UNIVERSITY
OF
CALIFORNIA

UCOP
ITS
Systemwide CISO Office
Systemwide IT Policy

UC Information Security Incident Response Standard

Revision History

Date:	By:	Contact Information:	Description:
06/05/18	Robert Smith	robert.smith@ucop.edu	Approved by the CISOs for consideration by ITLC and shared governance. Interim until approved by ITLC.
09/28/2018	Robert Smith	robert.smith@ucop.edu	Vocabulary changes made according to OGC suggestions.
08/21/2019	Robert Smith	robert.smith@ucop.edu	Updated to conform to style sheet.
10/3/19	Robert Smith	robert.smith@ucop.edu	Approved by ITLC.

Contents

1 Introduction

1.1 Background and Purpose

Information Security Incident response is a vital component of adequate cyber risk management. Recognizing that effective Incident response is a complex undertaking whose success depends on planning and resources, this Standard establishes the minimum requirements for a Location's Information Security Incident Response Program and the Information Security Incident Response Plan.

The primary focus of this Standard is to provide assistance to Locations and Units as they develop their Information Security Incident Response Plans. The secondary goal of this Standard is to guide Locations in developing their overall Information Security Incident Response Program.

The Incident response process outlined in this Standard encompasses four phases: Preparation; Detection and Event Analysis; Containment, Eradication and Recovery; and Post-Incident Activity. The dynamic relationship between those phases is highlighted in Section 3 below. These phases are defined in NIST SP 800-61 (Computer Security Incident Handling Guide). This Standard aligns with the NIST Cyber Security Framework.

Locations may extend their plans beyond this Standard to meet requirements for specific use cases, such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI), the European Union General Data Protection Regulation (GDPR), specific contracts and certain grants.

This Standard supports the systemwide Electronic Information Security Policy, IS-3.

1.2 Scope

This Standard applies to all Locations, Institutional Information and IT Resources of the University of California.

Because of the complex and varied mission of UC, Locations deal with a variety of Information Security Incidents. Incidents are divided into "Routine" and "Significant" for the purpose of this Standard. Although both are included, Significant Incidents are the primary focus of this Standard.

Routine Incidents are handled via Locations' local procedures.

1.3 Document Structure

Section 1: Introduction.

Section 2: Incident Response Governance Requirements.

Section 3: Overall Program Requirements.

Section 4: Location Information Security Incident Response Plan Requirements.

Section 5: Appendix - Roles and Responsibilities.

1.4 How to use this Standard

This Standard is intended to serve as a framework for Locations' Information Security Incident Response Program and Plan. Section 3 describes the requirements for the

Information Security Incident Response Program, which includes the response plan. Section 4 details the requirements for the plan specifically.

1.5 Definitions and Key Terms

Breach: The unauthorized acquisition, access, modification, use or disclosure of Institutional Information maintained by or for UC. Good faith acquisition of information by a UC Workforce Member for the purpose of supporting the mission of UC is not a breach of the security of the system provided that the information is not used for non-UC purposes or subject to further unauthorized disclosure.

Cyber Incident Escalation Protocol: A required process used to ensure that appropriate Incident communication occurs at the Location and from the Location to the UCOP cyber leadership team, UCOP supporting departments/functions and the Regents of the University of California. This process is related to, but separate from, the Location's Information Security Incident Response Plan.

Information Security Event (Event): An identified occurrence in a process, system, service or network state indicating a possible breach of information security policy, a possible breach of privacy policy, a failure of controls or a previously unknown situation that may be relevant to security. This also includes alerts and notifications.

Information Security Incident (Incident): (1) A compromise of the confidentiality (privacy), integrity or availability of Institutional Information in a material or reportable way, whether caused by unauthorized action or accident. (2) A single event or a series of unwanted or unexpected Information Security Events that have a significant probability of compromising business operations or threatening information security. Incidents are also called IT incidents, computer incidents, cyber incidents or security incidents.

Incident Communication Plan: A pre-scripted approach to informing others used to respond promptly, accurately and confidently during an emergency and in the hours and days that follow. The plan typically includes audiences, contract information, management contacts, law enforcement contacts, supplier contacts, the community, news media, responsible roles, approval processes, resources and scripted messages.

