| CSUN CALIFORNIA STATE UNIVERSITY NORTHRIDGE | **Information Technology Standard Operating Procedure**<br><br>Information Security Incidence Response Procedures | **Page** 1 of 8 | |
|---|---|---|---|
| | | **SOP#:**<br>90-08-004 | **Revision#:**<br>Version 6 |

| | |
|---|---|
| **Prepared by:** Hilary Baker, VP for IT<br>**Date:** August 27, 2008 | **Approved by:** CSIRT<br>**Date:** August 29, 2008 |
| **Last revised by:** CSIRT<br>**Date:** April 13, 2009 | **Last approved by:** Hilary Baker, VP for IT<br>**Date:** April 24, 2009 |
| **Last Reviewed By:** Kevin Krzewinski<br>**Date:** February 1, 2016 | |

## 1.0 PURPOSE

The purpose of this document is to outline procedures and guidelines for responding to CSUN information security incidents. This procedure allows for a coordinated response from Information Security, the Computer Security Incident Response Team (CSIRT), and others involved in investigation plus a follow-up of reported information security incidents.

## 2.0 SCOPE

This procedure applies to responses to all CSUN information security events reported to the IT information security team and covers both the CSUN and its auxiliary organizations.

## 3.0 RESPONSIBILITY

| | **Role (Title)** | **Responsibility** |
|---|---|---|
| 1 | Information Security Officer (ISO) | • Ensures that the campus incident response process for computing systems and data resources is followed.<br>• Handles the primary incident response and assigns an incident severity level.<br>• Ensures that system wide and campus notification procedures are followed.<br>• Reviews incidents potentially involving the unauthorized release of confidential or sensitive information with the CSIRT.<br>• Trains the individuals responsible for incident response inquiries.<br>• Prepare a CSIRT Interim Report as well as prepare final written report containing recommendations to the management staff of the campus unit for addressing the causes of the incident. |

| | | |
|---|---|---|
| 2 | Campus Authorizers and Managers are responsible for data oversight of the campus divisions | • Develops and maintains an adequate information security plan for paper based or computing systems within their control.<br>• Develops and maintains adequate guidelines and procedures for granting and monitoring access to confidential and sensitive information.<br>• Collects and maintains control records for those systems that contain confidential or sensitive information.<br>• Reports any information security breaches and files an initial report on the breach with the Information Security Officer.<br>• Ensures that the initial incident investigation and reporting are conducted in a timely basis. |
| 3 | Campus divisions | • Informs users who have access to confidential and sensitive information of their responsibilities to secure such data from unauthorized release.<br>• Develops and maintains data access control records in a secure environment.<br>• Establishes monitoring procedures to identify unauthorized access and abnormal activity.<br>• Reports suspected unauthorized acquisition of confidential or sensitive information to the Data Steward and the Information Security Officer.<br>• Recommends actions by the President, including notification of individuals whose confidential or sensitive information is reasonably believed to have been acquired by unauthorized individuals, based on discussions and findings of fact reported by the Information Security Officer.<br>• Monitors the progress of the Data Steward and Campus Divisions in respect to notification and remedial action authorized by the President, and formally closes the review of an incident after all remedial actions have been taken. |
| 4 | Computer Security Incident Response Team (CSIRT) | • Reviews any information security incident or information security breach that potentially involves the unauthorized access of confidential or sensitive information. The team will treat these incidents or breaches as suspected misuses of University resources.<br>• Determines whether an incident or information security breach resulted in the release of confidential or sensitive information to unauthorized individuals, based on findings by the Information Security Officer.<br>• Recommends actions by the President, including notification of individuals whose confidential or sensitive information is reasonably believed to have been acquired by unauthorized individuals, based on discussions and findings of fact reported by the Information Security Officer.<br>• Monitors the progress of the Data Steward and Campus Divisions in respect to notification and remedial action authorized by the President, and formally closes the review of an incident after all remedial actions have been taken. |

## 4.0 PROCEDURE

4.1 IT ISO will receive an incident from many areas: Help Desk, Network Operations, Campus Divisions, and the public. The IT ISO will assign the incident severity level, or assess the incident severity level assigned by the Help Desk or a member of the Office of Information Security.

