
1.0 Purpose

The purpose of this procedure is to outline the process for promptly responding to information systems security incidents. If a security incident occurs, a prompt and coordinated response will limit damage, speed up the recovery process and aid in restoring service.

The HIPAA Security rule governing this procedure is: *164.308(a)(6)(i) Security Incident Procedures*. Implement policies and procedures to address security incidents.

2.0 Definitions

2.1 Information Systems Security Incident: An information systems security incident is any event, suspected event, or discovery of a vulnerability that could pose a threat to the confidentiality, integrity, or availability of supporting systems, applications, or information.

Such an incident can pose actual or potentially harmful effects on a computer system. The types of activity that are widely recognized as harmful include but are not limited to:

- Attempts (either failed or successful) to gain unauthorized access to (or use of) an information system or the data stored on the system.
- Unwanted disruption or denial of service.
- Unauthorized changes to system hardware, firmware, or software, including adding malicious code such as viruses and worms.
- Detection of the above-named symptoms such as altered or damaged files, virus infection messages appearing during start-up, or inability to log in, and more.

2.2 Workforce: All faculty, staff, students, trainees, volunteers, and business associates who access restricted or confidential information during the course of their duties.

3.0 Procedures & Responsibilities

The following steps outline the duties of information system users, system administrators, system managers, and other personnel involved in the management of information systems when a suspected computer security incident occurs involving Medical Center or Campus information systems.

3.1 Incidents Involving Medical Center Systems: Refer to *Appendix B: Information Systems Security Incident Reporting Process Workflow*.

3.2 Incidents Involving both Campus and Medical Center (Enterprise): Instructions for reporting incidents that involve both Campus and Medical Center, refer to the UCSF HIPAA Security Departmental Compliance website http://www.ucsf.edu/hipaa/dept_compliance/ for the documents listed below:

- *Lost/Stolen Mobile Device and/or Media*
- *Incident Response Process for UCSF Hacked/Compromised Computers*
- *Unscheduled Outage Process*
- *Unscheduled Outage Flowchart*

3.3 Report All Incidents: All incidents that are unexpected, successful (or nearly successful), or those that indicate a new vulnerability or threat source must be reported immediately to the local Computer System Administrator, Unit Manager and Department Manager.

3.4 Incidents Involving both Campus and Medical Center (Enterprise): are posted at http://www.ucsf.edu/hipaa/dept_compliance/

3.4.1 Individual Users' Responsibilities:

Stop all work on the computer and report the information systems security incident to Customer Support (415) 514-4100, and to the local Computer System Administrator, Unit Manager and Department Manager.

3.4.2 Customer Support Responsibilities:

Administration

- Enter the incident into the Remedy database.
- Maintain a current list of IT system owners, system administrators, and system managers.

-
- Set up and maintain an emergency conference bridge for all computer security incidents.
 - Maintain status report in the event that the Computer Incident Response Team is activated.
 - Develop procedures for addressing information system security incidents that are reported after-hours.

Identification

- Document the incident in the Remedy system database.
- Notify the appropriate system administrator and/or system manager, the Information Security Manager and the Computer Incident Response Team, if applicable.

Incident Resolution

- Close the Remedy ticket.
- Inform user(s), system administrator and/or system manager, and any other individuals, who may have been affected, that the incident has been resolved and that they can resume using the information system.

3.4.3 Computer System Administrator/System Manager Responsibilities

- Quickly and briefly investigate system anomalies to determine if an information systems security incident is in progress or has occurred.
- If an information systems security incident has been detected, notify the system owner, the Customer Support Center, the Information Security Manager, and the Security Officer.
- If the incident has been determined to be a non-security incident, notify the Customer Support Center immediately by telephone or via email and reference the Remedy Ticket number, if available.

3.4.4 Information Security Manager Responsibilities

- Notify the Information Security Officer.
- Communicate the incident with members of the Computer Incident Response Team (CIRT).
- Provide technical solutions and specialized training for personnel involved with responding to information systems security incidents.

