

UNIVERSITY OF CALIFORNIA

UC Santa Barbara CISO Office

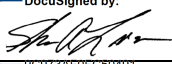
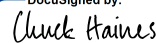
UC Santa Barbara Electronic Information Security Incident Response Plan

Emergency Contact Information:
email: security@ucsb.edu UC Santa Barbara Service Desk – (805) 893-5000 CISO, vacant – desk , mobile Associate CISO, [Kip Bates]– (805) 893-7393, mobile (805) 452-2735 Director of Security Operations, [Kevin Schmidt] – (805) 893-7779 SOC Manager, [Jennifer Mehl] – (805)-893-5080

Template Revision History

Date:	By:	Contact Information:	Description:
09/10/18	Robert Smith	robert.smith@ucop.edu	This is an IR Plan template created by UCOP for Locations to use.
9/26/19	Sam Horowitz	samh@ucsb.edu	Draft of UC Santa Barbara plan
5/1/2020	Sam Horowitz	samh@ucsb.edu	Version 1 released
7/30/2020	Sam Horowitz	samh@ucsb.edu	Minor revisions
12/31/2021	Sam Horowitz	samh@ucsb.edu	Minor revisions

Approvals

Date:	By:	Contact Information:	Signature/Approval Link
12/31/2021	Sam Horowitz CISO	(805) 893-5005	DocuSigned by: Sam Horowitz <small>51610A7D0676482...</small>
12/31/2021	Shea Lovan CIO	(805) 893-5533	DocuSigned by:  <small>9C973AFDFC50491...</small>
12/31/2021	Chuck Haines CRE	(805) 893-8541	DocuSigned by:  <small>686E8B2CC60B434...</small>

University of California - UC Santa Barbara
Incident Response Plan

University of California - UC Santa Barbara

Incident Response Plan

Table of Contents

1. Overview	4
2. Scope	4
3. General	4
3.1 Location Procedures: Preparation	4
3.1.1 Maintenance of the Plan	4
3.1.2 Testing	5
3.1.3 Appointment of Incident Response Team Members.....	5
3.1.4 Incident Categorization, Prioritization, and Use of Plan.....	7
3.1.5 Training and Reporting	10
3.1.6 Communication Plan	10
3.1.7 Confidentiality and Documentation	11
3.1.8 Conducting Investigations Under Attorney Client Privilege	11
3.1.9 Notification Requirements	12
3.1.10 Documentation.....	12
3.2 Location Procedures: Containment, Eradication, and Recovery	12
3.2.1 Relevant Expertise	13
3.2.2 Containment Strategy	13
3.2.3 Containment Procedure	13
3.2.4 Gathering, Handling, and Preserving Evidence.....	14
3.2.5 Notice, Notification and Regulatory Reporting	15
3.2.6 Eradication/Removal	15
3.2.7 Recovery	15
3.3 Location Procedures: Post-Incident Activity.....	16
3.3.1 Findings Report.....	16
3.3.2 Incident Response Plan Update.....	16
3.3.3 Root Cause Analysis and Trending.....	16
4. Appendix A – Information Security Incident Response Key Roles and Contact Information	17
5. Appendix B – Information Security Incident Summary and Checklist	19
6. Appendix C - Incident Handler - Cyber Incident Triage and Assessment Questions	26
7. Appendix D - Other Resources	27
7.1 Communication Plan	27
7.2 Information Security Incident Response Checklist	27
7.3 Notification letter samples	27
7.4 Pre-qualified Incident Response Suppliers	27
7.5 UC Incident Response Standard	27
7.6 NIST Computer Security Incident Handler Guide – SP 800-61 R2	27

University of California - UC Santa Barbara

Incident Response Plan

1. Overview

This document describes the overall plan for responding to Information Security Incidents at UC Santa Barbara. This Plan may also be used to handle other Incidents related to improper access or records generally. It defines the roles and responsibilities of participants, characterization of Information Security Incidents, reporting requirements, and relationships to other policies and procedures. The goal of the Information Security Incident Response Plan is to detect and react to Information Security Incidents, respond appropriately, determine their scope and risk, communicate the results and risks to appropriate stakeholders, and reduce the likelihood of reoccurrence.

This Plan outlines the general tasks for Incident Response (IR) and will be supplemented by specific Unit guidelines and procedures. Subject Matter Experts (SMEs) may also guide specific steps based on the nature of the Information Security Incident. UC requirements for an Incident Response Plan are detailed in the [Incident Response Standard](#).

Unit Workforce Members are often the first responders during an Information Security Incident and frequently make the determination that the Incident led to data loss. Determining the severity of data loss will result from the collaboration of the Unit/UIISL, the CISO's office, the Supplier (when involved), and forensic investigators.

2. Scope

This Plan applies to all IT Resources, all Institutional Information, all Units, and any Workforce Member accessing, or any device used to access, Institutional Information or IT Resources for any work or volunteer related purpose.