4.2 **High Severity Level Incidents**

An incident that could have long-term effects on business or affects critical systems or has campus wide impact or could damage campus reputation, or is a violation of state and/or federal law. Examples include:

a. Hacking of enterprise systems or applications
b. Cyber-stalking
c. Patriot Act Violations
d. Loss or theft of Level 1 – Confidential Information
e. International, Federal, State or Local Law Violation like the following:
    i. HIPAA
    ii. FERPA
    iii. Child Pornography
f. If there is imminent danger (the act is in progress) that confidential information can be read, modified, or destroyed by an unauthorized entity or the disclosure or access has already occurred, then assign the incident severity level High.
g. If there is imminent danger of disruption of business due to information security issues or malicious acts or the disruption is in progress, then assign the incident severity High.
h. For severity High Incidents the owner(s) or /operator(s) of the affected hosts should be directed to disconnect the device/system from the network and not to use or modify the device/system in any way until Information Security has contacted them and provided instructions.

4.3 The ISO or designee will immediately contact the individual that has reported the incident to obtain an initial understanding of the scope of the incident. As needed, the ISO will call an emergency CSIRT meeting to determine appropriate next steps and the ISO or designee will prepare a CSIRT interim report, which will include a description of the incident , the number of individuals affected, and the remedial steps that will be taken to address the cause of the incident. Legal counsel will be engaged if necessary.

4.4 The ISO will inform the CIO. Either the ISO or the CIO will inform the campus President and the ISO at the Chancellor's Office.

4.5 If the decision is made to notify impacted individuals, the notification process must be approved by University Advancement and other stakeholders as necessary. The notification letter will be mailed by return receipt having the receipt responses directed to the ISO. Notifications will be sent with certified mail return receipt requested for groups involving less than fifty (50) individuals being notified. For groups larger than fifty (50) the most effective method of notification will be determined.

4.6 The liability for the costs associated with production and dissemination of the notification letter are the responsibility of the department(s) responsible for controlling access to and security of the system(s).

4.7 If notices are sent to more than 10,000 individuals, the following consumer credit reporting agencies shall be notified:

a. Experian: E-mail to BusinessRecordsVictimAssistance@experian.com
b. Equifax: E-mail to lanette.fullwood@equifax.com
c. TransUnion: Email to fvad@transunion.com with "Database Compromise" as the subject CSIRT

4.8 University Advancement will prepare talking points to use if necessary in response to campus or media questions. Talking points should be shared with the following people:

- President
- Cabinet
- ISO
- CSIRT
- Designated individuals responding to any phone calls, emails, letters, and/or walk-in traffic:
    a. In general talking points will direct faculty and staff as follows:
        i. Do not to offer unsolicited information or comments to the media
        ii. Advise the inquirer that the incident is under investigation (if this is the case)
        iii. Direct the inquirer to a web site for incident information
        iv. Direct inquirers from external law enforcement to CSUN University Police
        v. Direct inquirers from the media to the Public Relations Director

4.9 The ISO or designee will prepare a final written report to share with the CSIRT team, including recommendations to the management staff of the campus unit for addressing the causes of the incident.

4.10 **Medium Severity Level Incident**

The threat of a future attack or the detection of reconnaissance on the network systems of California State University, Northridge is considered medium severity. . Any incident that has a strong possibility to impact a large portion of the campus is considered medium. Examples include:

a. Loss or theft of Level 2 – Sensitive Information
b. Web-site Defacement
c. Personal Business operations using university resources
d. Sending spam that degrades enterprise system performance
e. Unauthorized Excessive Resource Utilization
f. Account Compromised-Faculty or Staff
g. If there is imminent danger of modification of the public's perception of the University due to information security reasons other than disclosure of personal and sensitive information or disruption of service (i.e. main web page has been modified in an unauthorized manner, but orders can still be processed), then assign the incident severity Medium.

4.11 For severity Medium Incidents the owner(s) or /operator(s) of the affected hosts should be directed to disconnect the device/system from the network but not to use, modify or update the device/system in any way until Information Security has contacted them to provide further instructions.

4.12 The ISO or designee will immediately contact the individual that has reported the information to obtain an initial understanding of the scope of the incident. The ISO will review the severity of the incident and determine if a CSIRT meeting needs to be called to determine appropriate next steps.

4.13 The stakeholders of the incident will be notified and depending upon the impact to the campus the notification process may also involve the Vice President for Information Technology/ CIO, the Vice President for University Advancement, and the President of the University.

