CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

CSUSB Incident Handling Guidelines
CSUSB, Information Security Office

Last Revised: **01/30/2013**

Final

REVISION CONTROL

Document Title: CSUSB Incident Handling Guidelines

Author: Javier Torner

File Reference:

Date	By	Action	Pages
8/11/05	J Torner	Created Procedures Guide	All
02/25/06	G Pierce	Added Computer Forensic Analysis	Page 4
10/23/06	J Torner	Added DMCA Violations	Page 5
10/24/06	J Torner	Added Incident Interview Form	Page 6

Review/Approval History

Date	By	Action	Pages
			All

1.0 Incident Handling Guidelines

The following are guidelines followed by the Information Security Office for handling information security related incidents

- Computer Forensic Analysis
- DMCA-Violations-Housing
- Incident-Interview-Form-v09.doc: Incident interview form

1.1 Computer Forensic Analysis

These are the steps that need to be conducted on a forensic image using any one of the available computer forensic tools.

System Profiling Information

- Verify OS version and patch level install
- Verify version and last date of update of anti-virus software
- Extract configuration for auto-updates
- Determine and verify if system is part of a domain
- Administrator account - settings, including remote access
- Extract all user accounts
- Verify network setting - last IP-address, etc.

Define Scope of Investigation

- Malicious Code
- Policy violation
- Unauthorized access
- Attack Vector

Time Line

- Corroborate first date/time of incident
- Reconstruct sequence of events
- Correlate with independent data sources
    - Intrusion detection logs
    - Network flow logs
    - Firewall logs
    - Etc.

Summary

- Provide probable cause of incident
- Describe extent of compromise
- Provide possible mitigation strategies

2.0 Housing and Residential Life Copyright Infringements Procedure

Last Reviewed: October 2012

The following procedure has been specifically established for the Office of Housing and Residential Life in an effort to expedite the process and maintaining a consistent application of the CSUSB Acceptable Use Policy for Electronic Communication and CSUSB Housing Policy for resolving incidents associated with notices of copyright infringements. This procedure is accessible to students through the following link:

http://iso.csusb.edu:8888/infringement-procedure.html

2.1 Infringement Notices

When a notice of copyright infringement is received through the copyright agent identified on campus (copyright-agent@csusb.edu) the computer system corresponding to the claim will identified by IT staff and, after the alleged activity is confirmed, access to the network for that computer will then be restricted.

The restriction for access to the Internet may vary depending on how and from where the identified computer system gains access to the Internet. For example, the restrictions may be implemented by: blocking the MAC address associated with the identified computer, by blocking the Coyote ID, or by turning off the network port of the identified computer system.

Once access to the Internet has been restricted, an e-mail message with the particulars of the case will be sent to an e-mail distribution list which will distribute the information to:

- Housing and Residential Life Director
- Housing and Residential Life Associate Director
- Housing and Residential Life Coordinator of Judicial and Special Programs
- Telecommunications and Network Services
- Information Security Office

The user of the identified computer will be notified about the imposed restriction when the user attempts to gain access to the Internet with a web browser. The user will be redirected to a web page with information about the violation and given contact information. When possible, the user is also notified by e-mail, accessible via another device or a lab computer.

Once the block is in place, it is left up to the student to contact the Housing and Residential Life Judicial Officer.

Internet access will be restored pursuant to an e-mail originating from the Housing and Residential Life Judicial Officer, the Director, or the Associate Director. It is critically important that in order to facilitate the process all e-mails must contain the case number associated with a particular incident.

2.2 Discipline

Although these are the recommend disciplinary actions, the final decision is up to the Judicial Officer on case by case basis. The Judicial Officer can further refer the user to the University Judicial Officer for possible university disciplinary action.

The recommend Housing and Residential Life Judicial disciplinary process for DMCA infringement claims is as follows:

First Time Offense

- Internet access restricted
- User must meet with Judicial Officer
- Housing and Residential Life warning
- User must sign Agreement to Reinstate Access

Second Time Offense

- Internet access restricted for a minimum of one month up to one year
- User must meet with Judicial Officer
- User must meet with University Information Security Officer
- User is placed in Housing and Residential Life Probation
- User must sign Agreement to Reinstate Access

Third Time Offense

- Housing and Residential Life Contract Cancellation

2.3 Maintenance

This procedure will be maintained by:
Housing and Residential Life
University Information Security Officer

3.0 Incident-Interview-Form

Computer Incident Interview Form

The purpose of the interview is to determine the magnitude of a potential disclosure of confidential and personal information which involves a university computer system. It is imperative that the user of the computer system identifies as much as possible the nature and type of information they access in their day to day work related activities.

Please place a check mark on those activities that you conduct as part of your day to day operations. If there is an activity which is not included in the list, feel free to add it at the bottom of the form.

Date: _____ Location: _____

Property Tag: _____ Owner: (College/Dpt):_____

User Name: _____ Position: _____

Use Type: __Administrative Technical __Instructional __Student Lab __Other

Information Stored on the system: __Personal/Confidential __Other

Work Related Activities:
- __CMS Finance/Payroll
- __CMS Human Resources
- __Web access to Financial Aid/Work-Study
- __CSUSB Web-Mail
- __Web-Student Services
  - __DARwin
  - __Access to MyCoyote
  - __GRADE REPORT
  - __CLASS SCHEDULE
  - __CLASS CONFIRMATION
  - __BLACKBOARD
- __Other CSUSB Web Applications _____
- __Office Max
- __Procurement Card transactions
- __Travel Arrangements – Air Travel reservations
- __Hotel Registration/Car rental
- __Registration to Conferences/Seminars

Personal Activities:
- __Personal Banking
- __On-line Purchases - describe

Other Web-transactions: