Privacy and Information Security Incident Response Plan (IRP)

University of California
Agriculture and Natural Resources
March 2020

EMERGENCY CONTACT INFORMATION

- IT Service Desk – (530) 750-1212
- help@ucanr.edu
CONTENTS

1. Emergency response information
   a. Response team members and contact information
   b. Action steps
   c. Details Needed

2. Introduction to the UC ANR incident response plan
   a. Goals of the Plan
   b. Incident Response Program
   c. Organization of the Plan
   d. Use of the Plan

3. Incident response procedures
   a. Preparation
   b. Detection and analysis
      i. Detection
      ii. Preservation of evidence
      iii. Collecting evidence
      iv. Handling of evidence
      v. Forensic documentation
   c. Containment, eradication, and recovery
      i. Containment
      ii. Eradication/Removal
      iii. Recovery
   d. Post-Incident Activity
      i. Root Cause Analysis and Trending
      ii. Testing
      iii. Reviewing and updating the Incident Response Plan
      iv. Required Updates

4. Incident response governance
   a. Incident Response Overview and Lifecycle
   b. Handling Incident Response
   c. UC ANR’s Information Technology Control Environment
Appendix A – Incident communication plan

A. Introduction .................................................................................................................. 22
   I. High Degree of Uncertainty ....................................................................................... 23
   II. Professional Reporters/Bloggers .............................................................................. 23
   III. Cross-Functional Impact ....................................................................................... 23
   IV. Cross-Location Implications .................................................................................. 23
B. How to use this communication plan ....................................................................... 23
C. When to use this communication plan ..................................................................... 24
D. Plan Testing, Maintenance, and Updates ................................................................ 24
E. Roles and Responsibilities ......................................................................................... 24
F. Decision Making Protocol ......................................................................................... 25
G. Guidelines for communicating with the public, internally, and news media .......... 25
H. Escalation Plan ........................................................................................................... 25
I. Communication Checklist .......................................................................................... 26
J. Communication Best Practices ................................................................................... 26
   I. Be transparent but careful ....................................................................................... 26
   II. Develop a simple, accurate, and short message .................................................... 26
III. Establish the facts, and double-check them ................................................................. 26
IV. Focus on actions we are taking to address the issue .................................................... 27
V. Provide context .................................................................................................................. 27
VI. Respond quickly ............................................................................................................... 27
VII. Be visual .......................................................................................................................... 27
VIII. Learn from the Incident ............................................................................................... 27
K. Incident Status Call Sample Agenda ............................................................................... 27
L. What impacted people need to know ............................................................................... 27
Appendix B — Roles directory ............................................................................................. 28
A. Key Roles .......................................................................................................................... 28
B. Units, Unit Heads and Unit Information Security Leads .................................................. 28
Appendix C — Forms and Checklists ................................................................................... 29
A. Initial Assessment Check List ............................................................................................ 29
B. Security Incident Summary ............................................................................................... 29
C. Records About People or Organizations ......................................................................... 30
D. Record Contents ................................................................................................................ 30
Appendix C - Cyber Incident Triage and Assessment Questions for Incident Handler .......... 33
Information about the Event .................................................................................................. 33
APPENDIX D — REVISION HISTORY ............................................................................ 33
Approvals ............................................................................................................................... 34
1. EMERGENCY RESPONSE INFORMATION

In the event that a significant incident occurs at UC ANR the following emergency procedures and contacts are listed here.

A. RESPONSE TEAM MEMBERS AND CONTACT INFORMATION

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-Risk Responsible Executive (CRE)</td>
<td>Tu Tran</td>
<td>510-987-0022 <a href="mailto:tu.tran@ucop.edu">tu.tran@ucop.edu</a></td>
</tr>
<tr>
<td>Lead Location Authority (LLA)</td>
<td>CIO - Sree Mada</td>
<td>530-750-1300 <a href="mailto:smada@ucanr.edu">smada@ucanr.edu</a></td>
</tr>
<tr>
<td>Incident Response Team Coordinator (IRTC)</td>
<td>CISO- TBD David Hatter</td>
<td>530-750-1212 <a href="mailto:djhatter@ucanr.edu">djhatter@ucanr.edu</a></td>
</tr>
<tr>
<td>Incident Response Team (IRT)</td>
<td>CIO CISO Privacy Officer Risk and Safety Lead Unit head of affected department Other department heads as needed</td>
<td></td>
</tr>
<tr>
<td>Units</td>
<td>See Appendix B for Roles Directory</td>
<td></td>
</tr>
<tr>
<td>Unit Heads</td>
<td>See Appendix B for Roles Directory</td>
<td></td>
</tr>
<tr>
<td>Unit Information Security Leads (UISLs)</td>
<td>See Appendix B for Roles Directory</td>
<td></td>
</tr>
</tbody>
</table>

B. ACTION STEPS

Time is critical! Containing and limiting the exposure immediately is the first priority! The following contacts should be made within the first two hours of an incident.

1. Directors (UISL) becomes aware of an incident and determines it is significant
2. Directors (UISL) contacts the CISO
3. CISO contacts the CRE and IRT
4. Incident Response Team convened

C. DETAILS NEEDED

1. Date and time of incident discovery,
2. General description of the incident,
3. Systems and/or data at possible risk,
4. Actions they have taken since incident discovery,
5. Their contact information,
6. Any additional relevant information known at the time.
2. introduction to the uc anr incident response plan

This document describes the plan for responding to information security incidents at the University of California Agriculture and Natural Resources (UC ANR). The plan is based on the guidelines outlined in the UC Information Security Incident Response Standard.

The 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. It defines the roles and responsibilities of participants, characterization of information security incidents, reporting requirements, and relationships to other policies and procedures.

