Patch Management Procedure

Sits under: Patch Management Policy [version]. Owner: [Patch coordinator]. Cycle: monthly, starting on the second Tuesday.

Step 1 Keep the inventory current

Who: Patch coordinator with system owners.

Do: Reconcile discovery output with the inventory; assign an owner to every unowned asset; confirm each asset's maintenance group.

Record: Inventory snapshot dated [date]; list of assets added, removed, unowned.

Step 2 Watch for releases

Who: Patch coordinator.

Do: Check vendor advisories for every product in the inventory on the release day and again two working days later. Check the CISA Known Exploited Vulnerabilities catalog on each working day.

Record: Release log (product, advisory, release date, vendor label).

Step 3 Assess and prioritize

Who: Patch coordinator; policy owner for disputes.

Do: Match each release to affected assets; assign the policy class; set the deadline = release date + window.

Record: Assessment sheet (advisory, assets affected, class, deadline).

Step 4 Acquire and test

Who: Platform administrators.

Do: Download from the vendor's own channel; verify integrity; install on the canary set; observe for [2] working days (class 1: hours).

Record: Canary result and tester, rollback method.

Step 5 Approve and schedule

Who: System owner.

Do: Approve the deployment and the maintenance window, or state the reason for refusal; refusals go to the exceptions clause.

Record: Approval (name, date), scheduled window.

Step 6 Deploy

Who: Platform administrators.

Patch Management Policy, Patch management procedure, edition 19 Nov 2026, CC BY 4.0, https://patchmanagementpolicy.com/

Do: Install in the scheduled window in the order canary, then groups; force installation after the grace period; roll back if a stop condition is met: [list stop conditions].

Record: Deployment log per asset (installed, failed, pending, reboot required).

Step 7 Verify

Who: Platform administrators, checked by the patch coordinator.

Do: Confirm the patch is installed and has taken effect (version, rescan or attestation); chase failed and pending assets.

Record: Verification result per asset; list of assets still open at the deadline.

Step 8 Report

Who: Patch coordinator.

Do: Send the monthly report defined in policy section 8 to the executive sponsor within [5] working days of the cycle's last deadline.

Record: Report and the data export behind it.

Step 9 Review the cycle

Who: Patch coordinator, policy owner.

Do: List misses and their causes; change a maintenance plan, ring or window if the same cause occurs twice.

Record: Review notes and any change request to the policy.