Interim Vulnerability and Patch Management Policy

CSU Bakersfield Policy

Document Number:	ITS-90.028	**Last Revision Date:**	3/27/2023
Responsible Office:	Information Technology Services	**Effective Date:**	2/8/2023
Primary Author:	Chief Information Security Officer, CIO & AVP of Information Technology		

General Description

Purpose:

This document provides the processes and guidelines necessary to first maintain the integrity of the network systems and university data by applying the latest operating system and application security updates/patches in a timely manner, and secondly establish a baseline methodology and timeframe for patching and confirming patch-management compliance. Desktops, laptops, servers, applications, and network devices represent access points to sensitive and confidential University data as well as to technology resources and services. Ensuring that security updates and patches are distributed and implemented in a timely manner is essential for mitigating malware, exploitation, and other threats.

Definition:

VSS Score - The Common Vulnerability Scoring System provides a numerical (0-10) representation of the severity of an information security vulnerability. CVSS scores are commonly used by infosec teams as part of a vulnerability management program to provide a point of comparison between vulnerabilities and to prioritize remediation of vulnerabilities.

CVSS Score	Qualitative Rating
	None

0.0	
0.1 - 3.9	Low
4.0 - 6.9	Medium
7.0 - 8.9	High
9.0 - 10.0	Critical

High-Risk Workstation / Server – An endpoint or server that has access to Level 1 data or a large number of PII records as defined by the CSU Information Security Policy ISO Domain 6: Organization of Information Security

Scope:

The processes addressed in this document affect all managed campus systems, including desktops, laptops, servers, network devices, and applications that connect to the campus network.

Policy/Procedure

Responsibility

Role (Title)	Responsibility
Information Security Officer (ISO)	Review and approve changes to policy in regards to patch management, controls, or reports. Approve exception reports
Deputy Chief Information Officer	Review and approve changes to the patch management process.
Information Security Analyst /Administrator	Maintain the vulnerability scanning tool; conduct periodic scans of critical systems to identify known vulnerabilities, provide monthly reporting statistics, assist in identifying critical service updates.
Network Engineer/Analyst	Maintain asset inventory, install patches; review network device hardware configurations.
Desktop Administrator	Maintain asset and application inventory, install patches; generate and review patch reports at least monthly, remediate vulnerabilities on systems that cannot be patched to resolve known vulnerabilities.
Server Administrator	Maintain asset and application inventory, install patches; generate and review patch reports at least monthly, remediate vulnerabilities on

	systems that cannot be patched to resolve known vulnerabilities.
Change Control Team	Review and approve centrally-deployed patches prior to deployment
System Users	Ensure that their device(s) are connected to the CSUB network, remain powered on and regularly rebooted in order to receive all patches and updates.

Policy/Procedure

Any patch or hotfix released by a vendor identified by the vulnerability management system as critical, with a CVSS score of 9.0 or higher should be tested and deployed out of the regular patching maintenance window (out-of-band) within no more than one month of the vulnerability being identified by the vulnerability management system. If a patch is not available to resolve a vulnerability a secondary remediation to limit the risk is also acceptable.

If testing indicates that remediation cannot safely be deployed in the environment within that one-month timeframe, an exemption request will be sent to the Information Security Officer (ISO) and they will need to provide a waiver with an appropriate time frame to extend the remediation.

Security	Description	Service Level High-Risk/Servers	Service Level All others
Critical	Critical vulnerabilities have a CVSS score of 9.0 or higher. They can be readily compromised with publicly available malware or exploits.	30 days	60 days

High	High-severity vulnerabilities have a CVSS score of 7.0 or higher or are given a high severity rating by PCI DSS V3. There is no known public malware or exploit available.	45 days	90 days
Medium	Medium-severity vulnerabilities have a CVSS score of 6.0 to 7.0 and can be mitigated within an extended timeframe	120 Days	180 days
Low	Low-severity vulnerabilities are defined with a CVSS score of 4.0 to 6.0. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented in properly excluded if they cannot be remediated.	180 days	240 days
Informational	Informational vulnerabilities have a CVSS score lower than a 4.0. These are considered risks but are generally reference information for the state and configuration of an asset.	N/A	NA

Meetings and Reporting

Regularly scheduled vulnerability meetings will be held at a minimum of once a month. These meetings should include Information Technology Services Security, Desktop Support, and Infrastructure Services teams. At these meetings, reports will be reviewed and any outstanding patching items will be addressed.

Regularly scheduled weekly reports will be sent to Information Technology Services management for their review of compliance with this policy.

Desktops / Servers

As made available, download patches from a trusted source, Microsoft, Adobe, Apple, Dell, VMWare, etc.

