Title:	Patching and Vulnerability Management Procedure

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:	4/7/2023		
Related Policies or Procedures:	EWU 901-02: Appropriate Use of University Resources EWU 203-01: Information Security Policy Network and Security Monitoring Procedure Change Management Procedure Campus Outage Notification Procedure NIST SP 800-40 - Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology		

History

Revision Number:	**Change:**	**Date:**
1.0	Initial version	4/3/2023

A. Purpose

This procedure defines the patching and vulnerability practices for Eastern Washington University Information Technology. The purpose of this procedure is to ensure that vulnerabilities are mitigated and university systems are secured.

B. Definitions

Chief Information Security Officer (CISO) **-**The CISO is responsible for the University's information security program and for ensuring that policies, procedures, and standards are developed, implemented and maintained

Information Resources - Any information in electronic, audio-visual or physical form, or any hardware or software that makes possible the storage and use of information.

C. Procedure

1. Applicability

This procedure applies to all individuals that are responsible for the installation of new information resources, the operations of existing Information Technology resources, and individuals charged with Information Technology resource security.

2. Scope

This procedure applies to all IT assets, endpoints, infrastructure, systems, and networks under control of the university, including cloud assets.

3. Monitoring Activities

Responsible staff must conduct ongoing external threat intelligence gathering and sharing which at a minimum includes identification and use of threat intelligence feeds.

3. Identification and Prioritization Activities

Upon notification or discovery of vulnerable resources, responsible Information Technology staff will prioritize vulnerabilities for remediation based on criticality and likelihood of exploit using the CISA Known Exploited Vulnerabilities (KEV) Catalog and classification table. Vulnerabilities not listed in the catalog will be treated as critical vulnerabilities. The remediation timeline starts from the date the vulnerability is identified.

Vulnerability Classification	**Description**	**CVSS Rating**	**Remediation Timeline**
Critical	Indicates flaws could be easily exploited by an unauthenticated remote attacker and lead to compromise.	9.0 – 10.0	Within 3 days
High	Indicates local users can gain privileges, allow unauthenticated, remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service.	7.0 – 8.9	Within 30 days
Medium	Indicates flaws may be more difficult to exploit but could still lead to compromise under certain circumstances.	4.0 – 6.9	Within 180 days
Low	Indicates Vulnerabilities require unlikely circumstances to be able to be exploited or where a successful exploit would cause either no adverse effect or result in minimal adverse consequences.	Below 4.0	Within 365 days during normal maintenance cycles.

4. Remediation

After confirmation of a vulnerability, Information Technology staff will remediate the vulnerability using vendor security patches, system configuration changes, application modifications, or other appropriate mitigation strategies. All changes are documented according to our change management procedure.

Once the remediation steps have been performed, a confirmation scan of the information resource will be performed to ensure that the actions were successful. If the confirmation scan reveals that the patch or mitigation was unsuccessful, further action will be taken to remediate the vulnerability.

5. Compensating Controls

If the vulnerability cannot be patched and remediation is not possible, Information Technology must harden the affected information resource to reduce the probability of vulnerability exploitation. This is not a substitute for replacement or upgrade, which should occur as soon as possible.

6. Regular Patching Activities

All information resources must be patched on a regular basis, including hosted or vendor managed systems. All systems will be patched at least monthly, but may be patched more frequently commiserate with business criticality and risk. Patching of hosted and vendor managed systems will be coordinated with the appropriate vendor consistent with the applicable service level agreement or contract.

7. Documentation

Patch management procedures will follow established Information Technology Change Management practices, including evaluation, validation, and stakeholder sign-off.

8. Communication

Coordination and scheduling with stakeholders for patching activities will follow established Information Technology Campus Outage Notification practices.

9. Exceptions

Test resources and networks must conform to the requirements of this procedure. The only exceptions to this policy must be related to pedagogical use and must be isolated from all other university resources.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.