Information Security Incident Response Plan: The written document detailing the steps required to address and manage an Incident.

Information Security Incident Response Program: The full, comprehensive effort to prevent, prepare for and recover from Incidents. This includes, but is not limited to, these elements:

- The Information Security Incident Response Plan.
- Acquiring the necessary tools (software, hardware, communication) and supporting materials (e.g. safes, locking cabinets).
- Training.
- Establishing a formal Incident response capability and supporting communication strategies.
- Developing Incident response procedures.
- Establishing rules and procedures regarding Incident-related information sharing.
- Staffing the Incident Response Team (IRT).

- Determining which services the IRT can provide and which ones should be obtained from Suppliers.
- Establishing Supplier relationships and completing Supplier prerequisites.

Routine Incident: A regularly occurring and low-risk Incident that can be handled adequately through a repeating or triage process and does not require a larger Incident response.

Significant Incident: A higher risk Incident that represents a material violation of policy, a risk of data loss or a material impact to the confidentiality, integrity or availability of Institutional Information or IT Resources.

For more information about definitions, consult the IT Policy Glossary.

2 Incident Response Governance Requirements

2.1 Overview

This section describes the establishment and oversight governance structure of the required processes for Incident Response.

This section covers:

- Incident response overview and lifecycle.
- Handling Incident response.
- Defining Routine and Significant Incidents for the Location.
- Prioritizing Incidents.
- Appointing the Lead Location Authority (LLA).
- Appointing and convening the Incident Response Team (IRT).
- Following the UC Cyber Incident Escalation Protocol.
- Informing others about Incidents.
- Reporting Incidents.
- Testing the Location Information Security Incident Response Plan.
- Reviewing and updating the Location Information Security Incident Response Plan.

2.2 Information Security Incident Response Overview

The following swim lane diagram provides a high-level overview of the process outlined in this Standard.

