STANDARD OPERATING PROCEDURE

Patch Management SOP

Document no.	SOP-IT-007
Revision	1.0
Owner	IT Security Manager
Effective date	September 15, 2026
Review cycle	Every 6 months

1. Purpose

To keep operating systems, applications and firmware current with security patches on a regular cadence, reducing exposure to known vulnerabilities while minimizing disruption to production systems.

2. Scope

Applies to patching servers, workstations, laptops and network devices, from advisory monitoring through testing, deployment and compliance verification, including expedited handling of critical vulnerabilities. Broader configuration changes follow the change management SOP.

Definitions

Critical vulnerability	A security flaw with a high likelihood of exploitation and severe impact, requiring expedited patching.
Patch window	The scheduled time during which patches are deployed to a group of systems.
Patch ring	A defined batch of systems that receive a patch together, often ordered from lowest to highest risk.
Compliance rate	The percentage of in-scope devices that have received a given patch.

3. Responsibilities

System Administrator	Tests patches, deploys them in batches, and remediates devices that miss the patch window.
IT Security Manager	Classifies patch severity, verifies compliance, and reports results.
Change Manager	Approves the patch deployment window as a standard or normal change.
End User	Restarts or makes their device available for patching when notified.

RACI matrix

Activity	System Administrator	IT Security Manager	Change Manager	End User
Classify patch severity	C	R/A	I	-
Test patches before deployment	R/A	C	I	-
Approve the deployment window	C	C	R/A	I
Deploy and monitor patches	R/A	I	I	I

Activity	System Administrator	IT Security Manager	Change Manager	End User
Verify and report patch compliance	R	R/A	I	-

R = Responsible, A = Accountable, C = Consulted, I = Informed

4. Materials and PPE

Materials, tools and systems

- Patch management console
- Vulnerability advisory feeds
- Test or staging environment
- Patch compliance dashboard
- Change request for the patch cycle

5. Procedure

Step	Task	Owner	Done
5.1	**Monitor vulnerability advisories** The System Administrator monitors vendor and vulnerability advisory feeds daily for newly released patches affecting in-scope systems.	System Administrator	☐
5.2	**Classify patch severity** The IT Security Manager classifies each patch by severity, flagging any critical vulnerability for expedited handling outside the regular cycle. **Checkpoint:** Every new advisory is reviewed and assigned a severity classification within one business day of release.	IT Security Manager	☐
5.3	**Test patches on non-production systems** The System Administrator deploys the patch to a representative sample of non-production systems and checks for functional issues before wider rollout. **Warning:** Never deploy an untested patch broadly to production, even under time pressure from a critical advisory.	System Administrator	☐
5.4	**Submit the patch cycle for approval** The Change Manager approves the regular patch cycle as a standard change, or fast-tracks a critical patch through the expedited emergency change path.	Change Manager	☐
5.5	**Schedule and notify** The System Administrator schedules the patch deployment window and notifies affected users of any expected restarts or downtime.	System Administrator	☐
5.6	**Deploy patches in batches** The System Administrator deploys patches to production systems in defined rings, starting with lower-risk systems before moving to critical ones.	System Administrator	☐
5.7	**Monitor for post-patch issues** The System Administrator monitors system health and the incident queue after each deployment ring for signs of a patch-related problem. **Checkpoint:** No new critical incidents are linked to the deployment before the cycle is marked complete.	System Administrator	☐

Step	Task	Owner	Done
5.8	**Roll back a problem patch** If a patch causes a service-impacting issue, the System Administrator rolls it back on the affected systems immediately and pauses further rollout.	System Administrator	☐
5.9	**Verify patch compliance** The IT Security Manager checks the patch management console to confirm which in-scope devices successfully received the patch.	IT Security Manager	☐
5.10	**Remediate missed devices** The System Administrator follows up on devices that did not receive the patch within the defined grace period, such as offline laptops, and forces the update.	System Administrator	☐
5.11	**Document the cycle results** The IT Security Manager documents the patch cycle results, including any exceptions and the final compliance rate.	IT Security Manager	☐
5.12	**Report compliance monthly** The IT Security Manager reports patch compliance trends to the Change Manager and leadership on a monthly basis.	IT Security Manager	☐

6. Quality checks

- Critical vulnerabilities are patched within the defined expedited timeframe.
- Patches are tested on non-production systems before broad deployment.
- Patch compliance rate is tracked and reported on a monthly basis.
- Every patch cycle has a rollback path ready before deployment begins.

7. Records

- Patch test results
- Change request or approval for the patch cycle
- Patch compliance report
- Rollback or incident record, if applicable

8. KPIs

- Patch compliance rate across in-scope devices
- Mean time to patch critical vulnerabilities
- Number of rollbacks per patch cycle
- Percentage of devices patched within the grace period

9. Common mistakes

- Deploying a patch to every production system at once instead of using rings.
- Waiting for the next monthly cycle to address a critical vulnerability.
- Not tracking which devices missed the patch window.
- Having no rollback plan ready before deploying a patch.

10. Revision history

Revision	Date	Description	Reviewed by

Revision	Date	Description	Reviewed by
1.0	September 15, 2026	Initial release	Ilia Pirozhenko

Approval

Prepared by	Approved by	Date

This is a template. Adapt it to your organization, equipment and local regulations before use.

Scan for the latest version

Opens this template online, where you can download it again in Word, PDF, Excel or CSV — free, no sign-up.

Or add it to Perfect Wiki so your team can find it and ask questions about it in Microsoft Teams, Slack, kChat or Mattermost.