A. Goals of the Plan

The goals of the plan are to:

• Detect and react to information security incidents
• Determine their scope and risk
• Respond appropriately
• Communicate the results and risks to appropriate stakeholders
• Reduce the likelihood of reoccurrence

B. Incident Response Program

This written plan is only one component of UC ANR’s overall incident response program. The program incorporates the comprehensive set of activities designed to prevent, prepare for, and recover from incidents. As described in the standard, UC ANR’s incident response program includes the following 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.

C. Organization of the Plan

The plan is organized into two principal sections plus appendixes:

• Incident Response Procedures
• Incident Response Governance
The Incident Response Procedures section is further organized according to the four phases of the incident response life cycle identified in the Standard (see figure, standard §3.0):

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

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. Requirements for the UC 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/UISL, the CISO’s office, the Supplier (when involved), and forensic investigators.

All additional plans or procedures that units create to meet their specific needs must be aligned with and support this incident response plan.

D. USE OF THE PLAN

Use of this incident response plan is required for all significant incidents. For Routine incidents, certain steps or requirements may not apply.

The ITRC and other workforce members must consider all information security incidents potentially significant incidents until evidence indicates otherwise.
### 3. INCIDENT RESPONSE PROCEDURES

#### A. PREPARATION

The IRT should collect and/or review the incident documentation and event reports. This information should first be verified as being factual (information may have been mis-reported, or incorrectly documented). The IRT should assign the incident severity or re-consider its appropriateness if already assigned. The IRT should determine who, outside of the IRT, needs to be notified of the incident, both internal and external to the affected location and the University, and make those notifications. Information should be restricted on a need-to-know basis.

If the incident requires computer forensic analysis, arrangements must be made to gain access to the data and devices involved in the incident. At this stage, thoroughness is more important than speed. The primary objective is to maintain and restore business continuity.

Every incident should be treated as if it will lead to a court case. Establish robust documentation procedures, by, for example, including the date and time of every entry in the incident log, and signing every page of the log. Document each individual’s time spent on the incident, and any other incident response costs. Forms and checklists are available in Appendix C.

#### B. DETECTION AND ANALYSIS

Once an incident has been declared and a decision has been made to preserve electronic evidence for use in either administrative, civil or criminal remedies, specific steps should be taken to ensure integrity of data and preservation of evidence.

Maintain a chronological log (date and time) of actions taken and sign each page.

**I. DETECTION**

Type of incident and possible locations for evidence: The list below is not all-inclusive and should not limit the scope of evaluation as to where digital evidence may only be found.

<table>
<thead>
<tr>
<th>Type of incident</th>
<th>Possible locations of relevant evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network intrusions</td>
<td>System logs, User logs, Proxy logs, Router &amp; Firewall logs</td>
</tr>
<tr>
<td>Email</td>
<td>Mail Servers, Router &amp; Firewall logs, Individual workstations, Backup tapes</td>
</tr>
<tr>
<td>Internal employee or affiliate activity</td>
<td>System logs, Mail Server Logs, User Logs, Proxy Logs, Router &amp; Firewall logs, Individual Workstations, Electronic organizers, Removable media</td>
</tr>
</tbody>
</table>
II. PRESERVATION OF EVIDENCE

When securing evidence from an employee’s device without consent, complete and submit the “Request to Inspect or Disclose Electronic Record - Access Without Consent” form provided by the Office of the Controller and Business Services. Do not access that device without approval.

Chain-of-custody: utilize a chain-of-custody form for documenting and securing evidence items recovered during an incident, and the date/time and identity of team members involved.

The following concepts should be applied:

- Actions taken to secure and collect electronic evidence should not change the evidence.
- Persons conducting examination of electronic evidence should be trained and preferably certified for this purpose.
- Activity relating to the seizure, examination, storage, or transfer of electronic evidence should be fully documented, preserved, and available for review.
- Note: Incident responders should use caution when seizing electronic evidence devices. The improper access of data stored on electronic devices may violate provisions of federal law, such as the Electronic Communications Privacy Act (ECPA). Consult with UC Counsel.

III. COLLECTING EVIDENCE

Securing and evaluating the scene: first responder should evaluate the scene and formulate a search plan. The condition of electronic devices should not be altered unless a threat to the safety of persons is indicated, or business operations are such that continued operation or non-operation threatens vital UC business operations. The decision should be made in consultation with the IRT.

Protect perishable data both physically and electronically, such as data found on pagers, caller ID boxes, cell phones, smart phones and other similar devices.

“Volatile” data, such as network connections, processes, login sessions, open files, network interface configurations, and the contents of memory, should be carefully captured from active systems.

IV. HANDLING OF EVIDENCE

Full forensic disk images should be made to sanitized write-protectable or write-once media. File system backups should not be used for investigatory and evidentiary purposes. The analysis should be performed on an image, rather than the original, which should be preserved in its original state to the greatest extent possible.

V. FORENSIC DOCUMENTATION

- Description of the incident and how it was detected. Determine when the incident started (if possible) and how soon the organization detected it.
- Record exact dates and times, if known.
- Observations about the condition and location of the computer system including power status of the computer (on, off, or in sleep mode), and related electronic components.
- Photograph, if possible, the entire scene to create a visual record as noted by the first responder.
• Preservation of evidence. Document how and when the evidence was returned or the manner in which it was disposed.

C. CONTAINMENT, ERADICATION, AND RECOVERY

I. CONTAINMENT

Containment strategy
Containment strategy is fundamental to incident response 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 senior leadership (e.g., OP Cyber) 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 is 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.

Containment procedure
UC established the following containment procedure for the IRT to follow:

• 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.
• If incident Handlers suspect the presence of Institutional Information Classified at Protection Level 3 or higher, immediately alert UC ANR IT at help@ucanr.edu. Use the phone to contact a member of the security team—see also the first page of this document.
• 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 the 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:
  - Collect forensic evidence as required, see Section 3.2.4.
  - Contact IT at help@ucanr.edu as a form of escalating the Information security incident.
  At that point, the IRTC will activate the IRT and lead the incident response.