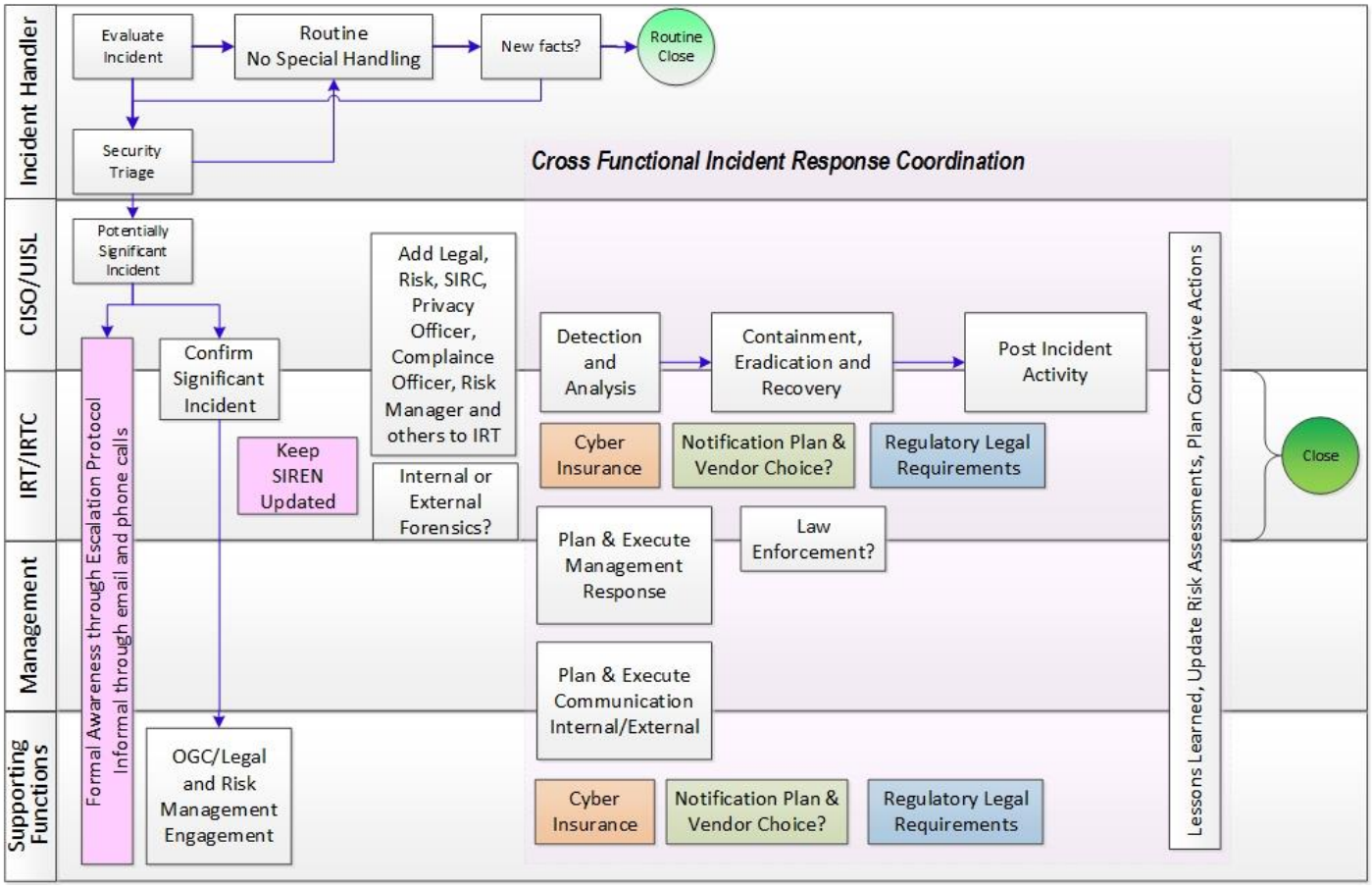

Figure 1

Information Security Incident Response Overview

2.3 Routine Incidents and Significant Incidents

The Location Information Security Incident Response Program must include provisions for Significant Incidents and Routine Incidents. The Lead Location Authority (or their designee) may determine when to convene an Incident Response Team (IRT).

Routine Incidents

For the purposes of guidance, characteristics of Routine Incidents include, but are not limited to:

- Common activity that can be handled with low risk, in a cost effective manner and that involves:
  - No prominent figures (e.g., celebrity, public official, university leader).

- Very low to no potential to lead to breach notification.
- Very low to no potential to lead to public notification (e.g., press releases, website announcements).
- Very low to no reputational impact related to the Incident.
- Very low to no regulatory risk.
- Very low to no impact to the ability to meet contractual obligations.

Routine Incidents require adequate documentation and evidence of resolution. "Adequate" documentation means the explanation will allow for later trending and analysis.

Significant Incidents

For the purposes of guidance, and in alignment with the Cyber Incident Escalation Protocol, characteristics of Significant Incidents include, but are not limited to:

- Incidents involving or likely to involve personally identifiable information (PII), information covered by breach notification laws/regulations or the General Data Protection Regulation's special categories.[1]
- Incidents affecting ten (10) or more individuals of any type.[2]
- Incidents involving legal, financial or human resource Units.
- Incidents requiring a press release or public notification, or about which media coverage is anticipated.
- Incidents that are likely to require breach notification to those affected due to state law, federal law or other regulatory regulations.
- Incidents likely to result in litigation or regulatory investigation.
- Incidents involving ransomware where paying ransom is contemplated.
- Incidents involving criminal or espionage activity likely to prompt the involvement of law enforcement.
- Incidents likely to result in the compromised integrity or loss of availability of Essential Systems.
- Incidents likely to result in material impact to Location operations.
- Incidents involving a prominent figure (e.g., celebrity, public official, university leader) at medical centers or Locations.
- Incidents involving key UC personnel, such as Location leadership, system leadership, Regents, police officers, prominent faculty or alumnae/i, etc.
- Other situations involving Institutional Information that is considered sensitive for a variety of reasons (e.g., political, cultural, religious).
- Measurable potential to lead to breach notification.
- Measurable potential to lead to public notification (e.g., press releases, website announcements).
- Measurable potential to lead to reputational risk related to the Incident.

[1] This regulation includes data that reveals a natural person's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership. It also includes the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health and data concerning a natural person's sex life or sexual orientation.

[2] Incidents involving fewer individuals may still be "significant" or "high-visibility" (e.g., those involving diagnoses, conditions or exposed data classified at Protection Level 3 or higher).