3.4.5 Information Security Officer Responsibilities

- Declare an information systems security incident has occurred and activate the Computer Incident Response Team (CIRT).
- Identify and assist in assigning resources required to support the CIRT.
- Communicate details of the information systems security incident to the Information Security Officer and the Chief Information Officer (CIO).
- Coordinate with UCSF Police and provide details of the incident as required.
- Gather information necessary for completing the Information Systems Security Incident Report.
- Submit the Information Systems Security Incident Report to the CIO within three business days.

3.1.6 Chief Information Officer Responsibilities

- The CIO has the final authority on all decisions related to the management of and response to information systems security incidents.
- Communicate the details of the information systems security incident to the Chief Executive Officer and/or other senior executives and provide periodic updates concerning the significance and severity of the threat.
- Determine appropriate level of information to release to the user community and coordinate

with the Office of Communications. Release of information must be consistent with applicable Federal and State regulations.

3.1.7 Computer Incident Response Team's Responsibilities.

The Computer Incident Response Team (CIRT) includes: System Administrators, System Managers, the Information Security Manager and his team who serve as computer security subject-matter experts, the Infrastructure and Network Operations Center (NOC) team, the Server and Technology Engineering team, the Customer Support Center, and a core group of system representatives called in for each of the involved platforms.

- Identify and document the nature of the information systems security incident.
- If declared a non-incident, notify the Customer Support Center at (415) 514-4100.
- If declared an information systems security incident:
 - Provide instructions to end user(s) concerning continued use of the affected system.
 - Identify whether other systems have been compromised.
 - Formulate a plan of action for containing, eradication and recovering systems and data.
 - Assign a priority level sufficient to ensure the availability of any required resources. Resources must be dedicated solely to the investigation until the incident is resolved and the CIRT has been deactivated.
 - Prepare detailed documentation in log of information systems security incidents, including the date, time and summary of the events and a description of activities

invoked by the intruder (or malicious code) as well as the actions taken to resolve the incident. Document time and effort and the costs associated with resolving the current incident.

- Submit prompt status reports as well as the information required to complete the Information Systems Security Incident Report (Appendix B) to the Security Officer and/or the Chief Information Officer.
- During containment, eradication and recovery:
 - Take screen captures and/or snapshots of pertinent files within the first ½ hour of any incident investigation.
 - Back up files, if required.
 - Secure and protect the affected system(s) and all related media.
 - Identify known risks to systems or data including any significant operational impact caused by the information systems security incident.
 - Continue investigating, reporting and mitigating the incident until it has been resolved.
 - Reduce and eliminate risk and clean up the affected system.
 - Monitor the Conference Bridge, monitor recovery process, maintain documentation, and communicate progress results to senior management.
 - Notify the Customer Support Center and Security Officer when the incident has been resolved.
 - Close the Remedy ticket.
- Documentation and archival of incident

-
- All reported information systems security incidents and their respective dispositions must be documented and archived. This includes documenting notable lessons-learned, such as lessons concerning needed improvements in security training and/or necessary changes to existing policy.
 - Report lessons-learned to the Security Officer and inform of all information systems security incidents that involve any apparent violation of State or Federal laws or regulations.

4.0 Initiation and Control Reporting

5.0 Initiation and Control Reporting

6.0 Related Records

HIPAA Security Rule: Security Incident Procedures	164.308(a)(6)
University of California Business and Finance Bulletin IS-3 Electronic Information Security	BFB IS-3 http://www.ucsf.edu/hipaa/dpt_compliance/ or http://www.ucop.edu/ucophome/policies/bfb/is3.pdf
UCSF Information Security and Confidentiality Policy	650-XX http://www.ucsf.edu/hipaa/dpt_compliance/
UCSF Medical Center Administrative Policy - Information Security and Confidentiality Policy	5.01.04 http://www.ucsf.edu/hipaa/dpt_compliance/
Incident Response Process for UCSF Hacked Compromised Computers (for incidents involving the Campus and Medical Center)	http://www.ucsf.edu/hipaa/dpt_compliance/
Lost/Stolen Mobile Device and/or Media flowchart (for incidents involving the Campus and Medical Center)	http://www.ucsf.edu/hipaa/dpt_compliance/
Unscheduled Outage Process and Unscheduled Outage Flowchart (for incidents involving the Campus and Medical Center)	http://www.ucsf.edu/hipaa/dpt_compliance/

REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	01/27/05	Binh Nguyen, Manager, IT Network Infrastructure and Security	Initial Release; modified to match SOM template.

