6. Exceptions

    a. Exceptions to the patch management policy require formal documented approval from the Security Officer. Any servers or workstations that do not comply with policy must have an approved exception on file with the Security Officer.

    b. Please refer to the Security Officer for details on filing exceptions.

7. Implementation and Enforcement

    The Security Officer will implement this policy. Enforcement of this policy is ultimately the responsibility of all employees at [Insert Company name]. The Security Officer may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action.

8. Rollback Process

    When applying patches to critical and sensitive information system components, system administrators should create rollback procedures as appropriate.

Violations: Consequences for non-compliance may include, but not be limited to, device quarantine, disconnection from the network, or denial of access to or from applications or services.

Any individual found to have violated this policy, may be subject to disciplinary action up to and including termination of employment. Violations shall be noted in the [Insert Company name] issue tracking system, and support teams shall be dispatched to remediate the issue.

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.