3. General

These are UC Santa Barbara applicable procedures for Information Security Incident handling. They are divided into three sections:

- Preparation and Communication;
- Containment, Eradication, and Recovery;
- Post-Incident Activity.

All additional plans or procedures that UC Santa Barbara Units create to meet their specific needs must be aligned with and support this Incident Response Plan.

3.1 Location Procedures: Preparation

3.1.1 Maintenance of the Plan

The Lead Location Authority (LLA) is responsible for the maintenance and updating of this Plan. The Plan must be reviewed annually and updated as needed after Incidents or material changes in the organization or operations. The CRE must approve the review of and any updates to the Information Security Incident Response Plan. See also the [Incident Respond Standard](#), Section 2.10.

University of California - UC Santa Barbara

Incident Response Plan

3.1.2 Testing

The Incident Response Team Coordinator (IRTC) is responsible for annual testing of the Incident Response Plan. Having to use the Plan for IR does not count as a test. Proper testing ensures that assigned Workforce Members are aware of their role in the process and well prepared for a potential event. It also allows UC Santa Barbara to improve its response effectiveness in a non-crisis period.

The IRTC must plan cyclical testing to:

- Ensure contact information is up-to-date.
- Ensure Workforce Members have access to tools and understand the Plan.
- Ensure the Plan matches changes in technology footprint.
- Ensure there are no material errors or omissions in the Plan and supporting documents.

3.1.3 Appointment of Incident Response Team Members

Please see the Incident Response Standard Section 4.2 for a list of roles and functional areas that may be included on the IRT.

Role	Name	Duties
Cyber-Risk Responsible Executive (CRE)	Chuck Haines chuck.haines@ucsb.edu (805) 893-8989	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)	Acting Associate CISO Kip Bates kip.bates@ucsb.edu (805) 893-7393	Accountable 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.
CISO	Acting Associate CISO Kip Bates kip.bates@ucsb.edu (805) 893-7393	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 makes recommendations regarding the reduction/management of cyber risk.

University of California - UC Santa Barbara

Incident Response Plan

Incident Response Team Coordinator (IRTC)	Jennifer Mehl jennifer.mehl@ucsb.edu (805) 593-5080	Responsible for assembling all the data pertinent to the Incident, serving as the project manager of the response, communicating with appropriate parties, ensuring that the information is complete, and reporting on Incident status both during and after the investigation.
Incident Response Handlers	Security Operations Center (security@ucsb.edu) Windows IRT – Roger Padilla (roger.padilla@ucsb.edu) Linux IRT – Ted Cabeen (ted.cabeen@lscg.ucsb.edu)	Workforce Members who gather, preserve, and analyze evidence so that an Incident can be brought to a conclusion.
Unit Information Security Lead (UISL)	To be assigned by campus Units	Responsible for ensuring a Unit has the technical controls, detection processes, and response processes in place to address cyber security events and Incidents. Supports the IRT as required.
Risk Manager	Ron Betancourt ron.betancourt@ucsb.edu (805) 893-5837	Responsible for assessing operational risks at the Location, implementing programs to reduce claims at the Location, and filing cyber insurance claims.
Counsel	Nancy Hamill Nancy.Hamill@ucop.edu (510) 987-9720	The advisor on legal risks and obligations who serves as the liaison with OGC. Advised on the decision to notify impacted or potentially impacted individuals and regulators. Provides advice on the extent and form of disclosures to law enforcement and the public. Makes recommendations related to the scope and nature of investigations.
Law Enforcement	Alex Yao	Liaison with UCPD and outside law enforcement and UCOP Law

University of California - UC Santa Barbara

Incident Response Plan

Coordinator	alexiao@ucsb.edu (805) 893-4151	Enforcement Coordinator (e.g., FBI, Secret Service, CHP, local police departments).
-------------	------------------------------------	---

The IRTC, LLA, or CRE may remove Workforce Members from the Incident Response Team under special circumstances, such as:

- Suspected insider threat.
- When a particular Incident Response Team member is a person of interest.
- Internal Audit requests the removal.

At the determination of the LLA, some Workforce Members or teams may not lead investigations within their own areas of responsibility in order to avoid possible conflicts of interest.

3.1.4 Incident Categorization, Prioritization, and Use of Plan

IS-3 categorizes Information Security Incidents as either Significant or Routine. According to the [Incident Response Standard](#), a Significant Incident is “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.” A Routine Incident is “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.”

Under this Plan, the following are categorized as Routine Incidents:

- Incidents involving no prominent figures (e.g., celebrities, public officials, university leaders).
- Incidents involving very low to no potential to lead to notification of (possibly) affected individuals.
- Incidents involving very low to no potential to lead to public notification (e.g., press releases, website announcements, regulators).
- Incidents involving very low to no reputational impact related to the Incident.
- Incidents involving very low to no regulatory risk.
- Incidents involving very low to no impact to the ability to meet contractual obligations.
- Incidents that do not show any of the characteristics of a Significant Incident.