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.

**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 from IT 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**

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.

**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.

• 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:

• Avoid speculation; stick to the facts.
• 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 Brian Oatman, baoatman@ucanr.edu, 530-750-1264.

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
The IRT will determine if UC Office of General Counsel will lead an investigation under attorney client privilege. Once OGC makes the decision to lead the investigation, the IRTC must complete the Information Security Incident Summary and Checklist as soon as practical and submit to infosec@ucop.edu and to:

• Rachel Nosowsky, rachel.nosowsky@ucop.edu, (510) 987-9407.
• Alternate: Maria Shanle, maria.shanle@ucop.edu, (510) 987-9845.
• Backup: Kelly Drumm, kelly.drumm@ucop.edu, (510) 987-9765.

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.

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.

The LLA and CRE, in consultation with the IRT will make the decision to notify affected individuals.

II. 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.

III. RECOVERY
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.

D. POST-INCIDENT ACTIVITY
The IRTC will develop a findings report to guide analysis of the likely cause of the incident. In the report the IRTC will recommend follow-up action, including technical actions, procedural review, and recommendations for improvements.

The CISO and UISL will review the findings report within 45 days of its issuance and take appropriate follow-up action based on report recommendations, using a risk-based approach to prioritize these actions.

I. ROOT CAUSE ANALYSIS AND TRENDING
The CISO will review the findings report and make needed adjustments to risk assessments, risk treatment plans, or control implementation to manage the risks/problems/trends noted in the findings report.

The LLA and CISO will review trends of routine incidents and significant incidents to determine if preventative and detective controls are operating well. They will also make adjustments according to the findings of their review.

II. TESTING
The Incident Response Team Coordinator (IRTC) is responsible for annual testing of the incident response plan. Having to use the plan for incident response 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 ANR 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.

III. REVIEWING AND UPDATING THE INCIDENT RESPONSE PLAN
The plan is routinely reviewed and updated. Updates are required at certain milestones, as follows:

• **Annually** – the plan must be reviewed annually and updated as appropriate.
• **Quarterly** – 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.
• **Events Requiring Updates** – the plan must be updated as needed after incidents or material changes in the organization or operations. Specifically:
  o The IRTC and LLA must update this plan to correct any problems or shortcomings found during an information security incident response or noted in the finding report. Updates must also include lessons learned.
  o When members of the IRTC change or their contact information changes.
  o Plan updates must also occur after the regular testing of the plan.

The LLA is responsible for the maintaining and updating of the plan. The CRE must approve the review of and any updates to the incident response plan.

IV. REQUIRED UPDATES
The CRE must approve the review of and any updates to the Information Security incident response plan. The update log within the plan must be updated as appropriate to document updates.

4. INCIDENT RESPONSE GOVERNANCE
The standard identifies a recommended governance structure for location incident response (§2.0). This plan follows those recommendations by incorporating the following governance components, adapted for UC ANR as described in this section:

• 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 plan.
I. INCIDENT RESPONSE OVERVIEW AND LIFECYCLE

The following diagram, incorporated from the UC standard (§2.2), provides a high-level overview of UC ANR’s incident response process.

II. HANDLING INCIDENT RESPONSE

I. UC ANR’S INFORMATION TECHNOLOGY CONTROL ENVIRONMENT

UC ANR incident response procedures are based on the unique nature of UC ANR’s IT configuration, which is very different from the typical configuration found at a UC campus. Owing to its statewide public outreach mission, UC ANR’s personnel are located all across the state, in various locations. To support these personnel, IT resources are also highly distributed, and exhibit varying control environments depending on where personnel are housed. The following table summarizes the distribution of UC ANR’s IT resources:

<table>
<thead>
<tr>
<th>Location</th>
<th>Description</th>
<th>IT Control Environment Managed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second Street, Davis</td>
<td>Central support location housing UC ANR academics and staff</td>
<td>UC ANR &amp; UC Davis</td>
</tr>
<tr>
<td>UCOP, Oakland</td>
<td>Central support location housing UC ANR staff</td>
<td>UCOP Information Technology Services</td>
</tr>
<tr>
<td>UC Campuses</td>
<td></td>
<td>Each campus</td>
</tr>
<tr>
<td>County Government Offices</td>
<td></td>
<td>County government IT</td>
</tr>
<tr>
<td>County UC ANR Offices</td>
<td></td>
<td>UC ANR</td>
</tr>
</tbody>
</table>
II. UC ANR PROGRAMS

Another consideration in defining UC ANR’s cyber-security approach is the wide variety of programs UC ANR administers and delivers to its stakeholders across the state. These programs require varying IT resources, both in terms of IT devices and the data collected and stored on those devices. The principal programs UC ANR administers, along with which locations those programs deliver services from, are outlined in the following table.

<table>
<thead>
<tr>
<th>Program Role</th>
<th>UCOP</th>
<th>RECs</th>
<th>Counties</th>
<th>2nd Street, Davis</th>
<th>Campus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture Experiment Station (AES)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Specialist</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Advisor</td>
<td>✓</td>
<td>✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓</td>
<td>—</td>
</tr>
<tr>
<td>Statewide Program Community Educators</td>
<td>✓</td>
<td>✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Staff</td>
<td>✓ ✓ ✓</td>
<td>✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Program Directors</td>
<td>✓ CIWR; NPI</td>
<td>✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ UC 4H; UC MG; UC MFP; EFNEP; UC IPM</td>
<td>✓ IGIS; AIC; SAREP (UC CalFresh)</td>
</tr>
</tbody>
</table>

Legend

✓ ✓ ✓ Principally located here
✓ Some located here
✓✓ Split “home”

