Division Of
TECHNOLOGY &
INNOVATION

C H A N N E L
I S L A N D S

California State
University

Process Number:	BP-02-003	**Effective Date:**	08/31/2010
Approved By:	A. Michael Berman	**Page 1 of 3**	
	VP for Technology & Innovation		

Business Practice for Server Vulnerability Scanning and Configuration Management

PURPOSE:
To assure the confidentiality, integrity, and availability of CSU Channel Islands information assets by regularly assessing the University's network and information systems for vulnerabilities and insecure configuration.

BACKGROUND:
The University is required by CSU system-wide policy to protect its information assets. An industry best practice in information security is regular assessment of the computing environment for security vulnerabilities and insecure configurations. T&I will scan the University network, including non-University-owned hardware connected to the network, on a regular basis. Scanning for vulnerabilities and insecure configuration will occur only on University-owned hardware.

BUSINESS PRACTICE:

Accountability:
The Vice President for Technology and Innovation (CIO).

Applicability:
General scanning: all hardware connected to the University network whether University-owned or not.
Vulnerability and secure configuration scanning: all University-owned hardware.
All users of networked information resources at CSU Channel Islands, the Security Incident Response Team, and T&I system administrators.

Definitions:
SCAP. Security Content Automation Protocol pronounced "S Cap", is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance).

SCCM. Microsoft's System Center Configuration Management is a systems management software product developed by Microsoft for managing large groups of computers running Windows NT, Windows Embedded, macOS (OS X), Linux or UNIX, as well as Windows Phone, Symbian, iOS and Android mobile operating systems. Configuration Manager provides remote control, patch management, software distribution, operating system deployment, network access protection and hardware and software inventory.

Text:
In order to ensure the confidentiality, integrity, and availability of the University's information assets, T&I will implement the following procedures.

Address space scans

Channel Islands T&I operates one or more address space scanning appliances. T&I will regularly scan the entirety of the University's address space to create and maintain an inventory of connected devices. These scans are non-invasive and will not affect properly configured systems.

For purposes of this business practice, "University's address space" includes—
(1) All internal Internet Protocol (IP) addresses, including those address spaces allocated to University auxiliaries and departments, and those addresses allocated to University wireless networks, and
(2) All externally-facing Demilitarized Zone (DMZ) IP addresses assigned to the Channel Islands campus.

These scans will retain the following information about devices discovered for use by T&I personnel in the performance of their duties:
(1) The date and time of the device's discovery,
(2) The IP address of the connected device,
(3) The Media Access Control (MAC) address of the connected device, along with the mapping of the MAC address to the device's manufacturer,
(4) A list of open Transmission Control Protocol (TCP) and Universal Datagram Protocol (UDP) ports on the device, and
(5) The scanning device's best guess as to the device's operating system.

System vulnerability scans

Certain systems operated by T&I contain information or provide services critical to the University's operation. These systems will be periodically scanned for software vulnerabilities. Channel Islands T&I operates one or more vulnerability scanning appliances for this purpose.

Vulnerability scanning is a more intrusive process than address space scanning and will only be applied to a University-owned system with notice given to the administrator.

Automated regular vulnerability scans will not be applied to non-University-owned systems connected to the University network.

OS Configuration scans

Operating system configuration has the potential for securing a system from unauthorized access when applied appropriately, or allowing unauthorized access to the systems they run on when applied improperly. As a result, secure configurations must be applied appropriately to all University-owned hardware, re-assessed on a regular basis, and properly change managed.

Channel Islands utilizes the secure NIST approved configuration Security Content Automation Protocol (SCAP) templates for all of the operating systems for their University-owned hardware. These templates are downloaded, reviewed and modified as necessary to securely accommodate the University's business practices without impeding those practices.

Channel Islands utilizes Microsoft's (System Center Configuration Manager) SCCM product to distribute new or updated configurations, add or remove software as prescribed, as well as build hardware and software inventories.

OS Configuration Change Management

Change management of approved secure server or workstation configuration template values located in SCCM shall be administered using the existing CI change management process, **BP.00.002 – T&I Change Control.**

Incident vulnerability scans

In the event of a threatened, suspected, or actual security event or incident, Channel Islands T&I may employ a vulnerability scan against any device connected to the University network. A reasonable effort, commensurate with the severity of the ongoing incident, will be made to contact the owner or administrator of the system being scanned.

Reviewing scan results
Channel Islands T&I will review the results of address space scanning. This information will be used to assess demographic information about the University's computing environment, such as the types and kinds of devices being operated on the University network. This information will also be used to note changes to the computing environment. The information may also be used in response to an incident for containment or forensic purposes.

Channel Islands T&I Security Incident Response Team (SIRT) will review the results of system vulnerability scans on a monthly basis. The information will be used to assess and mitigate security risks on the scanned systems.

Attachments:
SCAP definition information
BP.00.002 – T&I Change Control

Assessment Requirements
Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned
Annual review of business practice	Annual	Director, Infrastructure Technology

Revision History

BP Nbr:	BP-02-003	**Enacted Date:**			
Revision Nbr:	001	**Revision Date:**	08/14/2017	**Revised By:**	Neal Fisch