Southern University Law Center
Policy #IT0013

Title: Incident Response

Authority: Department
Original Adoption: 5/7/2007
Effective Date: 5/7/2007
Last Revision: 9/17/2012

1.0 Purpose:

The policy outlines appropriate actions to minimize the consequences of a virus, malicious software, or an intrusion, and emergency response procedures and responsibilities are documented, understood, and properly executed when necessary.

2.0 Scope:

This policy applies to all SULC users.

3.0 Definitions:

User – SULC employees and students, contractors, vendors, and agents working under the auspices of the Law Center.

Computer Security Incident - An event that may result in, or has resulted in, the unauthorized access to, or disclosure of, sensitive or classified information; unauthorized modification or destruction of systems data; reduced, interrupted, or terminated processing capability; malicious logic or virus activity; or the loss, theft, damage, or destruction of any IT resource. Examples of incidents include: unauthorized use of another user account, unauthorized scans or probes, successful and unsuccessful intrusions, unauthorized use of system privileges, and execution of malicious code (e.g., viruses, Trojan horses, or back doors).

4.0 Policy:

1. Incidents involving cyber threats, such as viruses, malicious user activity, and vulnerabilities associated with highly interconnected technology, require a skilled and rapid response before they can cause significant damage to computing resources, loss or destruction of data, loss of funds, loss of productivity, and damage to the agency's reputation. These situations require that SULC have a coordinated *computer security incident* response capability.

2. It is the policy of the SULC to assure that its systems and data are safe and secure from unauthorized access that might lead to the alteration, damage, or destruction of automated resources and data, unintended release of data, interrupted service, and denial of service.

3. SULC shall have an incident response capability to handle a computer security problem that occurs and have the means for reporting incidents and disseminating incident-related information to management and users. The response capability may be internal, external, or a combination thereof. In addition, the incident response

capability must not only react to incidents, but also must have the resources to alert and educate users to pertinent risks and heighten awareness about security threats and incident-handling procedures.

4. The Incident Response Team (IRT) will be composed on an ad hoc basis – depending on the nature of the event - to determine the nature and level of severity of a computer security problem, participate in the investigation, and resolve the incident.

5. The IRT shall document its actions and use such information as the basis in building or enhancing standard responses to discreet categories of threats.

6. The SULC Security Administrator shall serve as the central point of contact for required reporting of incidents, coordinating an agency's response to an incident.

7. The SULC Security Administrator in conjunction with the SULC Information Technology (IT) Director shall act as a clearinghouse for disseminating information concerning alerts and vulnerabilities.

8. Each IRT shall report incidents and their status to the SULC Security Administrator.

9. When available, management tools will be used to monitor for incidents. Incidents involving substantial, systematic attacks or significant loss of dollars or damage to SULC property or image shall be reported to: (1) the SULC Security Administrator; (2) the SULC IT Director; (3) the SULC Fiscal Officer; and (4) the Law Center Chancellor. Events affecting operations shall be reported immediately to the SULC Security Administrator, the SULC IT Director, and the affected operational department head.

10. The IRT shall keep the SULC IT Director apprised of events as they unfold and ongoing investigations, and shall prepare a report of findings upon completion of the incident.

11. If during the course of an investigation, it appears possible that a violation of the law exists, the IRT shall inform the SULC Security Administrator and the SULC IT Director. If deemed necessary, appropriate state and federal investigative agencies will be notified.

12. The IRT shall work with investigative agencies to determine whether to gather evidence, monitor an intrusion, or allow an intrusion to continue, and which agencies shall assume jurisdiction in an incident. The IRT shall only be responsible for addressing the technical aspects of the case.

13. If the IRT finds employee, contractor, or other misconduct caused the incident, then the IRT shall request assistance from the SULC IT Director, the SULC Fiscal Office, the SULC Human Resources Officer, or contractor representative. The aforementioned management team shall determine what actions need to be taken, and they shall be responsible for completing the investigation of the employees case in conjunction with

other appropriate SULC offices and, if necessary, investigative agencies. The IRT shall only be responsible for addressing the technical aspects of the case.

14. After the incident has been resolved, a 'lessons learned' session shall be conducted so that the IRT can learn from the experience and, if necessary, update any relevant procedures. As a result of the post-incident analysis, the IRT may need to issue alerts or warnings to its constituency about certain actions to take to reduce vulnerabilities that were exploited during the incident. The IRT shall use the post-incident analysis to ascertain its effect on SULC as a result of handling and resolving the incident.

Roles & Responsibilities

SULC IT Director

The position has overall oversight for establishing and implementing the information security policies in responding to the detection of adverse events and assuring that appropriate action is taken to minimize the consequences of each such event.

SULC Security Administrator

1. Developing and disseminating information concerning the potential dangers of computer security incidents, guidelines for its control, and reporting of incidents;

2. Notifying appropriate parties as defined in this policy of computer security incidents;

3. Serving as the focal point for incident reporting and subsequent resolution;

4. Developing and issuing instructions for detection and removal of malicious software;

5. Providing guidance for determining what constitutes criminal intent and employee misconduct;

6. Establishing and implementing policy, procedures, and practices that are consistent with IT Department requirements to assure that SULC systems, programs, and data are secure and protected from unauthorized access that might lead to the alteration, damage, or destruction of automated resources, unintended release of data, and denial of service;

7. Ensuring that all SULC employees and contractors comply with this policy;

8. Ensuring that IT security requirements, procedures, and practices are provided in computer security training materials; and

9. Ensuring the establishment of IRT(s) to participate in the investigation and resolution of incidents.

10. Work with the IRT in the investigation, and resolution of events.

11. Communicating information to appropriate SULC officers regarding the identification, nature, scope, progress and resolution of incidents.

12. Collecting and reviewing incident reports.

Supervisors and Managers

Supervisors and managers shall ensure that their staffs and contractors have an awareness of their security responsibilities for reporting any computer incidents.

Employees

Employees shall report any suspected or actual computer incidents immediately to their help desk support, the SULC Security Administrator, or other designated personnel.

Incident Response Teams

An IRT shall participate in the investigation and resolution of incidents which include (but are not limited to) unauthorized access or attempts; compromise of proprietary data using electronic means; computer misuse or abuse; vulnerability of hardware or software; and loss of data or computer availability sufficient to cause mission or programmatic impact.

In addition the IRT shall:

1. Consist of a designated core group with as needed ad hoc expertise;

2. Identify computer security incidents, characterize the nature and severity of the incident, and provide immediate diagnostic and corrective actions, when appropriate. Priorities must be considered in evaluating and responding with each incident because an incident may have many possible effects, ranging from the risk to human life and safety to protecting sensitive, proprietary and scientific data, and minimizing disruption of computing resources;

3. Receive incident reports from its intrusion detection system, pro-active scans, system administrators, law enforcement officials and other sources;

4. Report all incidents to the appropriate individuals and organizations as described in the Policy section;

5. Prepare a report of findings and perform a post-incident review.

Guidelines

See SULC IT Guidelines for information related to security and security tools