Key to abbreviations

<table>
<thead>
<tr>
<th>Program</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-H Youth Development Program</td>
<td>4-H</td>
</tr>
<tr>
<td>Agricultural Experiment Station</td>
<td>AES</td>
</tr>
<tr>
<td>Agricultural Issues Center</td>
<td>AIC</td>
</tr>
<tr>
<td>California Naturalists</td>
<td>CalNat</td>
</tr>
<tr>
<td>California Institute for Water Resources</td>
<td>CIWR</td>
</tr>
<tr>
<td>Expanded Food and Nutrition Education Program</td>
<td>EFNEP</td>
</tr>
<tr>
<td>Informatics and GIS</td>
<td>IGIS</td>
</tr>
<tr>
<td>Nutrition Policy Institute</td>
<td>NPI</td>
</tr>
<tr>
<td>Sustainable Agriculture Research and Education</td>
<td>SAREP</td>
</tr>
<tr>
<td>UC Integrated Pest Management</td>
<td>UC IPM</td>
</tr>
<tr>
<td>UC Master Food Preservers</td>
<td>UC MFP</td>
</tr>
<tr>
<td>UC Master Gardeners</td>
<td>UC MG</td>
</tr>
</tbody>
</table>

III. UC ANR’S IT CYBER-SECURITY ORGANIZATIONAL APPROACH

Given the nature of UC ANR’s IT configuration described above, the programs it administers, together with the required roles identified in IS-3, and which apply on responding to incidents, UC ANR has developed the IT cyber-security organizational approach described below.
IV. RELEVANT EXPERTISE

The LLA maintains a list of individuals, units, and other entities that are qualified to assist in incident response. See Appendix B for Roles Directory. 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 incident response.

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

https://ucdavis.box.com/s/tvxrxx002x55uyidj5ad8afhppscpx4

V. 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 ANR uses the following tools as systems of record:

- Zendesk.
- UC’s SIREN.
- Box (or SharePoint if the incident impacts Box).
- Text, DOCX, XLSX, PPTX, JPEG, and other common document formats are acceptable forms of storage.

The IRTC may also approve some forensics tools that produce proprietary formats.

III. DEFINING ROUTINE AND SIGNIFICANT INCIDENTS FOR THE LOCATION

IS-3 categorizes information security incidents as either significant or routine. The UC standard defines these two incident types as follows:

I. 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.

Under this plan, routine incidents are those involving:

- No prominent figures (e.g., celebrities, public officials, university leaders).
- Very low to no potential to lead to notification of (possibly) affected individuals.
- Very low to no potential to lead to public notification (e.g., press releases, website announcements, regulators).
- Very low to no reputational impact related to the incident.
- Very low to no regulatory risk.
- Very low to no impact on the ability to meet contractual obligations.
- 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.
- Isolated Digital Millennium Copyright Act (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.
II. 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.

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 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.
- 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., Active Directory, 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.

IV. MECHANISMS

UC ANR uses semi-automated mechanisms to support handling routine incidents. UC ANR may use semi-automated mechanisms to support handling significant incidents. These include dynamic reconfiguration or blocking as part of the incident response capability.

V. 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 can recover.

Incident prioritization must follow the low/medium/high impact scheme detailed below. For more information, see the Incident Response Standard, section 2.4.

I. 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.

II. MEDIUM
Unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in: (a) moderate damage to UC, its students, 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.

III. 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.

VI. INCIDENT RESPONSE TEAM MEMBERS

The following table identifies IRT members.

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Duties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-Risk Responsible Executive (CRE)</td>
<td>Tu Tran Associate Vice President Business Operations</td>
<td>Responsible for the appointment of the Lead Location Authority/Authorities (e.g., Campus LLA, Health LLA). Ensures that the Cyber Escalation Protocol is followed.</td>
</tr>
</tbody>
</table>
Role | Name | Duties
---|---|---
Lead Location Authority (LLA) | TBD | 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 (Interim) | TBD | 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.
Incident Response Team Coordinator (IRTC) | TBD | 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 | Privacy and Information Security Board | Workforce members who gather, preserve, and analyze evidence so that an incident can be brought to a conclusion.
Unit Information Security Lead (UISL) | See Appendix B | 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 | Brian Oatman Director Risk & Safety Services | Responsible for assessing operational risks at the location, implementing programs to reduce claims at the location, and filing cyber insurance claims.
Counsel | Robin Sanchez Interim Director Administrative Policies & Business Contracts | 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 Coordinator | Brian Oatman Director, Risk & Safety Services | Liaison with outside law enforcement (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.
VII. TRAINING AND REPORTING

The LLA and Workforce Managers must ensure that Workforce Member 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.

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:

- Robin Sanchez, rgsanchez@ucanr.edu, 530-750-1235
- Dave Hatter, djhatter@ucanr.edu, 530-750-1212

And the backup contact is:

- Brian Oatman, baoatman@ucanr.edu, 530-750-1264

APPENDIX A – INCIDENT COMMUNICATION PLAN

Proper communication regarding incidents, their severity and their effects is vital during incident response. The UC standard requires that location incident response plans contain an Information Security Incident Communication Plan (§4.4.4). The plan must “identify how and when to use the plan. This will also address privacy incidents.” The standard defines the communications plan as follows:

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.

A. INTRODUCTION

The LLA has the responsibility of overseeing the communication plan and delegating responsibilities to the appropriate role or individual. The LLA is responsible for consulting with location leadership, counsel, and the IRT when making decisions regarding notification.

The communication process must take into account the severity of the incident and its potential impact. Once an incident is confirmed to be a Significant Incident, the IRTC must ensure the communication plan is followed. If widespread email compromise is possible or suspected, use out-of-band communication options (alternate e-mail, Signal, SMS messaging, etc.).

What counts as an information security incident can include a wide spectrum of types of malicious cyber activity. For the UC system, these incidents range from the theft of protected personal information to
the theft of money, and from fraud and defacement to a disruption of operations. The threat of malicious cyber activity is real and, as our world becomes more interconnected, growing.

