CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

CSUSB Containment Guidelines

CSUSB, Information Security Office

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

Final

REVISION CONTROL

Document Title: CSUSB Containment Guidelines

Author: Javier Torner

File Reference:

Date	By	Action	Pages
03/30/05	J Torner	Created Guidelines	All
07/25/05	J Torner	Added Evidence Preservation	
08/11/05	J Torner	Added Incident Handling	
10/30/06	J Macdonell	Added Incident Containment Procedure	
08/01/07	J Macdonell	Added Incident Interview	

Review/Approval History

Date	By	Action	Pages
			All

1.0 Incident Notification

The following are general guidelines when sending notification for security incidents to the owners or custodians of computer or information systems.

However, when security incidents involve violations of state or federal laws, CSU or CSUSB policies, notifications must adhere to the procedures outline in the corresponding CSU or CSUSB policy.

If in doubt about the nature of the incident contact the University Information Security Officer.

An e-mail template for incident notification can be found in the IncidentNotificationTemplate document.

Individual Notification of Incidents

Individual notifications are to be used for those systems which belong to a department or are under the care of an identified group on campus. The notification must include the following information:

- Identification of the system in question, such as IP-address, MAC address, port number, location, etc
- verifiable evidence in the form of an excerpt of a log file
- action taken, if any
- be sent to the technician of record
- must be copied to the immediate supervisor/manager/department chair
- must include appropriate instructions in case the system in question contains or is used to access personal information
- must be cc to security@infosec.csusb.edu
- should include a digital signature

Notification of Incidents - Multiple systems

Notification of incidents when there are multiple systems under the care of different groups on campus can be sent to the technician listserv (techs@csusb.edu) for prompt action. The notification must include the following information:

- Identification of the systems in question, such as IP-addresses, MAC addresses, port numbers, locations, etc
- verifiable evidence in the form of an excerpt of a log file
- action taken, if any
- must be sent to techs@csusb.edu
- must be copied to the help desk at helpdesk@csusb.edu
- must include appropriate instructions in case the system in question contains or is used to access personal information
- must be cc to security@infosec.csusb.edu
- should include a digital signature

Escalation

In the event that no response is received within a reasonable amount of time (typically one business day) to an incident notification then a second notification must be sent and copied to the supervisor's supervisor. A third notice is sent directly to senior management with copies to technicians and direct supervisors.

2.0 Security Event Notification Template

Below is the recommended e-mail template for notifying owners and administrators of computer incidents involving computer systems under their control. This template is intended to help to preserve evidence should it become necessary to comply with CA Civil Code 1798 (formally SB1386).

The e-mail must be sent according to the guidelines described in the IncidentNotification guidelines.

Edit the *text in brackets* to fit the corresponding information for the incident.

Subject: [SECURITY] Suspicious activity - << computer or IP >>
From: James Macdonell <jmacdone@csusb.edu>
CC: Information Security Office <security@infosec.csusb.edu>

This is an incident notification for the following computer:

139.182.xxx.yyy << mac address >> << room # >>

This computer appears to be infected with one or more Malware:

```
Latest Event           Count Signature
2013-01-17 09:15:08    2 Outdated Windows Flash Version IE
2013-01-17 12:15:41    1 pamdql/Sweet Orange /in.php?q= Hostile landing
2013-01-17 12:15:48    1 Redkit Exploit Kit 3Char PDF Request
2013-01-17 12:15:52    2 Vulnerable Java Version 1.6.x Detected
2013-01-17 12:15:53    2 RedKit Exploit Kit Java Request to Recent jar
2013-01-17 12:15:53    2 RedKit - Jar File Naming Algorithm
2013-01-17 12:15:54    1 RedKit - Payload Requested - /2Digit.html
2013-01-17 12:15:55    7 RedKit - Potential Java Exploit Requested
2013-01-17 12:15:58    1 Maxmind geoip check to /app/geoip.js
2013-01-17 12:16:20    1 TROJAN Downloader HTTP Library seen with ZeuS
2013-01-17 12:16:20    1 Windows 98 User-Agent Detected
2013-01-17 12:18:13    2 TROJAN System Detection FakeAV (INTEL)
```

This computer should be examined and may need to be disconnected from the network.

