University of Illinois
University Administration

Procedure for Reporting Security Breach Incidents

Issue Date: February 1, 2008

This procedure is to aid University Administration (UA) technology users ("User") in reporting a known or potential breach of sensitive data. When the potential for a security related event has been discovered, Users are responsible to act promptly to:

1. Contain the environment.
2. Communicate the incident to appropriate parties.
3. Cooperate with investigation and remediation efforts.

Examples of a potential breach of sensitive data include:

- A UA computer is lost or stolen.
- A worm or virus is detected on a UA system.
- A report containing personal data such as Social Security Numbers is missing from the file.
- Suspicion develops over a UA computer that was left unattended and logged in.
- A User's login credentials become compromised.
- A User abuses the access they have to personal data for their job to look at personal data not related to their job, or a User distributes personal data to others that do not have appropriate security access.

PROCEDURE

<u>Contain the Environment</u>

It is very important for Users to take immediate steps to preserve the state of a potentially compromised computer and to provide the best opportunity to assess the impact of a potential security breach. Users should follow the steps below to minimize the potential risk to other UA resources but, in general, the environment should not be disturbed until the appropriate assessment or evidence is gathered.

1. Do not shutdown the computer as is normally done via keystroke command – instead, you must turn it off with the power button. (Most modern computers will require the power button to be pressed and held for several seconds before the machine will turn off.)
2. Do not attempt to diagnose or fix the problems that you notice with the computer.
3. Do not attempt to retrieve or remove data from the drive – a complete backup will be done on the machine before any action will be taken by investigators, and data may be retrieved from the backup if needed.
4. Do not attempt to run anti-virus or anti-spam software; this action may compromise investigation of the incident.

<u>Communicate the Incident</u>

Timely and accurate reporting of security breach incidents facilitates effective remediation of the problem and compliance with laws and University policies. Users are expected to treat security breach incidents confidentially and as a high priority by following these steps:

1. Inform your supervisor immediately.
2. Immediately report the incident to AITS by calling the appropriate AITS Help Desk: Chicago 312-996-4806; Urbana/Springfield 217-333-3102. Explain that the incident is a potential security breach of high priority. The AITS Help Desk will collect pertinent details/information and notify the appropriate individuals who will coordinate the incident remediation.
3. Your supervisor then informs the appropriate UA unit head.

4. If the incident involves stolen or missing University equipment, your supervisor must report the event to University Police (local police authority if off-campus) and the OBFS Property Accounting and Reporting unit.

Cooperate with Investigation and Remediation Efforts

The University considers the loss of sensitive data a serious matter. It may take considerable time and effort to fully understand the nature of the security incident and whether sensitive data has been compromised. Information from Users is essential to create appropriate documentation for each event. Users may be asked to:

1. Participate in an incident review interview with network security personnel.
2. Assist in the discovery effort to evaluate the nature of sensitive data exposure.
3. Work with local authorities to complete official police reports.
4. Implement corrective actions as recommended by network security personnel to ensure future safeguarding of sensitive data.

Related Policies:
For more information on University policies regarding security of University data, refer to the following policies in the Business and Financial Policies and Procedures Manual:

SECTION 12.4 - Acquisition, Transfer, & Disposal of Equipment (State and Non-State)
[http://www.UA.uillinois.edu/manual/central_p/sec12-4.html]

SECTION 19.2 - Social Security Numbers
[http://www.UA.uillinois.edu/manual/central_p/sec19-2.html]

SECTION 19.5 - Information Security Policy - The University of Illinois
[http://www.UA.uillinois.edu/manual/central_p/sec19-5.html]

SECTION 19.6 - Financial Information Access and Security
[http://www.UA.uillinois.edu/manual/central_p/sec19-6.html]