

Patch Management Policy Template

A free, adaptable template covering scope, patching SLAs by severity, four patching scenarios, emergency handling, exceptions, and the evidence auditors sample. Mapped to SOC 2, ISO 27001, PCI DSS, and HIPAA.

HOW TO USE THIS TEMPLATE

Replace every [bracketed value] with your own. Delete any section that does not apply, keep the numbering, and route the final version through your normal approval process. The SLA numbers are recommended defaults, not framework requirements: only PCI DSS 4.0.1 Requirement 6.3.3 sets a deadline (critical or high-security patches within one month of release). Set numbers your team can hit every time.

Company: [Company name]

Policy owner: [Role, e.g. Security Lead]

Version: [1.0]

Effective date: [Date]

Approved by: [Name, title]

Next review: [Date, at least annually]

1. Purpose and scope

Purpose. This policy defines how [Company] identifies, tests, approves, deploys, and verifies security patches and software updates so that known vulnerabilities are closed within defined timelines and every exception is recorded.

Scope. This policy applies to every asset in the asset inventory, including:

- Operating systems on laptops, servers, and virtual machines
- Applications and browsers installed on company devices
- Firmware for laptops, routers, firewalls, and other hardware
- Cloud workloads and container images, including base images
- Third-party and open-source dependencies in [Company]'s own code
- Network devices such as VPN gateways and firewalls

Out of scope. Vendor-managed SaaS. The vendor patches these systems; [Company] collects each vendor's audit report [annually] through its vendor review process. Assets not in the inventory are not covered, so the inventory must be kept current.

Related policies. Vulnerability Management Policy (detection, scanning, risk rating), Change Management Policy (approval and emergency change records), Asset Management Policy (inventory).

2. Roles and responsibilities

Role	Responsibility
Policy owner [Security Lead]	Owens this policy, approves exceptions, invokes the emergency process, reviews the monthly report
Asset owners	Name a maintenance window, validate function after patching, request exceptions
IT / engineering	Test and deploy patches, rebuild images, merge dependency updates, record dates in the ticket
Change approver	Approves routine and emergency changes under the Change Management Policy
All personnel	Install device updates by the deadline set through device management

3. Patch classification and SLAs

Each finding is assigned a tier. Raise a finding one tier if the affected system is internet-facing. Any finding with evidence of active exploitation is an Emergency regardless of score.

Tier	What triggers it	Deploy within
Emergency	Evidence of active exploitation on an in-scope system (for example a CISA KEV listing or a vendor advisory naming active attacks)	[72] hours
Critical	CVSS 9.0 to 10.0, or CVSS 7.0 or higher on an internet-facing system	[7] calendar days
High	CVSS 7.0 to 8.9 on an internal system	[30] calendar days
Medium	CVSS 4.0 to 6.9	[90] calendar days
Low	CVSS below 4.0	Next scheduled cycle, [180] days at most

Clock rules

- **Clock starts** at detection in [Company]'s environment (the scanner, dependency tool, or advisory flags it). For systems in PCI DSS scope, count from the vendor's release date.
- **Days** are calendar days.
- **"Patched"** means deployed to every affected asset in the group and verified by a re-scan or version check, with the ticket closed with evidence. A patch queued in a console is not patched.

ALIGNMENT

These tiers match the Critical 7 / High 30 / Medium 90 remediation figures in ComplyJet's vulnerability management policy template, so the two policies do not contradict each other.

4. Four patching scenarios

Based on the risk-response scenarios in NIST SP 800-40 Rev. 4 (April 2022). Every asset belongs to a maintenance group, and every group has a plan for each scenario.

Scenario	Rule
Routine patching	Patches on a regular release cycle. Deployed in the group's maintenance window within the SLA for the tier. Tested first, with rollback ready.
Emergency patching	A vulnerability being exploited now. Follows section 6.
Emergency mitigation	No patch exists yet. Apply a temporary control: disable the feature, block the port, restrict access, add monitoring. Record it, and remove or replace it when the patch is available.
Unpatchable assets	Systems that cannot take patches (vendor does not supply them, certification blocks changes). Isolate, limit access, monitor, and track in their own maintenance group with a review date.

5. Testing and deployment

1. Obtain patches only from the vendor or another reliable source.
2. Test on a representative pilot group before broad rollout. Give priority to high-risk and business-critical systems.
3. Keep the previous software version or image available so the change can be rolled back.
4. Deploy within the maintenance window: device management for laptops, rebuild-and-redeploy for cloud workloads and containers, automated update pull requests merged within the tier deadline for dependencies.
5. Verify with a re-scan or version check and record the deployment and verification dates in the ticket.
6. Roll back and raise an exception if a patch breaks a critical system.

6. Emergency handling

- **Trigger:** evidence of exploitation, a CISA KEV listing, or a vendor advisory naming active attacks.
- **Who may invoke:** [Security Lead] or their deputy [name].
- **Testing:** a smoke test on a pilot group is acceptable. Full-cycle testing is not required.
- **Deadline:** remediate or mitigate within [72] hours of the trigger.
- **Record:** complete an emergency change record within [48] hours of deployment.
- **Review:** the policy owner reviews the count of emergency changes each quarter.

7. Exceptions

Where a whole class of assets cannot follow the standard plan, create a maintenance group with its own plan instead of listing one-off exceptions. For any remaining exception, record the following in the exception

register. Exceptions expire after [90] days at most and must be re-approved before renewal.

Field	Entry
Asset and owner	[Asset name, owner]
Vulnerability and tier	[CVE or finding ID, tier]
Reason the deadline cannot be met	[Reason]
Compensating controls	[Isolation, access limits, extra monitoring]
Approver and date	[Name, date]
Expiry date	[Date, no more than 90 days]

8. Evidence and review

Keep the following records for at least [the audit period plus one year]. The monthly report goes to the policy owner and covers SLA hit rate by tier, the age of the oldest open item, and exceptions past expiry. Review this policy at least annually and after any significant change to the technology stack.

Evidence	What it shows
Approved policy and version history	The rules exist and someone with authority signed off
Asset inventory	What is in scope
SLA report by tier	Performance measured against the policy's own numbers
Sample tickets with dates	Detection, deployment, and verification are recorded
Exception register	Every miss has an owner, a reason, and an end date
Emergency change records	The fast lane left a trail
Vendor audit reports	Vendor-managed SaaS is covered by the vendor's evidence

Framework notes

Framework	Where it lives	What it says about patching
SOC 2	CC7.1, CC8.1	No criterion names patching or sets a number. Auditors sample your SLA against tickets and change records.
ISO 27001:2022	Annex A 8.8	Obtain vulnerability information in time, evaluate exposure, take appropriate measures. No number set.

PCI DSS 4.0.1	Requirement 6.3.3	Critical or high-security patches within one month of release. Others within a timeframe set by your risk assessment.
HIPAA	45 CFR 164.308(a)(1), (a)(5)	No timeframe. Risk analysis and risk management are required; malicious software procedures are addressable.
CIS Controls v8	Safeguard 7.3	Automated OS patching on a monthly or more frequent basis.

Free template by [ComplyJet](#). Read the full guide at complyjet.com/blog/patch-management-policy-template. This template is a starting point, not legal or audit advice. Adapt it to your environment and have it reviewed before adopting.