Given the importance of electronic information, UC ANR is preparing for how to respond to an information security incident on all fronts, including creating guidelines for internal and external communications.

This communication plan is the top-level controlling document guiding communications during an information security incident.

Preparations for multiple types of crises, such as natural disasters or large protests, can help UC ANR leadership prepare for an Incident. However, there are elements of information security incidents that require additional preparation. An information security incident differs from other situations in the following key ways:

I. **HIGH DEGREE OF UNCERTAINTY**
Information security incidents require serious investigation, but officials often need to communicate about them before many facts are known. UC ANR will need to demonstrate a high level of confidence and expertise while communicating, even if there has not been time to gather much information. However, UC ANR must ensure that any information conveyed is factual and must take into account long-term ramifications of publicly releasing such information (e.g., releasing data or internal processes that might jeopardize a criminal investigation).

II. **PROFESSIONAL REPORTERS/BLOGGERS**
Sharing information regarding an incident is easier than ever and writers covering cyber incidents are familiar with technical and policy issues. They also have a wide network of sources, which means that they may learn details about an Incident before leadership is prepared to share them.

III. **CROSS-FUNCTIONAL IMPACT**
Information security incidents require coordination across a range of units that may not normally work together.

IV. **CROSS-LOCATION IMPLICATIONS**
Information security incidents targeting one location can have effects on other UC locations.

This plan is a companion to the UC ANR incident response plan.

B. **HOW TO USE THIS COMMUNICATION PLAN**
All workforce members involved in the incident response process should be familiar with this plan prior to an Incident. UC ANR’s communication about information security incidents should be planned and controlled.

Once an information security incident is suspected, the LLA will determine if the activation of this plan is required. Once activated, the plan guides communications regarding incident response.
C. WHEN TO USE THIS COMMUNICATION PLAN

During a significant incident with medium impact or higher (see the UC Cyber Incident Escalation Protocol in the UC Incident Response Standard), the LLA will decide whether to activate the use of this plan. If the Incident is likely to become public and raise questions about how UC ANR is responding, or if the Incident affects (or potentially affects) the internal community (faculty, staff, students, etc.), the LLA should err on the side of activation. The LLA can always deactivate if the intensity declines.

Once the use of this plan is activated, the LLA, in consultation with the IRTC and the CISO, will decide which level applies based on an initial assessment. Once the LLA activates the use of this plan, all key IRT members will be notified of the activation by the IRTC. See Section I. Communication Checklist.

D. PLAN TESTING, MAINTENANCE, AND UPDATES

The communications plan must be reviewed and, if necessary, updated after an incident to include technical changes, evolutions in the threat or communication landscape, and lessons learned after a response. Updates should also happen when/if any IRT member changes roles or has new contact information. Periodic testing of the communication plan is required. Having to use this plan for incident response is not considered a test.

E. ROLES AND RESPONSIBILITIES

The CRE is the key decision-maker and provides a framework for reporting an Incident internally and externally. See Section I. Communication Checklist.

This section specifies who is responsible for communicating to key internal and external stakeholders (e.g., media, law enforcement, regulators).

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-risk Responsible Executive (CRE)</td>
<td>Key decision maker. Provides thresholds for reporting an incident internally and publicly.</td>
</tr>
<tr>
<td>CISO</td>
<td>Verifies technical details and facts. Coordinates information with suppliers and other locations. Makes the decision to contact outside law enforcement agencies.</td>
</tr>
<tr>
<td>Communications Coordinator (Designated Communications Officer)</td>
<td>Drafts (as needed), manages approvals, and distributes internal/external communications via appropriate channels. This includes both internal communications (e.g., workforce members) and external communications (e.g., public/media statements).</td>
</tr>
<tr>
<td>Compliance Manager/Officer</td>
<td>Verifies that compliance obligations are met.</td>
</tr>
<tr>
<td>Counsel</td>
<td>Verifies legal obligations are met.</td>
</tr>
<tr>
<td>Incident Response Team Coordinator (IRTC)</td>
<td>Verifies technical details and facts. Coordinates and facilitates communications among IRT members and other internal stakeholders as required.</td>
</tr>
<tr>
<td>Privacy Manager/Officer</td>
<td>Verifies that privacy obligations are met and reviews communications to ensure they are consistent with UC privacy values.</td>
</tr>
</tbody>
</table>
F. DECISION MAKING PROTOCOL

The CRE is the key decision-maker regarding the dissemination of information about an incident outside the IRT to others in UC ANR. The CRE and LLA must consult regarding the activation of this plan, and should coordinate with the IRT regarding internal/external communications.

The CRE decides what information to communicate and which IRT members have the responsibility of communicating with assigned people or entities. (See below.)

G. GUIDELINES FOR COMMUNICATING WITH THE PUBLIC, INTERNALLY, AND NEWS MEDIA

It is critical that any incident information shared with the public, internal community, and/or news media is thoughtfully planned, carefully coordinated, and approved in advance by the appropriate IRT members and university leaders.

In consultation with the CR and LLA, the IRT is responsible for all communications with the public, internal community, or news media.

Assessing the severity of a potential incident takes time and misinformation can spread quickly. The need to notify (potentially) affected individuals should be prioritized and assessed before any details regarding impact are shared outside the IRT, to the public, or to the news media. Even sharing details about the potential existence of an incident can lead to misinformation.

Public statements and communication with the public about an incident should remain tightly controlled until adequate information is available to determine the severity and scope of an Incident. Notification of (potentially) affected individuals should also inform decisions about which details to share publicly.

Communications to workforce members and/or other internal stakeholders about an incident must remain tightly controlled until a) adequate information is available to determine the severity and scope of an incident and b) a review and approval process is completed. The review and approval process must consider the need for legal advice, consultation/investigation with law enforcement, and other external obligations.

