees are aware of the reporting procedures and the security policy in place to protect UCA information systems, employees and property. They also bear responsibility for:
- The overall security of their business operations, in consultation with the UCA Risk Management Organization.
- Adherence to all UCA security policy and procedures to minimize the likelihood of incident occurrence.
- Timely reporting of security concerns and incidents to either UCA's IT Information Security Director.

3.1. Incident Report Template

The report content and format standards outlined below must be followed when completing the Incident Response Report:

I. Executive Summary:

Provide overview of the incident
– Include risk level (High, Medium, Low) during forensic analysis
– Specify if compromise has been contained

II. Background

III. List of regulatory or industry standard such as PCI Status/HIPAA/FERPA

Based on findings identified on the forensic investigation, list non-compliant requirements (e.g. PCI, HIPAA, FERPA)

IV. Network Infrastructure Overview

Include a diagram of the network

V. Investigative Procedures

Include forensic tools used during investigation

VI. Findings

Type of information at risk:
Number of individual accounts at risk
Timeframe of individual accounts at risk
Timeframe of compromise and source of compromise
Identify any data exported by intruder.
Provide specifics on firewall, infrastructure, host, and personnel findings
Explain how incident occurred

VII. Compromised Entity Action

VIII. Recommendations

4.1. Internal Communication

In the event of an incident, the Office of the President, along with the IRT, is responsible for creating information bulletins for internal distribution. These bulletins will provide details of the incident and keep internal stakeholders informed of ongoing issues and status. The IRT will determine the frequency of these bulletins. Each UCA leader is responsible for sharing this information with his/her employees. The Office of the President will determine who will have the responsibility for distributing the internal bulletins and updates via the email system.

4.2. External Communication

In the event of an incident, the Office of the President is responsible for communication to external customers, business partners, the media, and other outside official parties. The Office of the President is also responsible for engaging advisory support with the external communications contacts as needed.

4.3. Conducting the Post-Implementation Review Meeting

Once an incident is resolved, the IRT will conduct a post implementation review meeting (also known as post mortem review). A post implementation review is a problem-solving technique to analyze an event and identify the root causes and any contributing factors to that problem. The goal of this meeting is to develop action plans with owners and target dates that assist in eliminating the problem or issue from recurring. The review meeting minutes, including action items and target dates, will be distributed to interested parties.

4.4. Reporting and Prioritization of Incidents

Incident Priority Levels

This section describes problem reporting and escalation procedures that are in effect during a security incident.

4.4.1. Handling of Incidents

Major Incidents cause serious interruptions of campus activities and must be resolved with greater urgency. Major incidents will result in the assembly of the UCA IRT to resolve the incident and communicate progress/resolution to key internal/external stakeholders.

The majority of events will be resolved by tickets opened up to the IT Help Desk or Information Security Team. Major Incidents support is required for those events that cannot be resolved by the IT Help Desk or Information Security Team and thus merit classification as an incident. Regardless of the source, and in every case, the problem is logged and tracked through the IT Help Desk to ensure that escalation and auditing processes occur as required.

4.4.2. Problem Status

From the time a problem is entered into the ticket support system (TDX) as a problem request, until the resolution and the request are closed, it contains a status. A problem status indicates the current status of the problem request, and can also indicate at what stage in the support flow the problem currently remains.

Problem Status Stages:

- New
- In Process
- On Hold
- Open
- Client Action Required
- Resolved
- Closed
- Canceled
- Reopened

4.5. Declaring an Incident

The Office of the President can declare an incident upon a recommendation from the CIO. Once an incident is declared, the CIO will hold a meeting with the IRT and other designated team members. The primary meeting location will be determined by the IRC and communicated appropriately.

During an incident the IRC will be responsible for:

• The IRC will contact IRT Members and inform them that UCA has declared a security incident and is mobilizing the IRT.

• The IRC Inform affected UCA leaders to contact their team and begin activation of their Security Incident Plans and provide the incoming phone numbers of the Command Center so they can reach the team if required.

• Determine where the permanent Security Incident Command Center will be located.

• Provide the Office of The President with status updates and recommendations. - Review the list and status of entities (both internal and external) requiring notice.

- Receive Office of the President approval to notify list of entities

4.6. Notifications

The Office of the President must approve the decision to notify external parties of a security incident.

UNIVERSITY OF CENTRAL ARKANSAS

5.1. Incident Response Guide Revision History

Date	Section	Description	Author ID
11/2/22		Original Document Provided	KEVINC
1/18/23	All	Wholesale changes based on discussions and input from both Kevin Carmical and Trevor Seifert.	TROACH

Last reviewed: April 1, 2024