Data Security Incident Management Plan (Epidemiology)

Version: December 8, 2010

1. **PURPOSE:** The purpose of the Information Security Incident Response Procedure is to define the department's procedures for handling Information Security Incidents, including contact information for business unit personnel with responsibility for responding to the incident, plans to contain an incident, and procedures on how to restore information, if necessary. This procedure supplements the University's Incident Management Policy.

2. **SCOPE:** This procedure applies to all Epidemiology employees including temporary employees as defined within. A security incident includes any incident that is known or has the potential to negatively impact the confidentiality, integrity, or availability of UNC-Chapel Hill's information. This can range from the loss of a laptop or PDA to the virus infection of an end-user work station to a major intrusion by a hacker. All Epidemiology employees shall report actual or perceived security incidents or security threats in the following manner:

   a. Contact an Epidemiology Information Security Liaison:
      David Kleckner, 966-6649, or david_kleckner@unc.edu
      Spencer Gee, 843-9742, or spencer_gee@unc.edu

   b. If no contact or response, call the UNC Help Desk at 962-HELP

   c. If sensitive data is at risk alert the Information Security Office by calling the Information Technology Response Center at 919-962-HELP or submitting a critical Remedy ticket for assignment to the ITS-Security Remedy group. Do not include details regarding the nature of the incident during the initial call and/or in the ticket but have the details ready when an incident responder contacts you in response to your critical ticket.

3. **GENERAL:** Note: When there is an identifiable risk to sensitive information, departmental personnel will issue a critical ticket to the ITS-Security Remedy group prior to performing any system scanning or cleanup actions. Critical data may be lost or spoiled if appropriate care is not taken to preserve evidence. The department will respond to information security incidents by initiating a Departmental Incident Response Team (DIRT). The DIRT will be comprised of:

- An Epidemiology Information Security Liaison
- The System Administrator for the affected information system
- The person or person(s) capable of identifying the types of data residing on the affected system/s
- A representative from the ITS Security Office
- Others as needed or as specified by the department, such as the Principal Investigator of the affected project.

4. PROCEDURES

Preparation Stage of Incident Management

Epidemiology will anticipate the most likely types of information security incidents in their environment and prepare for them. Examples of the types of preparation by departments that are likely to be helpful during an incident are as follows:

1. **Inventory** -- An inventory of systems that host/process/access sensitive data or are critical to the university mission (sensitive/critical) is essential to efficient incident management.

2. **System Hardening, Profiling, and Backups** – Documentation and adequate backups of a system build prior to an incident can speed incident resolution.

3. **Vulnerability Management** – Regular vulnerability scans of sensitive/critical systems can help incident managers quickly assess likely vectors of intrusion. Such preparation often helps quickly identify the nature of the intrusion, contain and eradicate the damage with minimal downtime and restore business processes. ITS makes vulnerability scanning services available for free to departments for any sensitive/critical system and university requires such scanning, in some cases. See the Vulnerability Management policy for detail.

4. **Communication protocol**
    a. All contact information for the DIRT should be readily available prior to the onset of an incident. A copy should be maintained offline in case an incident results in loss of access to such contact information.
    b. External breach notification requirements should be catalogued and appropriate contact information should be catalogued and available prior to the onset of an incident (i.e. Federally funded research contract with contractual breach notification clauses)
    c. IT Directors and Security Liaisons should provide guidance to ISO regarding how they would like ISO to contact them or their delegates when incidents arise. Please provide such contact information via email to security@unc.edu or via Remedy ticket. Please keep in mind that incidents can occur any day of the week and any time of day. If ISO staff cannot reach administrators responsible for the relevant system, it may be necessary to disable network access for the system to assure protection of sensitive information.
    d. Sensitive/critical systems should be listed in the “Cujo” monitor. Cujo has two components: 1) Cujo reports loss of ping responses. 2) Cujo requires a listing of escalation contacts. This contact list is very helpful in incident management. You can initiate a new Cujo entry via help.unc.edu “Submit a Request” or by calling 919-962-HELP.

5. **Testing**
   Test your incident management procedures in advance of a real information security incident and again on a regular basis thereafter.