- Measurable potential to lead to regulatory risk.
- Any Incident with identified risks requiring notification of Location and/or senior management at the Office of the President using the UC Cyber Incident Escalation Protocol.

2.4 Incident Prioritization

Information Security Incident prioritization requires expert judgment. When there is doubt, Workforce Members must treat Incidents as Significant Incidents until data and analysis indicate otherwise.

UC uses a Low-Medium-High impact scheme for Significant Incidents:

- **Low** - Unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in minor damage, small financial loss or affect the privacy of a small group.
- **Medium** - Unauthorized use, access, disclosure, acquisition, modification, loss or deletion could: (a) result in moderate damage to UC, its students, employees, community or reputation; (b) conflict with the UC Statement of Privacy Values; (c) result in moderate financial loss; or (d) make legal action necessary. This impact level also includes lower-level impact items that, when combined, represent an increased impact.
- **High** - Significant fines, penalties, regulatory action, civil or criminal violations could result from disclosure. It could also cause significant harm to Institutional Information, major impairment to the overall operation of the Location or the impairment of essential service(s). This impact level also includes lower-level impact items that, when combined, represent an increased impact.

2.5 Lead Location Authority and Incident Response Team

The Cyber-risk Responsible Executive (CRE) is required to designate one or more people to fill the role of the Lead Location Authority (LLA). The LLA is required to be at a level high enough to allow that individual to speak with authority for the Location regarding Significant Incidents and to manage the Information Security Incident Response Program for the Location. The LLA occupies a functional role that is responsible for the oversight, investigation and determination of external notification for breaches of personally identifiable information or other reportable Incidents required by law, regulation or contract.

2.6 Convening the Incident Response Team

The Lead Location Authority or their designee will determine whether to convene an Incident Response Team (IRT) and will appoint the IRT Coordinator (IRTC).

2.7 Informing Others about Incidents

Cyber-risk Responsible Executive:

The CRE must ensure the Location follows the UC Cyber Incident Escalation Protocol.

Lead Location Authority:

The LLA must establish and document the Information Security Incident Communication Plan and delegate as needed, including:

- Noting communication used at the Location for Information Security Incidents.
- Reporting the Incident in the Systemwide Incident Escalation Report and Notification (SIREN) system and keeping SIREN up-to-date.
- Completing and submitting to c3@ucop.edu the document Reporting to Location Leadership - Roles and Responsible Party.
- During a potentially Significant Incident, consult the UC Cyber Incident Escalation Protocol for specific requirements regarding which Incidents are recorded in SIREN, when they are recorded, who reports to the next level in the organization and when the reporting occurs.

The LLA or their designee facilitates making the decision to notify law enforcement agencies (e.g., UC Police Department, Federal Bureau of Investigation, California Highway Patrol, Department of Homeland Security).

The LLA is responsible for consulting with Location leadership, Location Counsel and Compliance and Privacy to make the decision to notify affected individuals and/or regulatory agencies based on current laws, regulations or contracts requiring notification. The LLA must also consult UC systemwide and Location policy regarding breach notification and consider the risk of harm to the individuals impacted by the breach. In some cases, even though law may not require notification, it may be prudent to notify affected individuals.[3]

The LLA may designate Location resources and/or use the pre-approved notification vendors to notify affected individuals.

Unit Head:

Upon initial determination of an Incident, the Unit Head or their Unit Information Security Lead (UISL) must notify the CISO and/or the office designated by the Location.

Incident Response Team Coordinator:

The IRTC must:

- Consult with Location Risk Management/Services to determine eligibility and coordination of insurance coverage for the Incident.
- Ensure that resources are assigned to respond to the Incident.
- Inform the Privacy Officer/Manager of potential impact to privacy.
- Compliance Officer/Manager of potential impact to compliance.

The IRTC may designate IT Resources and/or use the pre-approved forensic vendors to conduct the forensic investigation and support the IRT.

The IRTC is responsible for ensuring that, if necessary, evidence is preserved and each Incident is adequately documented. “Adequate” documentation is defined as that which will stand on its own without requiring further explanation. The rationale to notify or not to notify must be clearly documented.