Typical examples of Routine Incidents are:

- Password resets/account lockouts with no other indicators of compromise.
- Lost or stolen phones managed by IT.
- Endpoint malware alerts involving no P3 or P4 Institutional Information that is present or processed.

University of California - UC Santa Barbara

Incident Response Plan

- Isolated DMCA alerts.
- Ransomware on a single device affecting no P3 or P4 Institutional Information.
- Ransomware on a single device affecting no A3 or A4 Institutional Information.
- Misrouting of information affecting 10 or fewer people and not involving Institutional Information classified at P4 (e.g., FAX sent to the wrong number, e-mail sent to the wrong recipient).
 - In this case, the Privacy Officer must be notified.

Under this plan, the following are categorized as Significant Incidents:

- Incidents involving or likely to involve personally identifiable information (PII), information covered by notification laws/regulations, or the General Data Protection Regulation's special categories.
- Incidents of any type affecting ten (10) or more individuals.
- Incidents involving legal, financial, or human resource Units.
- Incidents requiring a press release or public notification, or about which media coverage is anticipated.
- Incidents likely to require notification to those affected due to state law, federal law, or other regulatory requirements.
- Incidents likely to result in litigation or regulatory investigation.
- Incidents involving ransomware that include the contemplation of paying ransom.
- Incidents involving criminal (e.g., espionage, financial fraud, theft, sabotage, defacement, etc.) activity likely to prompt the involvement of law enforcement.
- Incidents likely to result in the compromised integrity or loss of availability of Essential Systems or IT Resources classified at Availability Level 3 or 4.
- Incidents likely to result in material impact to Location operations.
- Incidents involving a prominent figure (e.g., celebrity, public official, university leader).
- 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 reputational risk related to the Incident.
- Any Incident with identified risks requiring notification of Location senior management using the UC Cyber Incident Escalation Protocol.

Typical examples of Significant Incidents are:

- Ransomware on multiple IT Resources when the ransomware originates from a single or related Information Security Incident.

University of California - UC Santa Barbara

Incident Response Plan

- Webserver or file server compromises that involve malware insertion or unauthorized access that goes undetected for a period of time.
- Database compromises that involve any unauthorized access that is undetected for a period of time.
- Any Incident involving designated Critical IT Infrastructure (e.g., IAM, DUO, core networking equipment, etc.).
- Any Incident involving cash, banking, or investment management IT Resources.
- Any Incident involving the attempted or successful theft/compromise of any financial instrument, purchase order, or payment fraud through any electronic means.
- Loss or theft of any IT Resource containing more than ten (10) records of Institutional Information classified at P3.
- Loss or theft of any IT Resource containing any Institutional Information classified at P4.
- Incidents reported by outside law enforcement agencies (e.g., FBI, CHP, HHS, Secret Service, DHS).
- Incidents likely to require notification to individuals, government regulators, or third parties.
- Any other Incident designated significant by the Unit Head or UISL.

Use of the this plan

Use of this Incident Response Plan is required for all Significant Incidents. For Routine Incidents, certain steps or requirements do not apply. Established process for Routine Incidents should be followed.

The ITRC and other Workforce Members must consider all Information Security Incidents potentially Significant Incidents until evidence indicates otherwise.

Mechanisms

UC Santa Barbara uses automated or semi-automated mechanisms to support handling Routine Incidents.

UC Santa Barbara may use automated mechanisms to support handling Significant Incidents. These include dynamic reconfiguration or blocking as part of the IR capability.

Prioritization

Prioritization is vital to successful Incident Response. Knowing the severity of an Information Security Incident and the proper steps to take can improve response time, the effectiveness of the response, and the speed at which a Unit recovers.

Incident prioritization must follow the Low/Medium/High impact scheme, detailed below. For more information, see the [Incident Response Standard](#), section 2.4.

- **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 result in: (a) moderate damage to UC, its students,

University of California - UC Santa Barbara

Incident Response Plan

employees, community, or reputation; (b) conflict with the UC Statement of Privacy Values; (c) moderate financial loss; or (d) rendering 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, or 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.

3.1.5 Training and Reporting

The LLA and Workforce Managers must ensure that UISLs and Workforce Members in Information Technology positions training regarding the use of this plan occurs at the time of hire, at the time of any new assignment, and at least annually after the date of hire.

Updates to training materials must occur periodically and include lessons learned from managing Information Security Incidents.

The LLA must ensure that Workforce Members know how to report an Information Security Incident.

3.1.6 Communication Plan

Proper communication regarding Incidents, their severity and their effects is vital during IR.

The LLA has the responsibility of overseeing the Incident Response Communication Plan and delegating responsibilities to the appropriate role or individual.