If any computer system suspected of compromise is known to contain or access personal information (such as a combination of full name and any of the following: social security number, date of birth, medical information, financial information) YOU MUST NOTIFY the Information Security Office and prevent any further access to the computer.

A concern of any computer attack is the compliance with Civil Code Sections 1798.29 and 1798.82 - 1798.84 (formally SB-1386) which require notifying individuals whose personal information may have been compromised.

http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29
http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

Please keep us informed of the status of this system. If you have any questions or concerns, please do not hesitate to reply to this e-mail.

We look forward to your reply.

Logs available upon request.

3.0 Evidence Preservation

The following are the guidelines followed by the Information Security Office for preserving evidence which may have been collected or provided as part of an investigation.

In all cases the physical evidence will be protected to maintain its integrity during its collection, during the process to produce a forensic image, and during its storage while it is under the custody of the Information Security Office.

Physical evidence as well as the results of a computer forensic analysis will not be released to anyone without the written authorization of the University Provost or its designee, or the university legal counsel, after the conclusion of an investigation.

The physical evidence as well as the results of the computer forensic analysis will be preserved as follows:

- In those instances that an investigation involves CSUSB personnel, or involves any possible legal action, the physical evidence and computer forensic analysis results will be preserved for no less than 7 years from the date the evidence was collected.

- Otherwise the physical evidence and associated results of the computer forensic analysis will be preserved for no less than one year from the date the evidence was collected. The physical evidence may be released upon request at the completion of an investigation.

- The information Security Office will not clean, delete, or destroy any information residing on any collected or provided evidence, except in extreme circumstances by a written request and at the discretion of the Information Security Officer.

4.0 Evidence Preservation Template

An email template to use in cases where collection of the hard drive (or computer itself) is anticipated or compulsory:

To: Example Tech <example tech@csusb.edu>
Cc: Example Supervisor <example supervisor@csusb.edu>
Subject: [SECURITY] Preservation of evidence (IRN: 20080808_01)

This is an evidence collection request for the following computer:

139.182.1.1 (hackedbox.csusb.edu)

{{LOGS OR OTHER EVIDENCE}}

This computer needs to be physically secured. Follow the D.U.S.T. procedure:

D) Physically DISCONNECT the computer from the network.

U) UNPLUG the power

- Do not use standard shutdown procedure
- Do not attempt to login

- Do not attempt to find any information. Any of these actions can destroy valuable trace evidence.

S) Move the computer to a SECURE location

- An occupied/locked manager's office
- An occupied/locked computer workshop

T) TELL us and arrange for evidence collection.

When the Information Security Office receives information that a computer appears to be compromised (e.g. by a virus or worm), our standard procedure is to confirm the information, notify the technicians assigned to the VLAN, and also to notify an appropriate MPP.

As with any computer compromise, there is a potential liability to the University. This is why a manager is notified in addition to a technician.

Under California law (California Civil Code 1798), the University is obligated to notify anyone whose personally identifiable information (such as social security numbers and financial account information) is reasonably believed to have been disclosed to an unauthorized third party. As part of the University's incident handling procedures, our office will work to preserve evidence to protect the liability of the University and to meet our obligations under state and federal law.

The preservation of evidence often requires the collection of the compromised computer's hard drive. This makes the compromised computer unusable for at least a few days (the time necessary to create a forensic image of the hard drive) and perhaps up to seven years.