No IRT member (workforce member) should communicate with internal colleagues, non-UC individuals, or members of the media except the workforce members authorized and designated to do so. This communication restriction includes a ban on sharing any incident information via social media.

Notification of (potentially) affected individuals should also inform decisions about the timing of public communications and which details to share publicly.

H. ESCALATION PLAN

UC ANR uses the systemwide Cyber Incident Escalation Protocol. See:

https://security.ucop.edu/policies/incident-response.html
I. COMMUNICATION CHECKLIST

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date/Time</th>
<th>Who</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute Cyber Incident Escalation Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform LLA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform CRE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform IRT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform Labor Relations or Union Representatives as required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform impacted/involved Suppliers and/or Business Associates, and/or GDPR data controllers and/or GDPR data processors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enter in SIREN (NAVEX)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follow the Cyber Escalation Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform Risk Manager/Office</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform Business Continuity Manager/Office</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform UCSIRC as needed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform/coordinate with Cal-CSIC as needed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>As needed and if approved, Inform Regulators (e.g., state, federal, and possibly international)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Report with Police</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform External Law Enforcement Agencies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

J. COMMUNICATION BEST PRACTICES

I. BE TRANSPARENT BUT CAREFUL

Transparent communications build trust, yet they need not involve the sharing of information that is not yet verified. During an incident, responders have few facts in the early stages. Public comments can and should demonstrate that UC has experts handling the issue seriously and with the utmost care. No responder should share details that are subject to change during the investigative process. It is better to share limited information than too much information, or to share information publicly that would require subsequent corrections (which are especially difficult to make and manage).

Communications should also avoid any speculation about the perpetrator of an incident.

II. DEVELOP A SIMPLE, ACCURATE, AND SHORT MESSAGE

Communicators should develop a clear statement that contains only known facts. They should avoid complex messages. UC can provide additional nuance later. The ideal crisis message should be factual, succinct, straight-to-the-point, and include three points and no more than 50 words.

III. ESTABLISH THE FACTS, AND DOUBLE-CHECK THEM

Communicators must ensure they are working with accurate information, so facts must be verified by multiple sources before they are shared publicly. It is vital to ask all appropriate questions and investigate carefully before making statements or releasing information. This approach prevents the inadvertent sharing of misleading information.
IV. FOCUS ON ACTIONS WE ARE TAKING TO ADDRESS THE ISSUE

Even though factual details may require time to verify, UC can and should convey in all communications that expertly trained responders are managing the Incident. Communications should also specify steps being taken to protect UC’s Institutional Information and IT Resources and simply describe steps underway to address any broader risks to the system.

V. PROVIDE CONTEXT

During a high visibility Information Security Incident, the likelihood of public speculation is elevated. Communicators should counter speculation with facts and provide context to reduce the risk of undermining public trust. They should also include metrics whenever possible.

VI. RESPOND QUICKLY

Misinformation can spread rapidly through social media, word of mouth, and broadcast commentary. UC’s counter-message should be ready to disseminate as soon as possible. Workforce Members who become aware of misinformation should alert the IRTC.

VII. BE VISUAL

Cybersecurity can be challenging to understand thoroughly without appropriate training. To communicate with a general audience as quickly and effectively as possible, UC ANR should pair its message with a graphic.

VIII. LEARN FROM THE INCIDENT

The IRTC should use their experience and others to improve cybersecurity practices and crisis plans. After a response, conducting a lessons learned exercise is required to evaluate the response and suggest improvements.

K. INCIDENT STATUS CALL SAMPLE AGENDA

1. Roll call.
   a. Record attendance when possible.
2. Opening remarks by ITRC or other leader(s).
3. Brief operations summary (on-scene Incident Handlers or IRTC).
   a. Forensic report.
   b. External coordination.
4. Summary of major communications plans and events.
5. Attendee/invitee comments.
6. Messaging coordination and discussion.
7. Make and record key decisions.
8. Conclusion and next steps.

L. WHAT IMPACTED PEOPLE NEED TO KNOW

California law requires that statements include the following items in the event that notification is required:

- An explanation of what happened.
A description of what information was involved in the Incident.
Details about what UC is doing in response.
Details about what the affected person or entity can do in response.
Other potentially important information.
Whom to contact for more information.

APPENDIX B — ROLES DIRECTORY

A. KEY ROLES

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Phone</th>
<th>E-mail</th>
<th>IRT Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead Location Authority</td>
<td>TBD</td>
<td></td>
<td></td>
<td>Core</td>
</tr>
<tr>
<td>CRE</td>
<td>Tu Tran</td>
<td>510-987-0022</td>
<td><a href="mailto:tu.tran@ucop.edu">tu.tran@ucop.edu</a></td>
<td>Extended</td>
</tr>
<tr>
<td>CIO (Interim)</td>
<td>TBD</td>
<td></td>
<td></td>
<td>Core</td>
</tr>
<tr>
<td>CISO</td>
<td>TBD</td>
<td></td>
<td></td>
<td>Core</td>
</tr>
<tr>
<td>IRTC — Primary</td>
<td>TBD</td>
<td></td>
<td></td>
<td>Core</td>
</tr>
<tr>
<td>Privacy Manager</td>
<td>Robin Sanchez</td>
<td>530-750-1235</td>
<td><a href="mailto:rgsanchez@ucanr.edu">rgsanchez@ucanr.edu</a></td>
<td>Core</td>
</tr>
<tr>
<td>UISL</td>
<td>See Appendix B, Section B</td>
<td></td>
<td></td>
<td>Extended</td>
</tr>
<tr>
<td>Unit Head</td>
<td>See Appendix B, Section B</td>
<td></td>
<td></td>
<td>Extended</td>
</tr>
<tr>
<td>Compliance</td>
<td>Robin Sanchez</td>
<td>530-750-1235</td>
<td><a href="mailto:rgsanchez@ucanr.edu">rgsanchez@ucanr.edu</a></td>
<td>Core</td>
</tr>
<tr>
<td>Counsel</td>
<td>Robin Sanchez</td>
<td>530-750-1235</td>
<td><a href="mailto:rgsanchez@ucanr.edu">rgsanchez@ucanr.edu</a></td>
<td>Core</td>
</tr>
<tr>
<td>Law Enforcement Coordinator</td>
<td>Brian Oatman</td>
<td>530-750-1264</td>
<td><a href="mailto:baoatman@ucanr.edu">baoatman@ucanr.edu</a></td>
<td>Extended</td>
</tr>
<tr>
<td>Risk Manager</td>
<td>Brian Oatman</td>
<td>530-750-1264</td>
<td><a href="mailto:baoatman@ucanr.edu">baoatman@ucanr.edu</a></td>
<td>Extended</td>
</tr>
<tr>
<td>UC IT Security Committee</td>
<td></td>
<td></td>
<td></td>
<td>Core</td>
</tr>
</tbody>
</table>

For help with any security incident: help@ucanr.edu.

B. UNITS, UNIT HEADS AND UNIT INFORMATION SECURITY LEADS

Following are the three extended roles defined in IS-3 and the composition used by UC ANR to fill them.

<table>
<thead>
<tr>
<th>Group/Type</th>
<th>Composition</th>
<th>List link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Units</td>
<td>County Offices&lt;br&gt;Research and Extension Centers&lt;br&gt;Administrative Units&lt;br&gt;Statewide Programs</td>
<td><a href="https://ucanr.edu/p/65226">https://ucanr.edu/p/65226</a></td>
</tr>
<tr>
<td>Unit Heads</td>
<td>County Directors&lt;br&gt;Research and Extension Center Directors&lt;br&gt;Administrative Unit Directors&lt;br&gt;Statewide Program Directors</td>
<td><a href="https://ucanr.edu/p/65226">https://ucanr.edu/p/65226</a></td>
</tr>
<tr>
<td>Unit Information Security Leads (UISLs)</td>
<td>Unit Heads or could be delegated to below&lt;br&gt;• County Business Managers&lt;br&gt;• Research and Extension Center Office Managers&lt;br&gt;• Administrative Unit Business Manager&lt;br&gt;• Statewide Program Business Manager</td>
<td><a href="https://ucanr.edu/p/65226">https://ucanr.edu/p/65226</a></td>
</tr>
</tbody>
</table>
APPENDIX C — FORMS AND CHECKLISTS

A. INITIAL ASSESSMENT

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.

B. SECURITY INCIDENT SUMMARY

<table>
<thead>
<tr>
<th>#</th>
<th>Information Required</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Name of Workforce Member filling out incident summary</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Phone Number of Workforce Member filling out incident summary</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>E-mail address of Workforce Member filling out incident summary</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Unit name</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Unit Information Security Lead name</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Unit Head name</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Was the incident entered in SIREN (NAVEX)?</td>
<td>☐ Yes ☐ No</td>
</tr>
<tr>
<td>8</td>
<td>Date this incident summary was filled out or update</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>IT resources/database/system name</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Protection classification (see IS-3, 8.2.1)</td>
<td>☐ P1 ☐ P2 ☐ P3 ☐ P4</td>
</tr>
<tr>
<td>11</td>
<td>Availability level classification (see IS-3, 8.2.1)</td>
<td>☐ A1 ☐ A2 ☐ A3 ☐ A4</td>
</tr>
<tr>
<td>12</td>
<td>Does incident impact critical infrastructure?</td>
<td>☐ Yes ☐ No</td>
</tr>
<tr>
<td>13</td>
<td>Does the potential exist for embarrassment to UC ANR?</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Purpose/use of database/system</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Link to database/system (if applicable)</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>IP address(es) to IT resources (if applicable)</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Estimate of number of records potentially impacted</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Summarize what is known about the incident</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>IP address(es) of attacker (if applicable)</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Platform (including release and patch level)</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Were root or administrative privileges acquired?</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>How many other accounts may have been compromised?</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>What was the sequence of events?</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>What is the current level of risk?</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>What is the potential or actual rate of incident spreading?</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Scope of the attack</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Potential damage from the attack</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Preliminary forensic evidence</td>
<td></td>
</tr>
</tbody>
</table>
## C. RECORDS ABOUT PEOPLE OR ORGANIZATIONS

Indicate if the database or system contains information on the following types of persons or entities:

<table>
<thead>
<tr>
<th>Entity type</th>
<th>Place an X in the correct column</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Patient</td>
<td></td>
</tr>
<tr>
<td>2 Guarantor (Other than Patient)</td>
<td></td>
</tr>
<tr>
<td>3 Staff</td>
<td></td>
</tr>
<tr>
<td>4 Faculty</td>
<td></td>
</tr>
<tr>
<td>5 Student and/or Resident at the University</td>
<td></td>
</tr>
<tr>
<td>6 Research Subject</td>
<td></td>
</tr>
<tr>
<td>7 GDPR Data Subjects</td>
<td></td>
</tr>
<tr>
<td>8 Alumni or donors</td>
<td></td>
</tr>
<tr>
<td>9 Marketing prospects or other communication targets</td>
<td></td>
</tr>
<tr>
<td>10 Other (e.g., Research Sponsors, Suppliers, Volunteers)</td>
<td></td>
</tr>
<tr>
<td>☐ Research Sponsors</td>
<td></td>
</tr>
<tr>
<td>☐ Suppliers</td>
<td></td>
</tr>
<tr>
<td>☐ Volunteers</td>
<td></td>
</tr>
<tr>
<td>☐ Other:</td>
<td></td>
</tr>
</tbody>
</table>

## D. RECORD CONTENTS

Please indicate if the records contain the following information:

<table>
<thead>
<tr>
<th>Place an X in the correct column(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient</td>
</tr>
<tr>
<td>Guarantor</td>
</tr>
<tr>
<td>Staff</td>
</tr>
<tr>
<td>Faculty</td>
</tr>
<tr>
<td>Student or Resident</td>
</tr>
<tr>
<td>Research Subject</td>
</tr>
<tr>
<td>GDPR Data Subject</td>
</tr>
<tr>
<td>Alumni Donor</td>
</tr>
<tr>
<td>Marketing Prospects</td>
</tr>
<tr>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Please indicate if the records contain the following information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Name (First, Middle, and/or Last Name or Initials)</td>
</tr>
<tr>
<td>2 Street Address</td>
</tr>
<tr>
<td>3 Phone Number or E-Mail Address or personal URL</td>
</tr>
<tr>
<td>4 Medical Record Number</td>
</tr>
<tr>
<td>5 Social Security Number (last four digits only)</td>
</tr>
<tr>
<td>6 Social Security Number (full or partial, other than just last 4 digits)</td>
</tr>
<tr>
<td>7 Medicare ID Number</td>
</tr>
<tr>
<td>8 Other Government Identifier (e.g., passport number, driver’s license number)</td>
</tr>
<tr>
<td>9 Health Insurance Information (e.g., insurance policy number, health plan beneficiary number, claims history, any other identifier used to identify an insured)</td>
</tr>
<tr>
<td>10 Medical Information (e.g., diagnosis/condition; lab/test results; medications; treatment notes; genetic)</td>
</tr>
</tbody>
</table>
Please indicate if the records contain the following information:

<table>
<thead>
<tr>
<th>Place an X in the correct column(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>information; treatment date, discharge date, or other dates of service; claims history</td>
</tr>
<tr>
<td>11 FERPA covered information (e.g., exam scores, counseling records, grades, etc.); (Non-directory information)</td>
</tr>
<tr>
<td>12 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.)</td>
</tr>
<tr>
<td>13 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)</td>
</tr>
<tr>
<td>14 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)</td>
</tr>
<tr>
<td>15 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)</td>
</tr>
<tr>
<td>16 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)</td>
</tr>
<tr>
<td>17 Biometric Identifier (e.g., Fingerprint, Voiceprint, or full-face photos and related geometric expression)</td>
</tr>
<tr>
<td>18 Digital Signature (i.e., algorithm used to validate authenticity of an electronic document or message)</td>
</tr>
<tr>
<td>Please indicate if the records contain the following information:</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>19 Other Direct Identifiers (e.g., tracking ids, cookies, URL, IP addresses, etc.) for records not covered by GDPR</td>
</tr>
<tr>
<td>20 Driver license or other government information or images</td>
</tr>
<tr>
<td>21 Passport information or images</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Indicate if the records contain the following information:</th>
<th>Place an X in the Correct Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 “Controlled Information” Subject to UC/USA Export Control Policies</td>
<td>No</td>
</tr>
<tr>
<td>2 Institutional Information covered by Export Control regulations (e.g., ITAR, OFAC, etc.)</td>
<td>No</td>
</tr>
<tr>
<td>3 “Controlled Unclassified Information” (CUI) subject to contract requirements</td>
<td>No</td>
</tr>
<tr>
<td>4 Information from Dual Use Research of Concern</td>
<td>No</td>
</tr>
<tr>
<td>5 Information from Research Involving Select Agents</td>
<td>No</td>
</tr>
<tr>
<td>6 Human subject research protocols or test methods</td>
<td>No</td>
</tr>
<tr>
<td>7 Animal research protocols or test methods</td>
<td>No</td>
</tr>
<tr>
<td>8 Research Sponsors’ Confidential or Proprietary Data (Including Protocols, Case Report Forms, and Other Research Manuals)</td>
<td>No</td>
</tr>
<tr>
<td>9 Security Risk Assessments or similar reports documenting vulnerabilities in cybersecurity infrastructure</td>
<td>No</td>
</tr>
<tr>
<td>10 Architecture diagrams, network maps, source code, or other materials that would aid an attacker or compromise information security</td>
<td>No</td>
</tr>
<tr>
<td>11 Information documenting vulnerabilities in physical plant/infrastructure</td>
<td>No</td>
</tr>
<tr>
<td>12 Environmental Health &amp; Safety (EH&amp;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)</td>
<td>No</td>
</tr>
<tr>
<td>13 Payment Card Numbers (debit card numbers, credit card numbers, payment card security codes, bank account or other financial account numbers and/or PINs)</td>
<td>No</td>
</tr>
<tr>
<td>14 Other Institutional Information Classified at Protection Level 3 Describe:</td>
<td>No</td>
</tr>
<tr>
<td>15 Other Institutional Information Classified at Protection Level 4 Describe:</td>
<td>No</td>
</tr>
</tbody>
</table>
APPENDIX C - CYBER INCIDENT TRIAGE AND ASSESSMENT
QUESTIONS FOR INCIDENT HANDLER

Incident handlers must make an initial assessment of the severity of the information security incident. This appendix will guide triage activity. 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 UC ANR?

APPENDIX D — REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>By</th>
<th>Contact Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 21, 2019</td>
<td>Dave Krause, LLA, Interim CIO</td>
<td>No longer at ANR</td>
<td>Draft version complete</td>
</tr>
<tr>
<td>August 20, 2019</td>
<td>Dave Krause, LLA, Interim CIO</td>
<td>No longer at ANR</td>
<td>Final draft complete — Ready to Publish</td>
</tr>
</tbody>
</table>
### APPROVALS

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>By</th>
<th>Contact Information</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td></td>
<td>Tu Tran, CRE, AVP Business Operations</td>
<td><a href="mailto:Tu.tran@ucop.edu">Tu.tran@ucop.edu</a> 510-987-0022</td>
<td></td>
</tr>
</tbody>
</table>