[3] See the UC Privacy Balancing Process: https://www.ucop.edu/ethics-compliance-audit-services/_files/compliance/privacy/privacy-balancing-process.pdf

2.8 Incident Reporting

The LLA must ensure that sufficient methods are available for reporting Information Security Events or Incidents. The LLA should consider:

- Anonymous reporting.
- Reporting by third parties.
- Reporting by Workforce Members.
- Reporting by other interested individuals (e.g., guests, customers, etc.).

2.9 Testing the Information Security Incident Response Plan

The LLA must ensure the Location's Information Security Incident Response Plan is tested at least once annually. Results from the test must be documented; gaps and corrections must be identified; and action items must be tracked to completion. Implementing the Information Security Incident Response Plan in response to an actual Incident is not considered a "test" for the purposes of this section.

2.10 Review and Update

The LLA must identify and assign Location roles responsible for the annual review of the Location Information Security Incident Response Plan. (See section 3.1.)

The CRE must approve the review of and any updates to the Information Security Incident Response Plan.

3 Overall Program Requirements

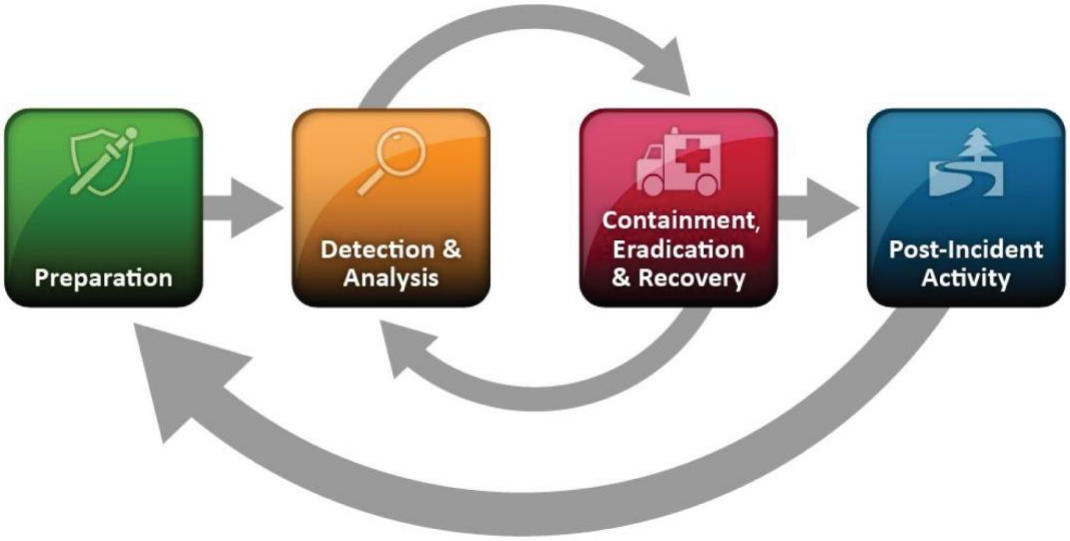

Figure 2

Incident Response Program Life Cycle

This section describes the establishment of the overall Information Security Incident Response Program.

This section covers:

- Preparation.
- Detection and Event Analysis.
- Containment, Eradication and Recovery.
- Post-Incident Activity.

The Location Information Security Incident Response Program must include documented evidence of the following steps.

3.1 Step 1: Preparation

The LLA must document and establish an Information Security Incident Response Program that encompasses the administrative and technical requirements outlined below.

- Administrative Details
  - Develop and update the Location Information Security Incident Response Plan and the Information Security Incident Response Program. Examples of updates include, but are not limited to:
    - Contacts, including changes in roles or assignments.
    - Noting trends in Routine Incidents that could indicate weaknesses in defense- and response-related controls and plans.