If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.
Contains Proprietary Information and is for the use of UCSF only.

Appendix A: Information Systems Security Incident Report

Incident Number: _____ Incident Type (defined below): 1 2 3 4 5 6 7
Date of Incident: _____ Time of Incident _____

1. Reporting Information:

Department/Unit: _____
Name: _____
Telephone #: _____
E-mail Address: _____

2. Target Host Information:

Host IP: _____
Host Machine Name: _____
System Description/Mission: _____
Operating System: _____

3. Source(s) Information:

Source(s) IP: _____
Source Host Name: _____
Source Name and Address: _____

4. Intrusion Information:

Type of Incident or Attack: _____
How Detected: _____
Description of Incident: _____
Was System Compromised? Yes _____ No _____
Impact on Operation: _____

Countermeasure(s): _____

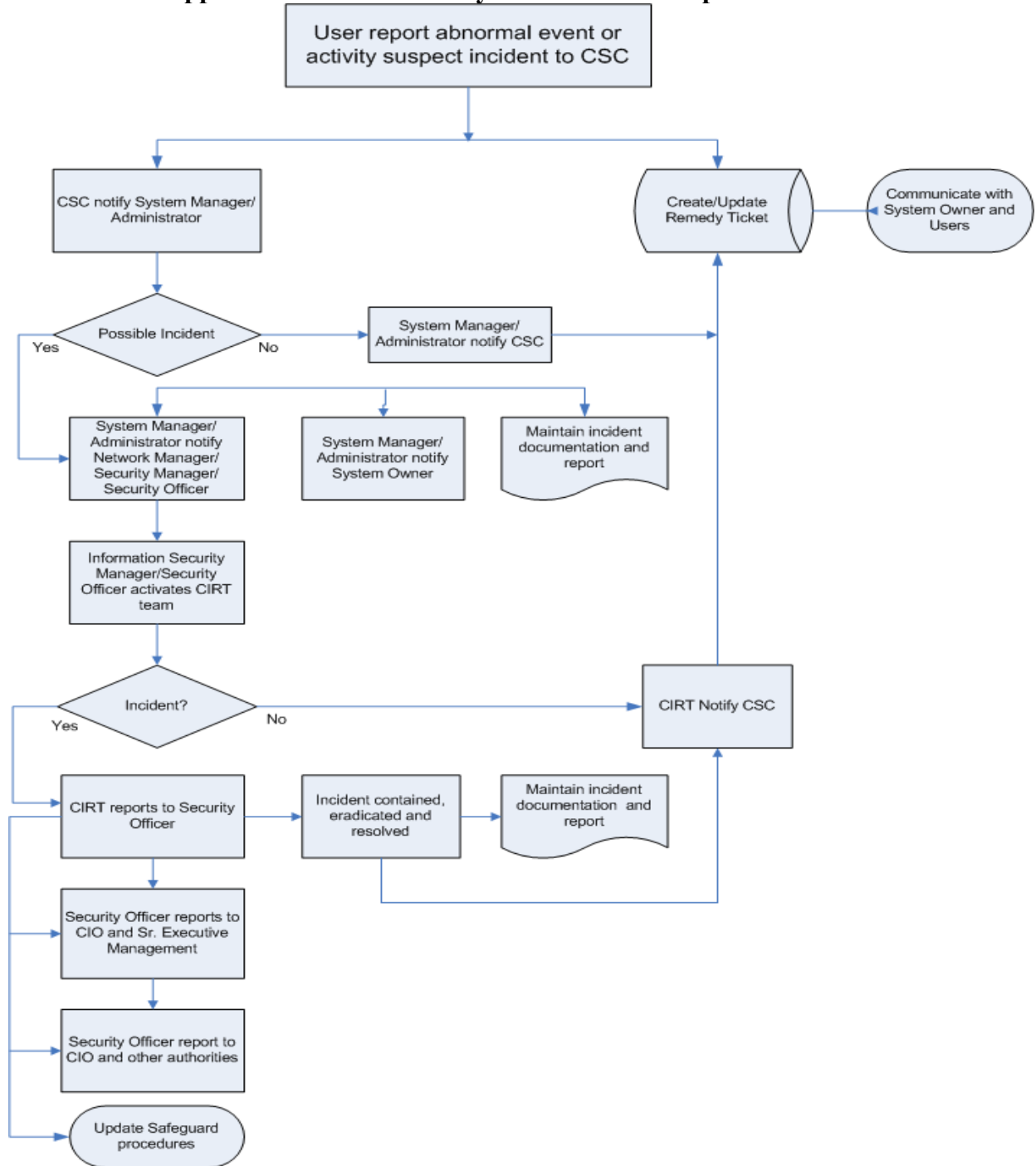
If this is a paper copy, it is *uncontrolled*, and you must verify the on-line revision level before using.
Contains Proprietary Information and is for the use of UCSF only.

