

## UC SECURITY INCIDENT RESPONSE COORDINATION

Accepted by UCITPS, April 16, 2007

### **UC Security Incident Response Coordination Mission**

The UC Security Incident Response Coordination (UCSIRC) fosters the immediate and secure sharing of sensitive protection, incident, and response information through a trusted collaborative environment. UCSIRC also fosters the sharing of technical security observations that may reflect precursory incident information among University of California (UC) staff with computing/network security responsibilities. The objective of UCSIRC is to reduce the occurrence and severity of computer/network security breaches within the University of California system.

### **UCSIRC Membership and Responsibilities**

- Two to three individuals per institution, annually appointed by the ITLC members of UC campuses and medical centers and UC affiliated national laboratory
- Individuals must have responsibility for institutional network and/or computing security
- It is expected that at least one of the campus appointed UCSIRC members will participate in the UC Information Technology Policy and Security group (UCITPS).
- UCSIRC members are responsible for the appropriate distribution of shared information within their respective campuses
- UCSIRC members are not responsible for remediation work related to an incident reported by another institution

### **UCSIRC Chairperson**

- UCSIRC will designate one of its members to serve as the chairperson. The chairperson will serve an annual term. The chairperson is responsible for UCSIRC administrative tasks and, as required, periodically provides reports to the UCITPS group and UC Information Technology Leadership Council.

### **UCSIRC Authority**

The UCSIRC or its members do not have the authority to direct any constituency to perform any action or implement security incident response measures for either protection or recovery. The UCSIRC may make recommendations or advise UCITPS and/or ITLC members about actions to reduce or prevent security exposures

### Membership Requirements

- UCSIRC members must have passed background checks by their respective institutions
- Members must have at least five years of technical computing and/or network security experience
- Members must be able to use PGP email encryption and share their PGP public key
- Members must respect any information sharing restrictions requested by incident reporting originator
- As appropriate, inform CIO of general characteristics of security incidents reported to UCSIRC.

### Why Should I Report Using UCSIRC?

- You may prevent a similar incident from occurring at another Internet community organization (RFC1281)
- You may receive technical assistance from your peers.
- You may be able to associate activity with other incidents.
- Contacting others raises security awareness.

### Characteristics of Incidents Subject to UCSIRC Reporting

Incident Criteria	Incident Characteristics
Urgency	<ul style="list-style-type: none"><li>- Active condition, or</li><li>- Recent condition reported by multiple sources on campus</li><li>- Immediate response advised to curtail or prevent outbreaks</li></ul>
Credibility	<ul style="list-style-type: none"><li>- Documentation available to support incident report</li><li>- Credible report sources</li></ul>
Severity	<ul style="list-style-type: none"><li>- Full or partial administrative compromise, and/or</li><li>- Multiple points of attack/malicious entry, and/or</li><li>- Multiple targets, and/or</li><li>- Significant recovery efforts</li></ul>
Impact	<ul style="list-style-type: none"><li>- Broad network infrastructure, or</li><li>- Focused attack on computing resources, including large DB (&gt;5k records) with personal identity/HIPAA data, or</li><li>- Health/Safety-threatening activity</li></ul>

## Reporting – Secure Incidents

UCSIRC incident(s) will be communicated through encrypted email, fax or through ad hoc conference calls. This communication must be initiated in a timely manner, within 48 hours of the identified incident. The incident description should include the below components. At a minimum, *general incident characteristics* must be shared that can be used to determine whether similar incidents are occurring at other UC campuses and/or to prevent similar incidents from occurring at other UC campuses. At the incident reporter's discretion, an incident may be determined appropriate for sharing over insecure communication channels; however, in the case of uncertainty, the use of secure communication channels should prevail. Sharing incident information with the UCSIRC should not preclude the reporter from sharing incident information with their respective legal counsel and/or law enforcement agency.

- "Source(s)" of malicious traffic/attack
- Target(s) involved in the incident
- Security vulnerability and/or exploit used in the security breach. If not known, incident attack characteristics
- Nature of security breach. This narrative should include but not be limited to the following questions:
  - o What is at risk as a result of the incident?
  - o What vulnerabilities were subject to exploitation?
  - o What unauthorized modifications were found?
  - o What malware was found?
  - o What operating systems, database, etc. products/versions were subject to successful attack?
  - o Which logs contained an indication of the security breach?
  - o What timezone and how accurate are the system clocks for the compromised systems?
- Response taken after incident confirmed
- Recommended preventive or observation actions for other UC institutions
- Identification of any incident components that cannot be further shared by UCSIRC members
- Assistance request

## Communicating and Managing UCSIRC Information

The following table describes the characteristics of UCSIRC reports.

	<b>Non-Secure Communication Channel</b>	<b>Secure Channel Communication</b>
<b>Email Report</b>	Clear text	Must be encrypted and digitally signed
<b>FAX Report</b>	No restriction	Cover sheet indicating restricted content and requesting immediate delivery of fax to addressee
<b>Conference Call</b>	Limited to UCSIRC members	Limited to UCSIRC members
<b>Content Sharing Restrictions</b>	No restriction	Content originator defines sharing restrictions; however, there are no sharing restrictions for <i>general incident characteristics</i>
<b>Incident Storage</b>	No restriction	Maintain incident information in encrypted format or on physically secure portable or paper media. Incident data must be securely deleted, consistent with retention requirements, to prevent unauthorized data recovery.