The LLA is responsible for consulting with Location leadership, Counsel, and the Compliance and Privacy Office when making decisions regarding notification.

The communication process must take into account the severity of the Incident and its potential impact.

If widespread email compromise is possible or suspected, use out-of-band communication options (alternate e-mail, Signal, SMS messaging, etc.).

Reporting Tools

Reporting tools are crucial to proper communication concerning any Incident.

- SIREN is a tool for reporting Incident information. The Workforce Members responsible for entering information into SIREN are:
 - CISO [vacant],
 - Becky Steiger, beckysteiger@ucsb.edu, (805) 893-4118
 - Shea Lovan, salovan@ucsb.edu, (805) 893-5533

And the backup contacts are:

- Doug Drury, doug.drury@ucsb.edu, (805) 893-5036
- Kevin Schmidt, kps@ucsb.edu, (805) 893-7779

University of California - UC Santa Barbara

Incident Response Plan

- o Kip Bates, kip.bates@ucsb.edu, (805) 893-7393

3.1.7 Confidentiality and Documentation

Workforce Members must keep the aspects of an unfolding Information Security Incident confidential. Some guiding rationale includes:

- The understanding of an Incident often evolves as an investigation progresses.
- The specific language used during an Incident is easily misunderstood and misquoted. For example, the words “breach” and “incident” are often informally used interchangeably, but “breach” is a legal determination made after counsel reviews an Information Security Incident.
 - o What constitutes a data breach is often not intuitive and any initial analysis of the Incident is tentative, conditional, and subject to revision. The IRT must use the term “Information Security Incident” or “Incident.” Counsel will make legal determinations.
- In situations involving law enforcement, public disclosure of even the existence of a possible Incident could hamper the investigation.

When responding to an Incident or preparing documentation, Workforce Members must:

- Stick to the facts.
- Avoid speculation.
- Limit distribution to the IRT or subgroups.
- Not post to social media.
- Not communicate with the media.
- Direct any inquiries to Communications.
- Direct any inquiries from law enforcement to Chief James Brock, james.brock@police.ucsb.edu, (805) 893-4151

3.1.8 Conducting Investigations Under Attorney Client Privilege

Counsel will direct some investigations. Investigations led by Counsel are “confidential communications between attorneys and their clients made for the purpose of obtaining or providing legal advice.”

Counsel

UC Santa Barbara Office of General Counsel (OGC) must determine if Counsel will lead an investigation under attorney client privilege.

Once OGC makes the decision to lead the investigation, the IRTC must complete the [Section 5 Appendix B – Information Security Incident Summary and Checklist](#) as soon as practical and submit it to:

- Nancy Hamill, Nancy.Hamill@ucop.edu, (510)-987-9720

University of California - UC Santa Barbara

Incident Response Plan

The following information regarding the role of Counsel in the investigation is required. The IRTC must note:

- If Counsel is leading the investigation.
- If so, the precise date of this decision.
- If so, who made this decision.
- If so, any subsequent changes to the role of Counsel.

OGC or their designated representative will advise the IRT on the obligations of maintaining attorney client privilege.

3.1.9 Notification Requirements

The IRTC, with the support of the UISL, will work with Counsel to determine notification requirements for the Institutional Information involved (or suspected to be involved) in the Incident.

Within 24 hours of the identification of a Significant Incident, the IRTC must have an initial consultation with Counsel about potential notification requirements.

Note: UC operates under a wide range of state, federal, and international regulations. Many contracts also have notification requirements (e.g., grants, research agreements, data sharing agreements, Payment Card Industry agreements, etc.) that may inform decisions regarding notification.

3.1.10 Documentation

The IRT must document not only information about the event, but also details concerning communication, classification, and the resources or services affected. From the moment the IRT forms, details must be documented and the LLA must allocate appropriate resources to ensure adequate and thorough documentation.

It is crucial to note that document authors must focus on the facts of the Information Security Incident. Authors must not speculate or offer opinions. Incidents can evolve quickly as investigations progress and the record must demonstrate the progression. All details must show fact-based findings.

Appropriate documentation is vital for legal consultation and also helpful for post-recovery discussion as it can guide strategies for improvement.

UC Santa Barbara uses the following tools as systems of record:

1. UC Santa Barbara RT in the SOC and similar IT response/ticketing systems used in divisions and departments.
2. UC's SIREN.
3. UC Santa Barbara Google Drive (or Box if the Incident impacts Google Drive).
 - a. Text, DOCX, XLSX, PPTX, JPEG, and other common document formats are acceptable forms of storage.
 - b. The IRTC may also approve some forensics tools that produce proprietary formats.

3.2 Location Procedures: Containment, Eradication, and Recovery

University of California - UC Santa Barbara

Incident Response Plan

3.2.1 Relevant Expertise

The LLA must maintain the list of individuals, Units, and other entities that are qualified to assist in IR. See Section 4 of [Key Roles and Contact Information](#).

