Channel Islands
CALIFORNIA STATE UNIVERSITY

DIVISION OF BUSINESS AND FINANCIAL AFFAIRS
Information Technology Services

Process Number:	BP-02-006	**Effective Date:**	08/25/2017
Approved By:	James August AVP for Information Technologies Services		**Page 1 of 2**

Business Practice for Patch Management

PURPOSE:

To assure the confidentiality, integrity, and availability of CSU Channel Islands information assets by regularly assessing the University's patch management practices and administration for efficacy and timeliness.

BACKGROUND:

The University is required by CSU system-wide policy to protect its information assets. One industry best practice in information security is the regular assessment and implementation of software and hardware patching of all computing devices within the computing environment.

BUSINESS PRACTICE:

Accountability:

Associate Vice President for Information Technology Services

Chief Information Security Officer

Applicability:

All University-owned hardware connected to the University network

Definitions:

Patch. A patch is a software designed to **update** a computer program or its supporting data to **fix** or improve it. This includes fixing security vulnerabilities and other bugs and improving the usability or performance with such patches, usually called **bugfixes** or bug fixes.

Process Number: BP-02-006 **Effective Date:** 08/25/2017

Approved By: James August
AVP for Information Technologies Services

Page 2 of 2

Business Practice for Patch Management

Patch Management: Patch management is a strategy for managing patches or upgrades for software applications and technologies. A patch management plan can help a business or organization handle these changes efficiently.

Text:

General

Information Technology Services (ITS) will implement the following regular patch management practices to ensure the confidentiality, integrity, and availability of the University's information assets.

Regular patch management practices

ITS will regularly test and apply available software and hardware patches across the University environment for University-owned computing devices, using an industry-accepted standard for patch management. Patch management and administration will follow CSUCI's existing standard change control practices (see BP.00.002).

The University currently utilizes Microsoft's Endpoint Configuration Manager (MCEP), as its patch management system.

Assessment Requirements

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned
Assessment of business practice	Annual	CISO

Revision History

BP Nbr:	BP-02-006	**Enacted Date:**			
Revision Nbr:	001	**Revision Date:**	11/15/2023	**Revised By:**	Carlos Miranda

REV-7/2012