4.14 The ISO may be a primary incident handler to complete the appropriate actions for a medium incident.

4.15 **Low Severity Level Incident**

Low incidents have an impact on only one or a few individuals. Incidents that are considered

Low Severity can be handled within IT and do not require escalation outside of IT. Examples include:

- Malware/ virus infected system connected to the campus network
- Copyright infringement violations (examples: RIAA, MPAA, DMCA)
- Unauthorized Chat/Game/File servers
- Illegal sharing of copyright material such as music, movies, and software
- An e-mail to Abuse regarding a Spam incident
- Account Compromised-Student
- If there is no imminent threat to California State University, Northridge systems, or university confidential and sensitive data, then assign the incident severity Low.

4.16 The ISO or designee will immediately contact the individual that has reported the information to obtain an initial understanding of the scope of the incident.

4.17 The ISO may assign a primary incident handler to complete the appropriate actions for a low incident.

4.18 **Process for all incidents**

All Information Security incidents will be recorded and investigated in a timely manner. Upon completion, incidents will be reviewed by management. .

a. Coordination of the incident may include but is not limited to the following:
    - Perform a preliminary analysis of the incident identifying incident cause, personal and university information at risk, collection of evidence, remedial action, and recommendations.
    - Examine incident computers or systems.
    - Remove the incident computing system from the campus network if necessary.
    - Coordinate additional assistance to provide and to preserve incident evidence.
    - Investigate information on web-site defacement.
    - Notify or alert campus users if newly reported vulnerabilities are identified on operating systems, server or services, applications, or network devices.

b. If the primary incident handler cannot be reached or does not confirm that they are responding to the incident in the necessary time, than the incident should be escalated to the ISO and then to the VP for Information Technology/CIO or designee.

c. A final report on the findings, causes, future concerns, and countermeasures will be completed upon closure of high and medium level incidents.

4.19 **Incident Numbering**

Incidents will be assigned a Case number. This number shall be used for Information Security incident tracking purposes.

## 5.0 DEFINITIONS:

Computer Security Incident Response Team (CSIRT) - The team responsible for the coordination and management of all High and some Medium incident responses. CSIRT is a team made up with members from the following Campus areas, Internal Audit, Risk Management, CSUN University Police, University Counsel, Public Relations, Information Security and the CIO.

Digital Millennium Copyright Act (DMCA) - A United States copyright law which implements two 1996 World Intellectual Property Organization (WIPO) treaties. It criminalizes production and dissemination of technology, devices, or services that are used to circumvent measures that control access to copyrighted works commonly known as Digital Rights Management (DRM) and criminalizes the act of circumventing an access control, even when there is no infringement of copyright itself.

Event - An observable occurrence; an aspect of an investigation that can be documented, verified, and analyzed.

Evidence - Data on which to base proof or to establish truth or falsehood.

Family Education Rights and Privacy (FERPA) - This privacy Act also governs how state agencies transmit testing data to federal agencies. The regulations cover violations such school employees divulging information to someone other than the child's parents about a child's home life, grades or behaviors, and schoolwork posted on a bulletin board with a grade.

Forensic Analysis - Examination of material and/or data to determine their essential features and their relationship in an effort to discover evidence in a manner that is admissible in a court of law; post-mortem examination.

Gramm-Leach-Bliley Act (GLBA) – This act provides for enhanced protection of nonpublic personal information, including health information, and for other purposes.

Health Insurance Portability and Accountability Act (HIPAA) – This act has administrative safeguards that are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system. The administrative safeguard provisions also address the information security and privacy of health data and relate to any private personal information.

Incident - An adverse event or series of events that affect information security or the ability of California State University, Northridge or its affiliates to do business.

Incident Response Management - A CSUN leadership team comprising of the Provost, Vice President for Administration/Finance, the VP of Student Affairs, Legal, and Public Relations.

Incident Response Team - A cross-functional team of technical and information security analysts that are responsible for investigation of information security incidents.

Incident Severity Levels - Level ratings for information security threat levels defined herein as High, Medium, and Low.

Motion Picture Association of America (MPAA) - The Motion Picture Association of America and its international counterpart, the Motion Picture Association (MPA) serve as the voice and advocate of the American motion picture, home video and television industries, domestically through the MPAA and internationally through the MPA.

Recording Industry Association of America (RIAA) - The Recording Industry Association of America is the trade group that represents the U.S. recording industry.

Sarbanes-Oxley Act (SOX) - This act covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure.

## 6.0 REFERENCES:

California Civil Code 1798.29 and 1798.82 to 1798.84

Policy 500-13 Security Breach of Personal Information Policy