Salisbury University

Patch Management Policy

1. PURPOSE

Patch Management is a proactive practice designed to prevent exploitation of known vulnerabilities within an organization's IT infrastructure. An effective patch management process helps mitigate the costs of time and effort expended defending against vulnerabilities known to the information security field at large. Timely patching of known security issues is recognized as a best practice critical to maintaining the confidentiality, availability, and integrity of information systems. The time immediately after the release of a patch is a particularly vulnerable moment for organizations because the window of time between obtaining, testing, and deploying a patch to the vulnerable IT Systems is sufficient for malicious entities to attempt various exploitation strategies.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication

3. SCOPE

This policy is applicable to all **Information Technology Assets** owned and managed by Salisbury University. Information Technology Assets include systems and applications with software or firmware updates provided by a vendor or developer in response to functional or code improvements, flaw or interoperability issues, or version/feature updates.

4. BASE POLICY AND COMPLIANCE REFERENCES

SUIT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other organizations. This policy serves as SU's authoritative adaptation of these policies with specific amendments to meet the business and operational needs of the University.

Policy References

- State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy-List.aspx

- USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

5. POLICY

This policy describes an overall strategy to implement timely patch management processes within the Salisbury University Information Technology (SUIT) department. Results of vulnerability scans against critical systems must be submitted to USM internal audit for review each quarter.

5.1 Requirements for Security Patches

SUIT will establish documented patch management processes to address the deployment of **security related patches**. These processes should entail:

1. A methodology for discovering and tracking SUIT managed assets, which include ensuring all assets are inventoried properly and meet the minimum standards described in the configuration management approved baseline for hardware, software, and applications
2. Active monitoring of security sources for vulnerability announcements, patch and non-patch remediation, and emerging threats that correspond to the software within SUIT systems
3. Establishing a priority for remediation
4. Establishing a methodology of tracking updates applicable to the organization
5. Performing testing of patches where feasible within a lab environment or within a core group of test machines to ensure patch functionality within the infrastructure (in order to help ensure that updates do not cause interoperability issues)
6. Scheduling full Enterprise remediation either through automated tools to comply within a reasonable timeline
7. Addressing and remediating failed updates
8. Conducting periodic vulnerability scanning to identify non-compliant assets for remediation

5.2 Patch Management Prioritization

5.2.1 Asset Classification

In order to effectively deliver patches to systems, assets need to be identified by SUIT according to the *SU Asset Management Policy* and classified according to *SU Security Assessment Policy*.

5.2.2 Patch Category

Additionally, patch management must be prioritized based on the severity of the vulnerabilities the patch addresses. SUIT shall use the **Common Vulnerability Scoring System (CVSS)** or a directly compatible alternative to assist with prioritizing the severity of vulnerabilities. Severity scores are categorized in the table below:

Vulnerability Severity	CVSS Severity Score
High	7 – 10
Medium	4 – 6.9
Low	0 – 3.9

5.2.3 Patch Management Timeline

SUIT will assign patches a priority level based on combining the risk classification of each asset and the patch severity score. To the extent possible, the patching process should follow the general timeline in the table below unless a more specific patching procedure for a particular system is documented and approved by the CIO:

Priority Level	Patch Initiated	Patch Completed
1	Within 2 business days of patch release	Within 1 weeks of patch release
2	Within 2 week of patch release	Within 1 month of patch release
3	Within 1 month of patch release	Within 3 months of patch release

Timeliness of patch management prioritization may be impacted by several factors, including but not limited to:

- Consideration of asset classification and data affected by the vulnerability
- Stricter requirements set by regulatory standards (such as HIPAA and PCI DSS)
- Discretion of CIO or delegated authority regarding the potential risk to the environment
- Lack of connectivity to the device preventing the ability to perform patching
- Availability of a sufficient workaround that mitigates the risk presented by the patch
- Level of testing required to ensure patches do not introduce interoperability issues

5.3 Requirements for Non-Security Patches

Timely implementation of **non-security related patches** should be conducted to mitigate against degradation of functionality and/or interoperability. Examples of non-security patches include software updates to increase functionality. The applicable Patch Management Group will establish a documented patch management process to address the deployment of non-security patches. This process will meet the following requirements:

- Deployment of security patches is to be prioritized over non-security patches, where possible

- Test for the stability and functionality of patches before deployment
- Incorporate non-security patch management into the organizational configuration management process
- Require the use of the same patch management solution as for security related patches, where possible

5.4 Change Management Requirements

5.4.1 Requirements for Patch Deployment

All patch implementations will adhere to configuration management processes and approvals as documented in the *SU Configuration Management Policy*. Standard patch deployments will be classified as low-risk configuration changes and must be approved by the corresponding SUIT Director responsible for the impacted system. Campus stakeholders should be notified of any downtime or impact to functionality at least one business day prior to the change whenever possible.

5.4.2 Approved Baseline Gold Image Requirements

Approved Baseline Gold Images for servers and workstations will be updated at least biannually to maintain the timeliness of the approved baseline configuration. Updating the Gold Image helps minimizes the time spent updating the asset to the current patch cycle.

6. EXEMPTIONS

If an exemption from this policy is required, an SUIT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted**.**

7. DEFINITIONS

Term	Definition
Common Vulnerability Scoring System (CVSS)	An open framework for communicating the characteristics and impacts of IT vulnerabilities which ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.
Information Technology Assets	The collection of SU owned & managed networked devices and infrastructure systems critical to the business functionality of Salisbury University. These assets are typically inventoried and audited/accounted for periodically and include servers, virtual servers, desktop workstations, and laptops.

Non-Security Related Patch	A widely released fix for a specific problem, addresses a non-critical, non-security-related bug or a new product functionality that is first distributed outside the context of a product release.
Patch Management	The process for identifying, acquiring, installing, and verifying patches for products and systems.
Security Related Patch	A widely released fix for a product-specific, security-related vulnerability, rated by severity.

8. ENFORCEMENT

SUIT is responsible for managing security assessments for the University according to established requirements authorized in the SUIT Security Program Policy. Any systems under the policy authority of SUIT with requirements that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.