Test patches to identify adverse effects.

Input a Change Control Request ticket and discuss at the weekly change control meetings. Follow the Emergency Change Control process for critical security patches that require immediate attention.

Communicate to stakeholders.

Deploy patches campus-wide:
A. Windows Workstations:

- i. At least once per month.
- ii. Critical security patches that resolve a known vulnerability: Deploy as soon as possible following release.
- iii. High-Risk Workstations must have all medium or higher vulnerabilities addressed within 30 days of release.

B. Macintosh Workstations:

- i. At least once per month.
- ii. Critical security patches that resolve a known vulnerability: Deploy as soon as possible following release.
- iii. High-Risk Workstations must have all medium or higher vulnerabilities addressed within 30 days of release.

C. Windows Servers

- i. At least once per month.
- ii. Critical security patches that resolve a known vulnerability: Deploy as soon as possible following release.
- iii. High-Risk Servers must have all medium or higher vulnerabilities addressed within 30 days of release.

D. UNIX/Linux Servers:

- i. At least once per month.

- ii. Critical security patches that resolve a known vulnerability: Deploy as soon as possible following release.

- iii. High-Risk Servers must have all medium or higher vulnerabilities addressed within 30 days of release.

Network Hardware/Devices (Routers, Switches, etc.)

Download patches as available. Patch notifications originate from vendors (Cisco, Aruba, etc.)
Test (where a test environment is available).
Adhere to the campus Change Control Review process for release to production.
Implement.
Review device configurations to identify known and potential vulnerabilities.

Printers / Scanners or other network-attached devices

All things that comprise or connect to CSUB network must apply security updates to all code that resides on it, based on the vulnerability risk and remediation schedule. If a security update does not exist to remediate the vulnerability within the associated timeframe, additional mitigating controls must be implemented to reduce the risk to an acceptable level.

Unpatched Systems

Any system that fails to meet this policy and contains unpatched vulnerabilities aged longer than policy allows and that has not received an exception from the Information Security Officer will be blocked from joining the network or accessing campus computing resources until such time the appropriate patches are applied and compliance with policy has been verified.

Management Tools

The campus Information Technology Services Department utilizes management systems to keep the campus-owned and managed computers patched. If a computer has not checked into one of these management systems for more than 30 days, that computer will be subject to being blocked from joining any network including the internet. The block will remain in place until the user has contacted the ITS Support Center and they can verify that the computer has been connected to the management system and brought back into compliance with this policy. The ITS Support Center will validate that the computer has, in fact, connected to the management systems and will unblock the computer.

Specialty Software

University Staff may, as a part of their job duties, install and run applications or tools unique to their role on approved devices that are not centrally managed by ITS given approval through the Information Security Office (ISO) as well their respective management (MPPs).

These tools, applications, and IOT devices may not have their vulnerabilities tracked by the campus vulnerability management system. In those cases is the responsibility of the application owner or administrator to verify with the vendor on a monthly basis any patches or upgrades that need to be installed.

These staff members, having been granted local system administrative rights on their workstations, have the responsibility to keep their applications and tools up to date in accordance with this policy.

Exemption Process

Patches on production systems (e.g. servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. Any systems that transmit or store protected data and cannot be patched to resolve a known vulnerability in a timely manner will be brought to the attention of the data owner (typically the IT Manager/Director for that department) and to the campus Information Security Officer (ISO) through the exemption process.

- Systems or applications that cannot be patched to resolve a known vulnerability will have the justification documented in an exception request by the device/application owner. The request will document the systems impacted, the identified vulnerabilities, the business justification, any necessary compensating control(s), and the duration for the exemption.

- The Information Security Officer, along with the Security Team and Infrastructure Services team will review the outstanding exception requests at least monthly.

- Exemptions must include an expiration date where the issue will be remediated by and no exemption will be granted for longer than a one-year period.

Only the Information Security Officer (ISO) upon advice from the Information Technology Services Security team can evaluate and accept the risks presented by non-compliant computing systems and will determine the actions required to address them.

The Information Technology Services department is authorized to limit network access to anything or anyone connected to or using CSUB network in any case where University resources are actively threatened or fail to comply with this policy. Information Technology Services will act in the best interest of the University by securing the resources in a manner consistent with the Information Security Incident Response Plan and minimization of threats to information systems.

Review (Frequency and Process)

This policy shall be reviewed every two years by the Associate Vice President & CIO or a designate and provided to the Vice President of Business and Administrative Services for approval and then to Cabinet for final approval.

Related Documents

Related Content:

CSU Security Policy ISO Domain 12: Operations Security Policy
NIST Guide to Enterprise Patch Management