In large or complex cases, other UC Locations or third-party entities may be needed to determine scope and accurately triage response. The IRTC must keep a record of people and roles added to a particular IR.

UC maintains contracts with Incident Response Suppliers who specialize in forensics and notification. The lists of pre-qualified Suppliers are found here:

<https://ucop.box.com/s/b32sahonlf6u752xqh3ig8lyxyt5cpyf>

(With access to Box: All Files > UCOP IT Policy and Implementation > Incident Response Plan.)

3.2.2 Containment Strategy

Containment strategy is fundamental to IR because it prevents an attack from increasing in severity. The IRTC and UISL must ensure that appropriately trained responders effectively contain any attack, preventing it from spreading or causing further disruption to safety, security, and/or business functions.

The IRTC, UISL, CISO, and LLA must consult UC Santa Barbara senior leadership (e.g., CIO, Executive Vice Chancellor, Vice Chancellor for Administration, Vice Chancellor for Student Affairs, Vice Chancellor for Research) to determine the extent to which services can or should be disrupted in the process of containment. Containment involves both technical controls (e.g., system disconnects, power-down, etc.) and administrative controls (e.g., curtailing services, limiting access, etc.).

For Critical IT Infrastructure and IT Resources processing Institutional Information classified at Protection Level 3 or higher and IT Resources classified at Availability Level 2 or lower, complete forensics may be more important than restoring availability. Decisions regarding prioritization should take this into account.

For all other IT Resources, restoring availability can, but need not, take priority over forensics, provided the method(s) of compromise is/are preventable.

3.2.3 Containment Procedure

UC established the following four-step containment procedure for the IRT to follow:

1. Containing the Significant Incident: remove any networking cables or virtual networks and/or disable any wireless connectivity balancing Availability Level classification with the nature of the Incident. Seek Unit Head approval if possible, but prioritize containment over Availability unless expressly directed otherwise.
 - Use [Section 6. Appendix C - Incident Handler - Cyber Incident Triage and Assessment Questions](#) to complete an initial assessment. This assessment must be promptly shared with the IRTC and UISL.

University of California - UC Santa Barbara

Incident Response Plan

- If Incident Handlers suspect the presence of Institutional Information Classified at Protection Level 3 or higher, immediately alert the UC Santa Barbara Security Office at security@ucsb.edu. Use the phone to contact a member of the security team—see also the [first page](#) of this document.
2. Continue with the assessment of the Significant Incident: work with the primary Unit Information Security Lead (UISL), the user or individual responsible for determining the nature of the IT Resource(s) and Institutional Information, and complete [Section 5 Appendix B – Information Security Incident Summary and Checklist](#) . If the analysis shows that no Institutional Information classified at Protection Level 3 or Protection Level 4 exists on the IT Resource **and** no administrative credential was compromised, then proceed with recovery (rebuild/restore and remediate) and close the Information Security Incident.

If the analysis increases the suspicion that Institutional Information classified at Protection Level 3 or Protection Level 4 exists (or may exist) on the IT Resource OR an administrative credential was compromised, move on to:

1. Collect forensic evidence as required, see Section 3.2.4.
2. Contact the security office at security@ucsb.edu as a form of escalating the Information Security Incident. At that point, the Security Office will activate the IRT and the IRTC will lead the IR.

In emergency situations, it may be necessary to disconnect the Location from the Internet or turn off services/subnets. If possible, the IRTC must confirm this step with the LLA and CISO before taking action.

3.2.4 Gathering, Handling, and Preserving Evidence

Forensic Analysis

When analyzing data, the IRT should report only verifiable information, focusing on precision and detail.

Workforce Members must generally keep the system running until an Incident Handler can examine it.

The preferred strategy is: remove the network cable and/or network connectivity, and take no other action.

Except for triage steps necessary to prevent further damage, the system operator or administrator should take no corrective or investigatory actions, except under the direction of the Incident Handler. This helps preserve forensic evidence of unauthorized activity on the system.

Depending on the current level of risk, some immediate actions may be required. If other systems or accounts are at risk, then compromised systems should be physically disconnected from the network or otherwise prevented from posing a threat to other systems.

Evidence Collection vs. SLA-Uptime Preservation

University of California - UC Santa Barbara

Incident Response Plan

The goal of Incident Response is to reduce and contain the scope of an Information Security Incident and to ensure that IT Resources are returned to service as quickly as possible. Rapid response is balanced by the possible requirements to:

- Collect and preserve evidence in a manner consistent with the requirements of rules 26-34 of the Federal Rules of Civil Discovery;
- Abide by legal and administrative requirements for documentation and chain of custody.

The IRTC or their designee must maintain and disseminate procedures documenting how to perform evidence preservation. As technologies change, the IRTC or their designee will regularly adjust/update those procedures.

