System Patching Policy

Ryan Coon

CYB-515

Dr. Edward Marchewka

October 30, 2024

**Overview:**

This policy outlines the procedures for managing software patches across all systems within the organization. The goal is to ensure that all systems are kept up-to-date with the latest security patches and software updates, minimizing vulnerabilities and risks. This policy aims to maintain a secure and reliable IT environment by proactively addressing security threats and improving system stability.

**Scope:**

This policy applies to IT personnel that is tasked with the organizations computer systems upkeep. This will serve as a guideline detailing procedures and standards that are to be followed in the patching process.

This includes but is not limited to:

* All desktop computers, laptops, and mobile devices
* Servers, network devices, and other infrastructure components
* Software applications and operating systems

**Quality Assurance Plan:**

Pre-Implementation Testing:

Patch Verification – All patches will be thoroughly tested in a controlled environment before being deployed to production systems. This includes:

Functionality Testing – Verify that the patch does not introduce new bugs or negatively impact system performance.

Security Testing – Ensure the patch addresses the intended vulnerabilities and does not create new security risks.

Compatibility Testing – Confirm compatibility with existing software and hardware.

Change Management Approval – All patch deployments will be reviewed and approved by the Change Management team to ensure they meet organizational standards and procedures.

Post-Implementation Testing:

Monitoring – System performance and security logs will be closely monitored after patch deployment to identify any unexpected issues.

Regression Testing – Perform regression testing to ensure that the patch has not introduced any new bugs or broken existing functionality.

Feedback Collection – Gather feedback from users and system administrators to identify any issues or concerns related to the patch.

**Frequency:**

Scheduled Patching:

Patches will be deployed on a regular schedule, typically on a monthly basis.

The specific schedule will be determined by the IT Security Manager, considering the criticality of the systems and the severity of the vulnerabilities addressed by the patches.

Critical Patches – High-severity patches addressing critical vulnerabilities will be deployed within 24 hours of release.

High-Severity Patches – High-severity patches will be deployed within 72 hours of release.

Medium-Severity Patches – Medium-severity patches will be deployed within 7 days of release.

Low-Severity Patches – Low-severity patches will be deployed within 30 days of release.

Emergency Patching:

Immediate Deployment – Emergency patches addressing critical vulnerabilities that pose an immediate threat to the organization will be deployed immediately, regardless of the scheduled patching cycle.

Approval Process – Emergency patches will be approved by the IT Security Manager and the IT Director.

**Patching Exceptions:**

Mitigation Controls – If a patch cannot be immediately applied due to compatibility issues or other constraints, a mitigating control may be implemented.

Exception Request – Requests for exceptions must be submitted to the IT Security Manager, outlining the reason for the exception and the mitigating control being implemented.

Requirements: Exceptions to the patching policy may be granted if:

* The patch causes significant system instability or performance degradation.
* The patch introduces new vulnerabilities or security risks.
* The patch is incompatible with existing systems or applications.

Process: Requests for patching exceptions must be submitted to the IT Security Manager and must include:

* A detailed explanation of the reason for the exception.
* A description of the mitigating control that will be implemented.
* An estimated timeframe for the mitigation.

Approval Process – The IT Security Manager will review the request and approve or deny it based on the severity of the vulnerability and the effectiveness of the mitigating control.

**Rollback/Reversal Procedure:**

Timeline – A rollback plan will be developed for each patch, outlining the steps necessary to revert to the previous system state. The rollback process should be completed within 24 hours of identifying a critical issue.

Notifications – All users and relevant stakeholders will be notified of the rollback process.

Supporting Departments – The IT Operations team will be responsible for implementing the rollback plan, with support from the IT Security team and the Change Management team.

Change Management – The rollback process will be documented and reviewed by the Change Management team to ensure compliance with organizational procedures.

**Authorizing Authority:**

Patching – The IT Security Manager is responsible for authorizing all patch deployments. Emergency patches require an additional level of approval from the IT Director.

Rollback – The IT Director will authorize the rollback of a patch in the event of a critical issue.

Organizational Notification Requirements:

Patching – Users will be notified via email of upcoming scheduled patch deployments.

Rollback – Users will be notified via email of any patch rollback, outlining the reason for the rollback and the expected impact.

**Audit Controls and Management:**

Change Management Tracking – All patch deployments and rollbacks will be documented in the Change Management system, including the date, time, patch version, and any issues encountered. This system should include a process for documenting the change, the impact of the change, and the approval chain of command for the change.

Regular Audits for Compliance and Improvement – Regular audits will be conducted to assess compliance with this policy and identify opportunities to enhance the patch management process.

Regularly Review and Update the Patch Management Policy – This patching policy should be reviewed and updated regularly to ensure it remains relevant and effective.