Incident type and definitions

<p>1 – Electronic User Compromise</p> <ul style="list-style-type: none"> <input type="checkbox"/> Compromised/Stolen/Altered Data <input type="checkbox"/> Theft and use of Others ID's <input type="checkbox"/> Unauthorized Root/Administrative Access <input type="checkbox"/> Other 	<p>5 - Web Site Defacement</p> <ul style="list-style-type: none"> <input type="checkbox"/> Defacement of Web Site(s) <input type="checkbox"/> Redirected Web Site(s) <input type="checkbox"/> Other
<p>2 – Denial of Service</p> <ul style="list-style-type: none"> <input type="checkbox"/> Denial of Service <input type="checkbox"/> Dictionary Attacks <input type="checkbox"/> Other 	<p>6 – Reconnaissance Activity</p> <ul style="list-style-type: none"> <input type="checkbox"/> Probes/Scans <input type="checkbox"/> Unauthorized Monitoring <input type="checkbox"/> Other
<p>3 – Misuse of Resources</p> <ul style="list-style-type: none"> <input type="checkbox"/> Unauthorized Use of Remote Control <input type="checkbox"/> Unauthorized Use of Software <input type="checkbox"/> Inappropriate Use of Email <input type="checkbox"/> Inappropriate Use of Medical Center Resources <input type="checkbox"/> Unauthorized Solicitation <input type="checkbox"/> Illegal Log-in Attempt <input type="checkbox"/> Hoaxes <input type="checkbox"/> Storage and/or Distribution of Illegal Software <input type="checkbox"/> Other 	<p>7 – Malicious Code Activity</p> <ul style="list-style-type: none"> <input type="checkbox"/> Worm <input type="checkbox"/> Virus <input type="checkbox"/> Trojan Horse <input type="checkbox"/> Root Kits <input type="checkbox"/> Other
<p>4 – 4. Physical</p> <ul style="list-style-type: none"> <input type="checkbox"/> Unauthorized Access <input type="checkbox"/> Access Control Avoidance <input type="checkbox"/> Equipment Stolen or Damaged <input type="checkbox"/> Tornado/Storm <input type="checkbox"/> Fire <input type="checkbox"/> Floods <input type="checkbox"/> Bomb Threats <input type="checkbox"/> Bio/Chemical Hazards <input type="checkbox"/> Other 	<p>Internet Complaint: Describe:</p> <p>A Notification was sent to:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Medical Center Customer Service Center <input type="checkbox"/> Medical Center Security Officer <input type="checkbox"/> Medical Center Network Security Manager <input type="checkbox"/> Medical Center Network Operation Center <input type="checkbox"/> Medical Center IT Director <input type="checkbox"/> Medical Center Network Operation manager <input type="checkbox"/> Other:

If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.
Contains Proprietary Information and is for the use of UCSF only.

Appendix B: Information Systems Incident Response Workflow



If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.
 Contains Proprietary Information and is for the use of UCSF only.