        - Integrating lessons learned from Significant Incidents and trends in Significant Incidents that could indicate weaknesses in defense- and response-related controls and plans.
        - Incorporating changes related to updates in this Standard.
        - Noting changes resulting from risk management processes.
        - Recording changes in the technical environment.
        - Documenting changes in the administrative environment.
        - Incorporating changes in law, regulation and policy.
        - Making note of any other changes needed to maintain the effectiveness of the plan.
    - Establish and execute distribution and notification methods for the Information Security Incident Response Plan and updates to the Incident Response Team roles.
    - Develop procedures for the Unit Information Security Leads (UISL) to document the collaboration of Unit Information Security Incident Response Plans (when they are used) with the Location Information Security Incident Response Plan or the Unit's initiation of the Location Information Security Incident Response Plan.
    - Establish procedures regarding Incident-related information sharing.
    - Staff the IRT.
    - Establish a cyber security training and awareness program. This training must:
        - Provide Workforce Members with general information security awareness education.
        - Explain how to report an Incident.
        - Provide directions for handling an Incident to Information Security Incident responders.
  - Develop procedures for handling Incidents.
  - Develop criteria for classifying Incidents that include the requirements of the systemwide Cyber Incident Escalation Protocol.
        - Include using the Low-Medium-High impact scale in the systemwide Cyber Incident Escalation Protocol.
  - Assemble a list of Suppliers who can assist in handling an Incident (e.g., Incident response, forensics, notification vendors).
  - Develop an Information Security Incident Communication Plan.
  - Complete a cyber incident escalation questionnaire and provide it to C3.
  - Establish record retention requirements for Institutional Information affected by an Incident in consultation with Legal, Compliance and Records Management.
  - Acquire necessary tools (software, hardware, communication) and supporting equipment (safes, locking cabinets, forensic laptops, forensic storage and cabling).
- Technical Details
    - Make sure inventories and classifications of Institutional Information and IT Resources are up-to-date.

- Develop, update and test plans for Incident prevention (e.g., tools and procedures focused on protecting Institutional Information and IT Resources from cyber attack and user error).
- Ensure detection measures are in place.
- Develop method(s) for reporting an Information Security Event or Incident (e.g., ServiceNow, email, web form, etc.).
- Locations must document the rationale used to establish which types of Incidents will be classified as Routine Incidents.

3.2 Step 2: Detection and Event Analysis

The LLA must document and establish an Information Security Incident Response Program that encompasses:

- Verifying that detection tools and processes are working as expected.
- Verifying that Institutional Information and IT Resources are properly protected.
- Designating the party responsible for detecting Significant Incidents.
- Verifying that Information Security Events are analyzed and Information Security Incidents are properly identified.

3.3 Step 3: Containment, Eradication and Recovery

The LLA must document and establish an Incident Response Program that encompasses:

- Establishing criteria for determining an appropriate containment strategy. Criteria may include:
  - Incident type and Incident severity.
  - Potential damage to Institutional Information and IT Resources.
  - Need for evidence preservation.
  - Service availability (e.g., data availability, network connectivity, services provided to external parties).
  - Time and resources needed to implement the strategy.
  - Effectiveness of the strategy (e.g., partial containment, full containment).
  - Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).
  - Possible side effects of containment.
- Identifying Suppliers or other UC Locations that can assist in containment, eradication and recovery.
- Verifying that backups and restores work as expected for Essential Systems.
- Verifying that fail-over or mirrored Essential Systems can be placed into production.
- Completing and updating business continuity plans related to Essential Systems.
- Reviewing forensic information to ensure that the Incident does not impact the ability to use backup or mirrored systems and Institutional Information.

3.4 Step 4: Post-Incident Activity

The LLA must document and establish an Incident Response Program that encompasses:

- Creating a documented process to capture lessons learned from responding to Significant Incidents.
- Creating a documented process to review the handling of Routine Incidents, their metrics and the effectiveness of planned defenses and responses.
- Updating the Location Information Security Incident Response Plan as needed.

4 Location Information Security Incident Response Plan Requirements

4.1 Overview

This section covers the specific requirements for the Location Information Security Incident Response Plan.

4.2 Incident Response Team (IRT)

The following is a list of roles, functional areas and individuals that make up the IRT during a Significant Incident. The specific demands of the Incident determine the Workforce Members' level of involvement. A Workforce Member may perform more than one role.

- Lead Location Authority (LLA).
- Chief Information Officer (CIO).
- IRT Coordinator (IRTC).
- Privacy Officer (may also serve as IRT Coordinator).
- CISO (may also serve as IRT Coordinator or LLA).
- Incident handlers.
- Legal Counsel - Location.
- Risk Management and/or Risk Services.
- Unit Head of affected department (Dean, Chair, Director, AVC, VC, etc.) or their designee.

