Appendix C:
UCSC Campus Incident Response Team (CIRT) Checklist

Instructions:
Complete checklist for each incident for which the CIRT is convened. Identify whether existing procedures and incident documentation suffice or if additional documentation is needed.

Checklist:

Related to Data Involved

- ❑ Types of data involved:
  - ○ SSN
  - ○ Driver's License or State ID
  - ○ Financial account information
  - ○ Credit card or account numbers
  - ○ Personal health, medical or medical insurance information
  - ○ Other Restricted Data (specify):
  - ○ FERPA-protected data (will need to notify Registrar)
  - ○ "Significant" or "high-visibility" incident (specify):
- ❑ Refer to *Information Breach Decision Tree for California State Law* for guidance on regulatory requirements for the timing of notifications to affected individuals, regulatory agencies, and the media, if appropriate.
- ❑ If ePHI was involved:
  - Refer to *Information Breach Decision Checklist for HIPAA* (available from UC HIPAA Officers or Health Lawyers) for guidance on regulatory requirements for the timing of notifications to affected individuals, regulatory agencies, and the media, if appropriate.
  - Perform and document a risk assessment to determine whether there is a significant risk of harm to the individual whose PHI was inappropriately disclosed.
  - Ensure compliance with required notifications.
  - Include any unauthorized disclosure of PHI on the HIPAA Accounting for Disclosures log.
  - Include any sanctions in the HIPAA sanctions log.
- ❑ Is redaction required for any security sensitive information?
  e.g. "Target of the attack [Host Name/IP Address] should not be listed for incidents involving protected health information or sensitive student information"

Incident Handling

- ❑ Do we need to involve any external agencies? E.g., law enforcement, regulatory agencies.
- ❑ Is law enforcement involved? If so, how does it affect incident handling?
- ❑ Is there a potential for insurance claim? If so, how does it affect incident handling?

- ❑ Are there any other factors that affect containment of the incident?
  Containment is the combination of actions, including technical controls such as network and system disconnects, that limit the damage to University resources.
- ❑ Is preservation of evidence required?
  Documentation per "Proper preservation of evidence requires establishment of chain of custody procedures prior to an incident. Any electronic evidence should be properly tracked in a documented and repeatable process. "
- ❑ Is a forensic analysis required?
- ❑ Do we document estimated technical impact of the incident (i.e. data deleted, system crashed, application unavailable)?
- ❑ Do we track total hours spent on incident handling and/or additional non-labor costs involved in handling (estimate), and any other incident response costs?

Notification

Considerations for notification (See Exhibit B in UC Incident Response Plan)

- ❑ Develop a Call Center
  Decide on using an internal vs. external; toll-free telephone number; determine the staffing (numbers) and coverage hours and days of week; train staff to respond to incident calls (provide standard scripts); comfortable setting (head-sets, quiet area, computer); bilingual skills, etc.
- ❑ Communications Plan
  Identify who needs to be notified (internal / external), who is responsible, coordinate the response and message; develop internal FAQs; press release draft; escalation guide for call center; formal notification to other agencies, vendors, stakeholders, media contact persons; press briefing
- ❑ Notification methods
  Internal e-mail, US mail, media alert/press release; mail house/breach response company; type of letterhead and whose signature; envelope style; finalize the letter and determine whether to include FAQs with the letter.
- ❑ Regulatory agencies
  Determine which agencies (e.g., CA Attorney General, CDPH, OCR, etc.), if any, require notification; provide each agency with their required information, in the format and manner (electronic, written, etc.) they require
- ❑ Mail house
  Determine whether the mail house is required to cleanse the list with National Change of Address Office; if so, determine if you want to be notified of address updates; execute a HIPAA Business Associates Agreement (BAA) with the external mail house if the incident is associated with a breach of PHI (protected health information)
- ❑ Do we need to document responses to letters and concerns?
- ❑ Do we need to document the source of notification addresses and alternatives?

Incident Report

Additional documentation:

- ❑ Contact information for all parties involved in the incident
  (include why)
- ❑ Complete incident handling log/technical report (supplemental to the incident report)
  - Comprehensive incident log including documentation of all activities and include a date / time log as appropriate, e.g., who did what when
  - Detailed information about the event, including actions taken and personnel involved
  - Detailed information about the investigation
  - When, where, and from whom the evidence was received (or taken)
  - The physical analysis (visual evaluation), including brand names, model numbers, and serial numbers
  - The forensic duplication, including how the image was made (for digital evidence), the software and hardware used to make the image, and the hash comparison results
  - Every step taken in the analysis of media. Explain what tools were used and what was or was not discovered as a result of these processes. Document other information such as: number and size of sectors, operating systems, significant software, anti-virus, crash-guard software, etc.
  - All conclusions reached
  - How and when the evidence was returned or the manner in which it was disposed
  - Note: data used in this report should reference collected evidence, and be verifiable

Post-Incident Review (PIR)

- ❑ Complete PIR
  Determine if PIR should be done under attorney-client privileges.
  - Remaining action items related to remediation
  - Root cause
  - Lessons Learned:
    - What worked well; what didn't work so well
    - Cover technical measures; policy/guidelines, roles/responsibilities or org structure;
  - Recommendations based on lessons learned and root cause
- ❑ Communication plan (not related to notification), including
  - requirement (if needed) to use encryption or out-of-band mechanisms for incident-related communications
  - public statements or other communications external to the CIRT
  - notification of other campuses