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 of this policy is to ensure that all systems are kept up-to-date with the latest security patches and bug fixes, minimizing vulnerabilities and maintaining system stability.

Scope:

This policy applies to all employees, contractors, and vendors who have access to or manage systems within the organization.

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:

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 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 Security Manager, outlining the reason for the exception and the mitigating control being implemented.

Approval Process: The 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: 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 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 Security Manager will authorize the deployment of all patches, except for emergency patches, which require approval from both the Security Manager and 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.

Regular Audits: Regular audits will be conducted to ensure compliance with this policy and the effectiveness of the patch management process.