These roles or functional areas may also be required on the IRT:

- Cyber-risk Responsible Executive (CRE).
- Information Technology.
- Records Management.
- Public Information Officer/Public Affairs.
- Government Relations/Legislative Liaison.
- Regulatory Affairs.
- Location Compliance Officer.
- Human Resources.
- Academic Personnel.
- UCPD, other state and/or federal law enforcement, as appropriate.
- Other executives, as appropriate.
- Internal Audit.
- Cyber-risk Coordination Center (C3).

These roles or functional areas may be secondary stakeholders in the Incident response process:

- UC Security Incident Response Coordination (SIRC).[4]
- Other executives, as appropriate.
- Information Sharing and Analysis Centers (ISACs).[5]

Note: These lists are not comprehensive. Other functions may be added as needed.

4.3 Consulting Counsel

The LLA must consult with Location Counsel and Location Counsel must consult with the UCOP Office of General Counsel about the Incident and how investigations will be conducted. In certain cases involving legal and/or regulatory risks, Counsel may direct the investigation for the purposes of providing legal advice.

4.4 Information Security Incident Response Plan Requirements

Locations or designated parts of the Location must develop a written Information Security Incident Response Plan that meets the requirements in this section.

1. Identify Incident Response Team members.
    a. Determine and assign roles.
    b. Describe responsibilities for a role's duties pertaining to Incident response.
2. Indicate when to use the plan.
    a. Define Significant Incident.
    b. Define Routine Incident.
3. Assign to a role the responsibilities of entering information into SIREN.
4. Create an Information Security Incident Communication Plan and identify how and when to use the plan. This will also address privacy Incidents.
5. Determine if Counsel should lead the investigation and Incident response. This review and determination should occur at an early stage of the Incident response process and be reviewed when new pertinent information arises.
6. Determine Location procedures for Incident handling (run-books, playbooks, etc.).
    a. Determine how to gather evidence for detection and analysis.
        i. Collect and review initial Incident logs and information.
    b. Conduct Incident prioritization.
        i. In the absence of accurate inventory and based on the risk associated with the event, the LLA and IRTC must treat the event as a Significant Incident during the initial triage.
    c. Document the Incident.

[4] https://www.ucop.edu/information-technology-services/initiatives/it-policy-and-security/uc-security-incident-response-coordination.html
[5] https://www.us-cert.gov/Government-Collaboration-Groups-and-Efforts

i. Use the Location reporting tool(s) (e.g., ServiceNow).

ii. Evaluate the initial information about the Incident using the Incident classification criteria.

iii. Incident characteristics:

1. Impact to Protection Level and Availability Level.
2. Number of records affected.

iv. Open a case in SIREN as needed for Significant Incidents.

v. Create other supporting documentation, which can include:

1. Meeting minutes.
2. Communication record.
3. Decisions log.

d. Include procedures for containment, eradication and recovery.

i. Identify and engage relevant expertise.

ii. Implement a containment strategy.

iii. Properly gather, handle and preserve evidence.

iv. Eradicate/remove the unauthorized tools used and the vulnerabilities present during the Incident.

v. Recovery.

e. Conduct forensic analysis.

i. Identify when to engage with forensic vendors/services.

f. Determine when to engage the UC Security Incident Response Coordination (SIRC).

g. Indicate when to engage supporting ISACs (e.g., National Health, Research and Education, Multi-State, etc.).

h. Explain when to engage with law enforcement.

i. UCPD.

ii. External law enforcement agencies.

iii. Coordinate California Department of Justice, California Highway Patrol, other states' law enforcement, FBI or other federal law enforcement engagement with UCOP's Systemwide CISO's office, c3@ucop.edu.

i. Identify when to engage research sponsors and/or partners.

j. Determine when to notify affected individuals and/or regulatory agencies.

k. Develop a process to identify and comply with short notification deadlines (e.g., evolving state regulations, the 72-hour deadline to notify regulators as required by the General Data Protection Regulation

(GDPR), the duty to notify certain federal contracting parties within one hour of discovery, the duty to notify payment card processors or merchant banks of certain payment card incidents within 24 hours, etc.).