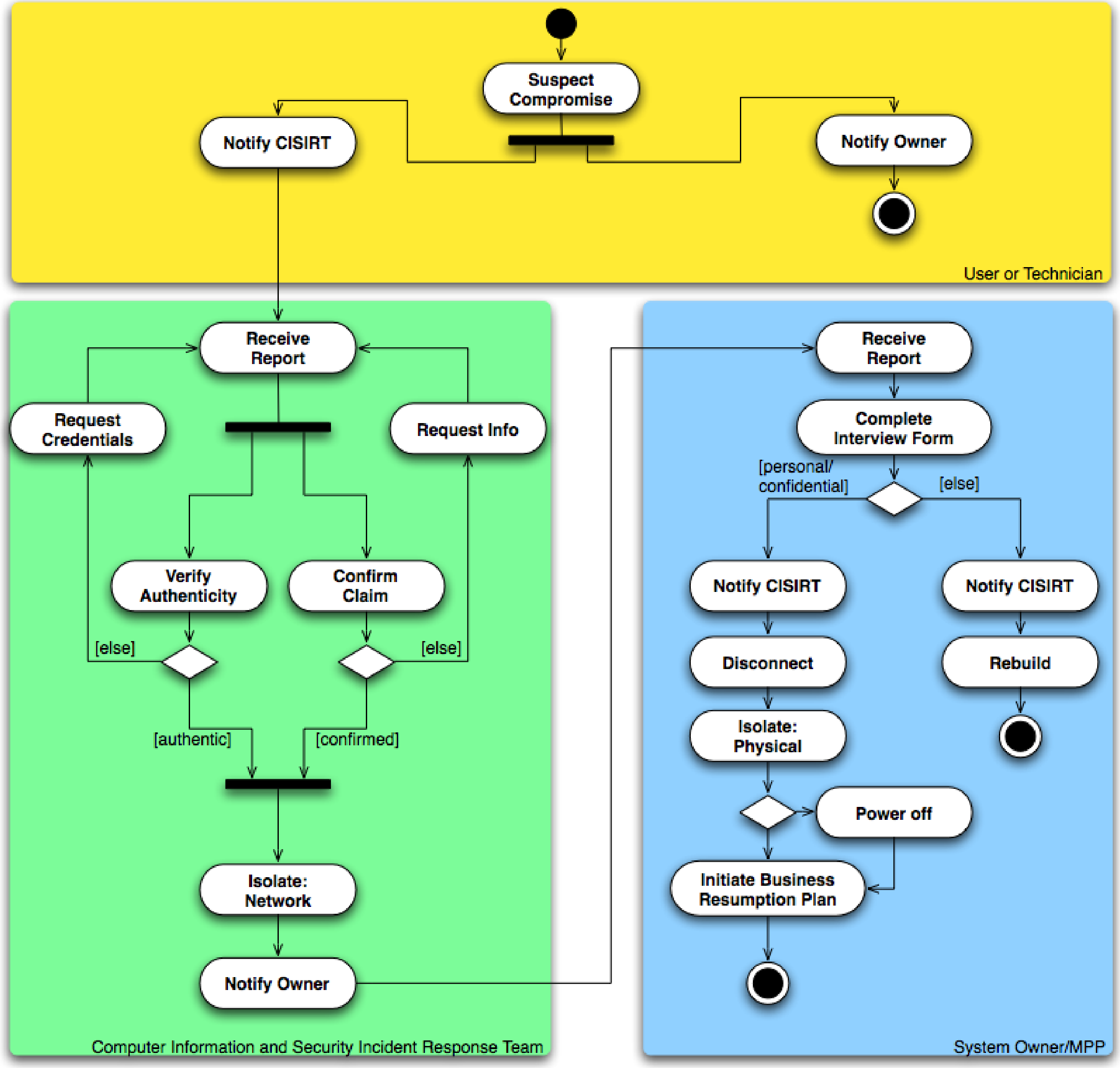
When the hard drive (or computer itself) is collected, managers are responsible for coordinating their college/division/department disaster recovery and business resumptions plans so the computer's user can regain productivity. Also, if during the course of an investigation, evidence is discovered that indicates that personally identifiable information was indeed disclosed without authorization, the manager will become involved in the decision and process to send notifications as required by law.

That said, most virus and worm infections on campus do not escalate to the point where notifications are required. The collection of evidence is most often simply a preventive measure to protect the University from future liability or lawsuits.

If you have any questions, please let us know. We look forward to your reply. Additional logs available upon request.

5.0 Incident Containment Procedure

Incident Handling: Containment and Recovery Procedures



6.0 Chain of Custody Document

NOTICE: The Information Security Office does not attempt to modify or remove files from a computer system since these systems may contain information of importance to the owner. For this reason, the responsibility to repair or remove files is left to the respective college/department computer technician.

IRN:
System Name:
Department:
Location:
Item(s):

Received from: Name Signature Date/Time

Received by: Name Signature Date/Time

Reason for change of custody: hold for possible litigation