Business Practice for Intrusion Detection

PURPOSE:

Document the use of intrusion detection systems on the Channel Islands network.

BACKGROUND:

Channel Islands T&I must take steps to protect the confidentiality, integrity, and availability of the University's information assets. To this end, Channel Islands T&I operates one or more intrusion detection systems on the Channel Islands network. Intrusion detection systems, or IDS, are designed to passively monitor the network and serve as a record of suspected intrusion events to support T&I investigations and quality assurance.

Monitoring of the University network by T&I employees to ensure quality of service, and to protect information assets, is permitted under Federal and state law, and required by the California State University Integrated State Administrative Manual, Policy 8045.500.

BUSINESS PRACTICE:

Accountability:

Manager of Infrastructure.

Applicability:

All users.

Definitions:

Text:

Intrusion detection systems

Channel Islands T&I operates one or more intrusion detection system sensors on the University network, including at least one device each in the Demilitarized Zone and the internal campus network. These devices are designed to monitor the University network looking for traffic that matches known or suspected attack patterns. Network traffic matching known or suspected attack patterns is retained by the sensor device and forwarded to a central logging server. The central logging server retains the traffic and provides for analysis and correlation with other T&I logs.

Business Practice for Intrusion Detection

IDS systems additionally provide insights into the performance and behavior of devices on the University network. A misconfigured device, or a device that has been compromised, may generate traffic that causes IDS alerts.

Use of IDS logs and retention of data

IDS logs are only used to investigate, or respond to, information security incidents, and to ensure quality of service. IDS logs are retained for not longer than thirty days. In conjunction with other logs maintained by T&I, IDS logs may be used to identify the person responsible for a network security incident.

IDS logs may contain personally-identifiable or other security-sensitive information and are treated as Confidential, Level 1 data by T&I, and will not be disclosed to anyone except as required by law or University policy. However, in cases where a University employee, member of the faculty, or student is responsible for an information security incident, T&I may disclose pertinent entries in IDS logs to the appropriate disciplinary authorities only with the express consent of the VP for Technology & Innovation.

Within T&I, access to IDS logs is limited to T&I Infrastructure personnel, the VP for Technology & Innovation, and the Information Security Officer or designee. In addition, access to IDS logs may be made available to the VISC to assist the campus in analysis and/or response.

Reviewing effectiveness

Channel Islands T&I will annually review the effectiveness of its intrusion detection systems as part of its ongoing review of its security incident response practice.

Business Practice for Intrusion Detection

Assessment Requirements

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned	Date Completed
General review of this business practice	Annual – July	Manager, Infrastructure	08/31/2010
Review of IDS Effectiveness	Annual – July	Manager, Infrastructure	

Revision History

BP Nbr:	BP-02-004	**Enacted Date:**	08/31/2010		
Revision Nbr:	001	**Revision Date:**	11/21/2012	**Revised By:**	NFisch
	002		02/02/2017		NFisch