Units may have operational-level agreements with the customers they serve. The process of evidence collection should be balanced with the impact on SLAs.

The IRTC and the UISL will cooperate to ensure that downtime is minimized.

However, the LLA and CISO can prioritize the investigation activities involving significant risk, and may result in temporary outages or interruptions.

3.2.5 Notice, Notification and Regulatory Reporting

The LLA is responsible for making the decision to notify affected individuals in consultation with the:

- CRE;
- Privacy Manager;
- Compliance Director/Manager;
- Counsel;
- CISO.

The LLA is responsible for following the Cyber Incident Escalation Protocol.

The Director of Compliance is responsible for making the decision to notify regulatory agencies and/or government contracting officers in consultation with the:

- LLA;
- CRE;
- Privacy Manager;
- Counsel;
- Export Control Manager/Officer;
- CISO.

3.2.6 Eradication/Removal

Once the environment is stabilized and the threat contained, the IRTC, working with the IRT Members, should initiate eradication/removal. The IRTC and UISL must assess how to remediate and correct potential security vulnerabilities before IT Resources are placed back online.

3.2.7 Recovery

University of California - UC Santa Barbara

Incident Response Plan

Recovery involves the thorough remediation of affected IT Resources. Hardening or remediation is required to reduce the risk of attack on vulnerable hardware or software.

Credentials may need to be reset or monitored to prevent additional Information Security Incidents.

The IRTC must determine the need for continuous monitoring or the creation of a new environment to ensure improved security.

3.3 Location Procedures: Post-Incident Activity

3.3.1 Findings Report

The IRTC must create a Findings Report that will guide analysis of the likely cause of the Incident. The Report can then inform decisions regarding follow-up action, technical actions, procedural review, and recommendations for improvements.

The CISO and UISL must review the Findings Report within 45 days of issuance and take appropriate follow-up action using a risk-based approach.

3.3.2 Incident Response Plan Update

The IRTC and LLA must update this plan to correct any problems or shortcomings found during the Information Security Incident response or noted in the Finding Report. Updates must also include lessons learned.

The IRTC must review and, if necessary, update contact information at least quarterly or when members of the IRTC change or their contact information changes.

Plan updates must also occur after the regular testing of the plan, as described in section 3.1.2.

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

3.3.3 Root Cause Analysis and Trending

The CISO must review the Findings Report and then make needed adjustments to risk assessments, Risk Treatment Plans, and/or control implementation to manage the risks/problems/trends noted in the Findings Report.

The LLA and CISO must review trends of Routine Incidents and Significant Incidents to determine if preventative and detective controls are operating well. They must also make adjustments according to the findings of their review/assessment.

University of California - UC Santa Barbara

Incident Response Plan

4. Appendix A – Information Security Incident Response Key Roles and Contact Information (emergency contact information is available on the UCSB emergency contact card distributed each quarter to campus leadership)

Role	Name	Phone	E-mail	IRT Member
Lead Location Authority	CISO [vacant] – Kip Bates (acting)	(805) 893-7393	kip.bates@ucsb.edu	Extended
CRE	Chuck Haines	(805) 893-8541	chuck.haines@ucsb.edu	Extended
CIO	Shea Lovan	(805) 893-5533	salovan@ucsb.edu	Extended
CISO	Vacant – Kip Bates (acting)	(805) 893-7393	kip.bates@ucsb.edu	Core
Associate CISO	Kip Bates	(805) 893-7393	kip.bates@ucsb.edu	Core
Campus Privacy Officer	Becky Steiger	(805) 893-4118	beckysteiger@ucsb.edu	Extended
Incident Handler	Security Operations Center	--	security@ucsb.edu	Core
SIRC Member	Todd Atkins	805-893-5077	todd.atkins@ucsb.edu	Core
SIRC Member	Kevin Schmidt	805-893-7779	kps@ucsb.edu	Core
SIRC Member	Jennifer Mehl	(805) 893-5080	jennifer.mehl@ucsb.edu	Core
SIRC Member	Libby Whitt	(805) 893-6005	lwhitt@ucsb.edu	Core
Linux SIRC	Ted Cabeen	(805) 893-4378	ted.cabeen@lscg.ucsb.edu	Extended
Windows SIRC	Roger Padilla	(805) 893-4863	roger.padilla@ucsb.edu	Extended
UISL	<i>assigned per Information Security Incident</i>			Core
Unit Head	<i>assigned per Information Security Incident</i>	--	--	Core
Communications	John Longbrake	(805) 893-2191	john.longbrake@ucsb.edu	Extended
Compliance	Becky Steiger	(805) 893-4118	beckysteiger@ucsb.edu	Extended
Counsel	Nancy Hamill	(510) 987-9720	nancy.hamill@ucop.edu	Extended
Cyber Coordination (C3)	<i>assigned per Information Security Incident</i>			Extended

