PATCH MANAGEMENT STANDARD (SEC-S001)

Austin Peay State University

1.0 OBJECTIVE:

1.1 Austin Peay State University (APSU) is responsible for ensuring the confidentiality, integrity, and availability of data stored on its systems. APSU has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of university systems and data, both on premise and in the Cloud. Effective implementation of this standard will reduce the likelihood of compromise from a malicious threat actor or threat source as well as preserving the stability of production systems. This document describes the requirements for maintaining up-to-date operating system and application versions and patches on all university computing resources.

2.0 RESPONSIBILITY:

2.1 Director, Information Technology Security

3.0 APPROVAL AUTHORITY:

3.1 Chief Information Officer

4.0 SCOPE:

4.1 This standard applies to all university computing resources and the administrators that support these resources. This includes systems that contain university data regardless of location. The processes addressed in this standard affect all managed campus systems, including desktops, laptops, servers, network devices, security appliances, and applications that connect to the campus network.

5.0 REQUIREMENTS:

5.1 Endpoints - Patching and Upgrades

a. As patches are made available, download from a trusted source.
b. Test patches to identify adverse effects.
c. Deploy patches campus-wide:
    i. All university owned endpoints will be maintained with the latest security patches to their operating systems and applications.
    ii. All high/critical patches must be applied as soon as possible and shall not exceed thirty (30) calendar days.
    iii. In cases where patching cannot follow the standard as outlined above, an exception report must be made to the Director of IT Security. All deferred patches will be reviewed quarterly.
d. OIT endpoint administrators will develop and implement Procedures to ensure proper implementation of server and endpoint patching.
e. OIT endpoint administrators will develop and implement Procedures to ensure operating systems and applications are maintained to versions that are vendor supported for critical and security vulnerability updates.

5.2 Servers - Patching and Upgrades

a. As patches are made available, download from a trusted source.
b. Test patches to identify adverse effects.
c. Deploy patches campus-wide:

i. All university owned servers will be maintained with the latest security patches to their operating systems and applications.
ii. All high/critical patches must be applied as soon as possible and shall not exceed thirty (30) calendar days.
iii. All medium/high criticality patches must be applied within sixty (60) calendar days.
iv. Any low criticality patches will be installed on a case-by-case basis.
v. In cases where patching cannot follow the standard as outlined above, an exception request must be made to the Director of IT Security. All deferred patches will be reviewed quarterly.
vi. All patches for vendor maintained systems and/or applications that are labeled high/critical must also be patched within thirty (30) days of the approved release from the vendor. The operating unit is responsible for maintaining knowledge of these patches and ensuring that vendors comply with this standard.

d. OIT server administrators will develop and implement Procedures to ensure proper implementation of server and endpoint patching.
e. OIT server administrators will develop and implement Procedures ensure operating systems and applications are maintained to versions that are vendor supported for critical and security vulnerability updates.

5.3 Network Devices and Security Appliances - Patching and Upgrades

1. All university network devices and security appliances should be patched immediately for any critical or security vulnerabilities. OIT network administrators must routinely monitor the various network and security vendors with devices resident on the university network for critical or security vulnerability alerts and apply the appropriate patches as soon as possible based on best practices and professional judgement.
2. Upgrades to network devices and security devices will be implemented in a timely manner at the discretion of the OIT network administrators. Care should be taken to ensure network devices and security appliances are not allowed to be more than two versions out of date.
3. OIT network administrators will develop and implement Standard Operating Procedures (SOPs) to establish the mechanism to identify vendor released patches and updates and to ensure the proper implementation of network devices and security appliances patching and updates.

5.4 Enterprise Resource Planning (ERP) and Oracle Systems - Patching and Upgrades

1. All university ERP systems and applications should be patched for any critical security vulnerabilities. Enterprise Applications management should ensure that ERP, Oracle and associated applications are monitored for critical patch availability.
2. Patching of ERP systems should be implemented in a timely manner and with time allowed for the following of change management best practices, test configuration, and user testing and validation.
3. Oracle databases should be patched within 91 days of each quarterly release and ERP systems should be behind in versions no farther than one quarterly release.
4. OIT application managers will develop and implement SOPs to ensure the proper implementation of information security patching and updates.

5.5. Patch compliance Review Procedures

1. Endpoint and server administrators will generate and review patch management and compliance reports at least monthly. These reports will be maintained in a secure area accessible to OIT staff. Unpatched computers that are identified as unpatched that connect to the campus network will be patched or reported to the Director of IT Security as exceptions.
2. Network administrators will generate and review patch management and compliance reports at least quarterly. These reports will be maintained in a secure area accessible to OIT staff. Unpatched devices that are identified as unpatched that connect to the campus network will be patched or reported to the Director of IT Security as exceptions.
3. Reports of deferred patches will be reviewed quarterly by the Director of IT Security along with the appropriate OIT administrators to determine progress towards completing implementation, or (in cases where implementation is not viable) to assess the risk to the university and to establish compensating controls. This process will be documented and maintained in a secure area accessible to OIT staff.

6.0 ASSOCIATED DOCUMENTS:

6.1 INF-P001, INF-P002, INF-P003, INF-P004, INF-P005, APP-P001

7.0 RECORD RETENTION TABLE:

Identification	Storage	Retention	Disposition	Protection
OITManagers file share	Electronic	Perpetual	Delete	Electronic Back-up

8.0 REVISION HISTORY:

Date:	Rev.	Description of Revision:
12/04/2020	1.0	Initial Release

*** * * E n d o f S t a n d a r d * * ***