7. Note how and when to account for special circumstances, such as:
    a. In the case of a suspected insider threat and/or when a particular Incident Response Team member is a person of interest, the Incident Response Coordinator, LLA or CRE will remove that person from the Incident Response Team.
    b. At the determination of the LLA, some individuals or teams may not lead investigations within their own areas of responsibility in order to avoid possible conflicts of interest.
8. Establish the process for coordination with:
    a. Location Counsel.
    b. UCOP's Cyber-risk Coordination Center (C3).
    c. UCOP's Office of General Counsel (OGC).
9. Develop a plan for post-Incident activity.
    a. Evaluate lessons learned.
    b. Report findings.
    c. Conduct Incident follow-up.
    d. Take required technical actions.
    e. Review procedures and team effectiveness.
    f. Develop recommendations and next steps.
10. Plan for periodic testing of the Information Security Incident Response Plan.

5 References

UC Policy

IS-3, III Section 16.1 Management of Information Security Incidents and corrective action

UC Standards

UC Institutional Information and IT Resource Classification Standard

External Resources

NIST SP 800-61 - Computer Security Incident Handling Guide - https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls – Section 16 Information security incident management

16.1 Management of information security incidents and improvements

16.1.1 Responsibilities and procedures

16.1.2 Reporting information security events

16.1.3 Reporting information security weaknesses

16.1.4 Assessment of and decision on information security events

16.1.5 Response to information security incidents

16.1.6 Learning from information security incidents

16.1.7 Collection of evidence

ISO/IEC 27035:2016 — Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management

ISO/IEC 27035:2016 — Information technology — Security techniques — Information security incident management, — Part 2: Guidelines to plan and prepare for incident response

6 Appendix A – Roles and Responsibilities

Role	Responsibility
Cyber-risk Responsible Executive (CRE)	Responsible for the appointment of the Lead Location Authority/Authorities (e.g., Campus LLA, Health LLA). Ensures that the Cyber Escalation Protocol is followed.
Lead Location Authority (LLA)	Responsible for the overall development, execution, improvement and maintenance of the Information Security Incident Response Plan and Program. Determines when to convene the IRT, appoints the IRTC and facilitates making the decision to notify affected parties.
IRT Coordinator (IRTC)	Responsible for assembling the Incident Response Team, capturing and documenting all the data pertinent to an Incident, communicating with appropriate parties, ensuring that the information is complete and reporting on Incident status both during and after the investigation.
Privacy Officer	Responsible for assessing privacy impacts and recommending what notification should occur, if any.
CISO	Responsible for assessing the impact of an Information Security Incident, the effectiveness of controls, the effectiveness of detection, the effectiveness of containment and recovery strategies and making recommendations for reducing/managing cyber risk.
Incident handlers	Responsible for containing the Incident, adjusting protective/detective tools and/or controls. Gathers and/or investigates technical details, documents the Incident investigation, determines root cause, obtains forensic evidence and preserves and analyzes evidence so that an Information Security Incident response can be brought to a conclusion.

Role	Responsibility
Legal Counsel - Location	The advisor on legal risks and obligations who serves as the liaison with OGC. Provides advice on the extent and form of all disclosures to law enforcement and the public. Makes determinations related to the scope and nature of investigations.
Risk Management and/or Risk Services	Responsible for assessing operational risks at the Location, implementing programs to reduce claims at the Location and filing cyber insurance claims.
Unit Information Security Lead	Responsible for ensuring a Unit has the technical controls, detection processes and response processes in place to address cyber security events and Incidents. See section 3 above. Supports IRT as required.
Unit Head	Responsible for ensuring that Unit resources and the Unit Information Security Lead support Incident response. In coordination with the IRTC, communicates with key stakeholders and sponsors or contracted parties.
Workforce Member	Every Workforce Member at UC has the responsibility to report immediately suspected or known unauthorized access of Institutional Information or IT Resources to the designated Unit Information Security Lead or the designated individual for their work area. This may be a local support person, an IT Help Desk, departmental management, compliance officer/department or similar function, as defined by the Location. Criminal acts, such as thefts or suspected criminal acts, must also be reported to campus police.