Incident Response, Containment and Eradication Phases

1. **Identification** – The first step in incident management is to identify and confirm the incident. When an incident occurs, care should be taken to understand the scope of the incident, the likelihood of proliferation to additional systems, and the types of data that are at risk due to the incident. Incidents will be classified according to incident levels specified in the University's Incident Management Policy.

Incident Level	Examples	Investigation Type
Level 1	• Violation of UNC Acceptable Use Policy • Virus infection of end-user desktops	• Basic investigation of an incident • Remediation advice for an incident is provided • Device isolation, if necessary
Level 2	A suspected incident involving Sensitive Information stored on a system or device owned or managed by the University or hosting University Sensitive Information	Investigation of an incident *potentially* involving unauthorized access of Sensitive Information or a Mission-Critical system
Level 3	An incident involving Sensitive Information on a University-owned or managed system or device or a system hosting such University information where the initial investigation indicates a likelihood that Sensitive Information was successfully accessed by an intruder	• Investigation of a likely or confirmed breach of a system processing/storing Sensitive Information or a Mission-Critical system • Investigation of information- technology-relevant issues performed in support of criminal or civil cases, as well as University internal investigations

Table 1: Incident Levels

2. **Don't Destroy Evidence of the Unauthorized** Activity -- When incidents occur resulting in possible risk to sensitive data, it is very important that no action be taken until an incident responder from the ISO is consulted. Scans of systems should not be started because they can reset last access times, result in log rotation and can modify malware resulting in incident management delays and an increased likelihood of notification. The system should not be shut down. Malware should not be deleted. Unauthorized accounts should not be deleted. Incident responders may need the above information/clues to help them determine the nature and extent of the incident.

   If it appears that sensitive data is actively being accessed by unauthorized parties, system administrators may disable access to terminate the unauthorized access but should not take additional steps until directed to do so by an incident handler. If the system administrator should decide to terminate access by unauthorized parties, s/he should take the minimum action necessary to disable the unauthorized access until communications with an ISO incident handler can be initiated. An example of the latter might include disabling of the network access by removing the network cable.

3. **How to reach ISO** -- If any UNC-Chapel Hill affiliate believes sensitive data to be in danger as a result of an information security incident, s/he should call the Information Technology Response Center at 919-962-HELP or submit a critical Remedy ticket for assignment to the ITS-Security Remedy group. It is very important that you provide contact information so that you can be reached by ISO staff. If you do not provide contact information, the incident responder may need to discontinue network access to the affected systems and take other actions, including attempting to contact relevant executive management, until effective incident management communications are underway. Do not include details regarding the nature of the incident during the initial call and/or in the ticket but have the details ready when an incident responder contacts you in response to your critical ticket.

4. **Collaboration to Contain and Eradicate the Unauthorized Activity** – Once you have reported the incident, ISO staff will contact you. You should anticipate the following requests from the ISO:
   a. What types and amounts of sensitive data in danger?
   b. What business critical services would be impacted by isolation of an affected host that performs critical business functions?

Recovery

1. **System Rebuild** -- Intrusions usually result in complex alterations of systems resulting in an inability to "clean" a system. After an intrusion, systems usually need to be rebuilt, if feasible. Anticipation of this need for rebuilding and investment of the energy to plan for minimal interruption of university business processes under "Preparation" (See above) provides dividends during recovery. Complete "cleaning" of a system usually takes more time than rebuilding and results in the risk of a recurrence of the same incident.

2. **Business Continuity Planning** – Anticipation of business needs during an outage due to an information security incident and provisioning to meet those needs while systems are down can result in minimal disruption to normal business processes. During an incident, senior IT staff are likely to be fully occupied working with ISO staff to respond to the incident. Advance planning for such a situation and ways to keep normal business processes working is essential.

Lessons Learned

1. After every incident, the ISO will be available for a "lessons learned" collaboration meeting. The purpose of the meeting is to collaborate to understand the root causes of the incident and consider actions that could prevent recurrence. The purpose of the meeting IS NOT to assign blame.
2. When lessons learned meetings reveal trends that could help avoid other such incidents at UNC-Chapel Hill, ISO management may choose to share relevant information with groups such as security liaisons group.

References:

- **Campus Incident Management Policy**: http://its.unc.edu/ccm/groups/public/@its/documents/content/ccm1_033423.pdf

5. APPROVAL:

____

(Department Head or Designate)