Channel Islands
CALIFORNIA STATE UNIVERSITY

DIVISION OF BUSINESS AND FINANCIAL AFFAIRS
Information Technology Services

Process Number: BP-02-003 **Effective Date:** 08/31/2010
Approved By: James August **Page 1 of 3**
AVP for Information Technology Services

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. ITS will scan the University network, including non-University-owned hardware connected to the network, on a regular basis. Scanning for vulnerabilities and insecure configurations will occur only on University-owned hardware.

BUSINESS PRACTICE:

Accountability:

The Associate Vice President for Information Technology Services (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 ITS 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).

MECP: Microsoft's Endpoint Configuration Manager, is a systems management software product developed by Microsoft for managing large groups of computers running Windows OS, Windows Server, MacOS (OS X), Linux or UNIX, and mobile operating systems. MECP provides remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory.

Text: To ensure the confidentiality, integrity, and availability of the University's information assets, ITS will implement the following procedures.

Address space scans

CSU Channel Islands ITS operates one or more address space scanning appliances. ITS 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, those addresses allocated to University wireless networks, and
(2) All externally-facing Demilitarized Zone (DMZ) IP addresses are assigned to the CSU Channel Islands campus.

These scans will retain the following information about devices discovered for use by ITS 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 ITS contain information or provide services critical to the University's operation. These systems will be periodically scanned for software vulnerabilities. CSU Channel Islands ITS 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.

CSU 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.

CSU Channel Islands utilizes Microsoft's Endpoint Configuration Manager, MCEP, to distribute new or updated configurations, add or remove software as prescribed, and 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 – ITS Change Control*.**

Incident vulnerability scans
In the event of a threatened, suspected, or actual security event or incident, CSU Channel Islands ITS 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
CSU Channel Islands ITS 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.

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

Attachments:
SCAP definition information
BP.00.002 – ITS Change Control

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

Description	Frequency	Role Assigned
Annual review of business practice	Annual	Chief Information Security Officer

Channel Islands
CALIFORNIA STATE UNIVERSITY

DIVISION OF BUSINESS AND FINANCIAL AFFAIRS
Information Technology Services

Revision History

BP Nbr:	BP-02-003	**Enacted Date:**			
Revision Nbr:	001	**Revision Date:**	08/14/2017	**Revised By:**	Neal Fisch
	002		11/15/2023		Carlos Miranda