University of California - UC Santa Barbara

Incident Response Plan

Role	Name	Phone	E-mail	IRT Member
Export Control	Brian McCurdy	(805) 893-3787	mccurdy@research.ucsb.edu	Extended
Law Enforcement Coordinator	Chief Alex Yao	(805) 893-4151	alexiao@ucsb.edu	Extended
FBI Cyber				Extended
UCPD	Chief Alex Yao	(805) 893-4151	alexiao@ucsb.edu	Extended
Risk Manager	Ron Betancourt	(805) 893-5837	ron.betancourt@ucsb.edu	Extended
UC IT Security Committee	Listserv	NA	ltseccomm-l@listserv.UCOP.edu	Extended
UC Security Incident Response Coordination (UCSIRC)	Listserv	NA	ucsirc-l@listserv.UCOP.edu	Extended

For help with any Security Incident: security@ucsb.edu (UC Santa Barbara internal security team).

University of California - UC Santa Barbara

Incident Response Plan

5. Appendix B – Information Security Incident Summary and Checklist

Initial Assessment Check List

Make an initial assessment of the severity of the Information Security Incident. This will guide triage efforts.

A useful technique is to retrieve from the connections logs, syslog/security log data, and packet captures (pcaps) between the targeted systems and the attacking hosts. Other sources of information may include system logs, forensic data from the attacked hosts, and reports from other sites.

Security Incident Summary

Name of Workforce Member Filling Out This Appendix	
Phone Number of Workforce Member Filling Out This Appendix	
E-mail address of Workforce Member Filling Out This Appendix	
Unit Name	
Unit Information Security Lead Name	
Unit Head Name	
Was the Incident entered in SIREN?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Date This Template Was Filled Out or Updated	
IT Resources/Database/System Name	
Protection and Availability Level Classification	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> A1 <input type="checkbox"/> A2 <input type="checkbox"/> A3 <input type="checkbox"/> A4 Or <input type="checkbox"/> Critical Infrastructure
Does the potential exist for embarrassment to UC?	
Purpose/Use of Database/System	
Hyperlink to Database/System (if applicable)	
IP address(es) to IT Resources	

University of California - UC Santa Barbara

Incident Response Plan

Estimate of number of records potentially impacted	
Summarize what is known about the Significant Incident	
IP address(es) of attacker	
Platform (including release and patch level)	
Were root or administrative privileges acquired?	
How many other accounts may have been compromised?	
What was the sequence of events?	
What is the current level of risk?	
What is the potential or actual rate of Information Security Incident spreading?	
Scope of the attack	
Potential damage from the attack	
Preliminary forensic evidence	

Records about people or organizations

Please indicate if the database/system contains information on the following types of persons/entities:	Place an "X" in the correct column	
	No	Yes
Patient		
Guarantor (Other than Patient)		
Staff		
Faculty		
Student and/or Resident at the University		
Research Subject		

University of California - UC Santa Barbara

Incident Response Plan

Please indicate if the database/system contains information on the following types of persons/entities:	Place an "X" in the correct column	
	No	Yes
GDPR Data Subjects		
Alumni or donors		
Marketing prospects or other communication targets		
Other (e.g., Research Sponsors, Suppliers, Volunteers)		
<input type="checkbox"/> Research Sponsors <input type="checkbox"/> Suppliers <input type="checkbox"/> Volunteers <input type="checkbox"/> Other: _____		

Record Contents

Please indicate if the records contain the following information:	Place an "X" in the correct column(s)									
	Patient	Guarantor	Staff	Faculty	Student Or Resident	Research Subject	GDPR Data Subject	Alumni Donor	Marketing Prospects	Other
Name (First, Middle, and/or Last Name or Initials)										
Street Address										
Phone Number or E-Mail Address or personal URL										
Medical Record Number										
Social Security Number (last four digits only)										
Social Security Number (full or partial, other than just last 4 digits)										
Medicare ID Number										
Other Government Identifier (e.g., passport number, driver's license number)										

University of California - UC Santa Barbara

Incident Response Plan

Please indicate if the records contain the following information:	Place an "X" in the correct column(s)									
	Patient	Guarantor	Staff	Faculty	Student Or Resident	Research Subject	GDPR Data Subject	Alumni Donor	Marketing Prospects	Other
Health Insurance Information (e.g., insurance policy number, health plan beneficiary number, claims history, any other identifier used to identify an insured)										
Medical Information (e.g., diagnosis/condition; lab/test results; medications; treatment notes; genetic information; treatment date, discharge date, or other dates of service; claims history)										
FERPA covered information (e.g., exam scores, counseling records, grades, etc.); (Non -directory information)										
Financial Information (e.g., financial account number; credit or debit card number; PIN, password, or other information that allows access to or use of a financial account, etc.)										
Automated License Plate Recognition System information										
GDPR data subject or personal identifiers (e.g., name; identification number; location data [Address, GPS, etc.]; online identifier [handle, e-mail]; one or more factors specific to one's physical, physiological, genetic, mental, economic, cultural, or social identity; online identifiers provided by devices, applications, tools, and protocols, such as internet protocol addresses, cookie identifiers, or other identifiers, such as radio frequency identification tags; behaviors; and any information relating to an identifiable person who can be directly or indirectly recognized/known in particular by reference to an identifier)										

