CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

CSUSB Detection Guidelines
CSUSB, Information Security Office

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

Final

REVISION CONTROL

Document Title: CSUSB Detection Guidelines

Author: Javier Torner

File Reference:

Date	By	Action	Pages
05/30/05	J Torner	Created Guidelines	All
06/19/06	J Macdonell	Added Intrusion Detection	
11/19/06	J Macdonell	Added Event Analysis	

Review/Approval History

Date	By	Action	Pages
			All

1.0 Detection

Intrusion Detection System

The intrusion detection system encompasses many sources of information including:

- Network Intrusion detection probe (e.g. Snort)
- Network flow probe (e.g. IPflows, packet shaping logs)
- Network Firewall syslog information
- Endpoint security software reports (e.g. malware report)

The staff in the information security office routinely analyses the log activity generated by the campus intrusion detection system for signs or indicators of possible compromised system.

Any possible sign of intrusion or compromise is:

- Analyzed
- Verified
- After verification, an Incident Report case number is assigned
- Collect and save all relevant evidence following the recommended guidelines for collection of evidence
- Notify the incident Response Triage team by sending an e-mail with all relevant information to security@infosec.csusb.edu

Release of Incident Data

Extracts of incident and event information, content of log files, network flow data or any information collected as part of the intrusion detection system can only be released to a non-affected parties with approval from the University Provost or the University Information Security Officer.

Retention Policy

Incident and event information, log files, network flow data and all information collected as part of the intrusion detection system will be retained for a period of no more than 365 days after the day of collection.

2.0 Incident Handling - Event Analysis