University of California - UC Santa Barbara

Incident Response Plan

Please indicate if the records contain the following information:	Place an "X" in the correct column(s)									
	Patient	Guarantor	Staff	Faculty	Student Or Resident	Research Subject	GDPR Data Subject	Alumni Donor	Marketing Prospects	Other
GDPR special identifiers (e.g., racial or ethnic origin; political opinions; religious/philosophical beliefs; trade union membership; genetic data; biometric data; health-related data; sex life/sexual orientation; criminal convictions and offenses)										
User Credentials (e.g., username or email address in combination with a password or security question and answer that would permit access to an online account)										
Administrative credentials (e.g., username or email address, in combination with a password or security question and answer that would permit access to an online account)										
Biometric Identifier (e.g., Fingerprint, Voiceprint, or full-face photos and related geometric expression)										
Digital Signature (i.e., algorithm used to validate authenticity of an electronic document or message)										
Other Direct Identifiers (e.g., tracking ids, cookies, URL, IP addresses, etc.) for records not covered by GDPR										
Driver license or other government information or images										
Passport information or images										

University of California - UC Santa Barbara

Incident Response Plan

Other Records Requiring Special Consideration or Handling

Please indicate if the records contain the following information:	Place an "X" in the correct column	
	No	Yes
"Controlled Information" Subject to UC/USA Export Control or Restricted Parties Policies		
Institutional Information covered by Export Control or Restricted Parties regulations (e.g., ITAR, OFAC, etc.)		
"Controlled Unclassified Information" (CUI) subject to contract requirements		
Information from Dual Use Research of Concern		
Information from Research Involving Select Agents		
Human subject research protocols or test methods		
Animal research protocols or test methods		
Research Sponsors' Confidential or Proprietary Data (Including Protocols, Case Report Forms, and Other Research Manuals)		
Security Risk Assessments or similar reports documenting vulnerabilities in cybersecurity infrastructure		
Architecture diagrams, network maps, source code, or other materials that would aid an attacker or compromise information security		
Information documenting vulnerabilities in physical plant/infrastructure		
Environmental Health & Safety (EH&S) Information (including information about receipt, processing/use, storage, or disposition of biohazards, radiation, or other dangerous materials; or about identification/remediation of non-containment events)		
Payment Card Numbers (debit card numbers, credit card numbers, payment card security codes, bank account or other financial account numbers and/or PINs)		
Other Institutional Information Classified at Protection Level 3 Describe: _____		
Other Institutional Information Classified at Protection Level 4 Describe: _____		

University of California - UC Santa Barbara
Incident Response Plan

University of California - UC Santa Barbara

Incident Response Plan

6. Appendix C - Incident Handler - Cyber Incident Triage and Assessment Questions

Incident Handlers must make an initial assessment of the severity of the Information Security Incident. This will guide triage efforts. A useful approach is to retrieve from the logs (e.g., connections logs, syslog data, pcaps, etc.) between the targeted systems and the attacking hosts. Other sources of information may include system logs, forensic data from the attacked hosts, and reports from other sites.

Information about the Event

The initial collection should include:

- IP address(es) of attacker and victim.
- Platform (including release and patch level).
- System owner(s) (or other responsible parties).
- Criticality of host.
- Scope of the attack.
- Potential damage from the attack.
- Preliminary forensic evidence.

Questions to ask:

- Were root, administrator, or other administrative privileges acquired?
- How many other accounts may have been compromised?
- What was the sequence of events?
- What is the current level of risk based on the Protection Level?
- Is the system being attacked classified as Critical Infrastructure or a critical network component?
- What is the potential or actual rate of the Information Security Incident spreading laterally?
- Does the potential exist for embarrassment to the University of California?

University of California - UC Santa Barbara

Incident Response Plan

7. Appendix D - Other Resources

7.1 Communication Plan

Under development December 2021

7.2 Information Security Incident Response Checklist

Refer to Appendix B

7.3 Notification letter samples

Developed on a case-by-case basis. Public relations and counsel will be involved for all notifications to agencies with a time limit.

7.4 Pre-qualified Incident Response Suppliers

These Suppliers specialize in forensics and notification related to information Security Incidents.

<https://ucop.box.com/s/b32sahonlf6u752xqh3ig8lyxyt5cpyf>

7.5 UC Incident Response Standard

<https://security.ucop.edu/policies/incident-response.html>

7.6 NIST Computer Security Incident Handler Guide – SP 800-61 R2

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>