Patch Management Policy

Owner: [Role, e.g. Head of IT]. Approved by: [Name, role]. Version: [1.0]. Effective: [date]. Next review: [date, no later than 12 months after approval].

1 Purpose and scope

1.1 This policy sets how [Company name] finds, tests, installs and verifies security patches and updates, so that known vulnerabilities in its systems are fixed inside the windows in section 4.

1.2 It covers every operating system, firmware, application, library, container image and cloud service that [Company name] owns, operates or administers, including systems run by a third party where [Company name] controls the patch schedule. Exclusions: [list each, with reason and approver]. An exclusion not listed here is not valid.

1.3 Software that no longer receives vendor security updates is removed from service or isolated and recorded under Annex A. It is not kept in service by default.

2 Roles and responsibilities

2.1 Policy owner ([role]): owns this policy, approves the windows, reports to [executive sponsor].

2.2 Patch coordinator ([role]): runs the monthly cycle, keeps the schedule and the evidence.

2.3 System owners ([role per system]): approve outage time and accept test results for their maintenance group.

2.4 Platform administrators ([role]): deploy, verify and roll back.

2.5 Executive sponsor ([role]): receives the monthly report and decides any window missed for more than [5] working days.

2.6 Third parties that administer a system must patch to these windows and report completion in writing.

3 Asset inventory

3.1 The inventory records, for every asset: owner; platform type (IT, OT, IoT, mobile, cloud, virtual machine, container); who administers it (internal, third party, shared); the tool that manages it; whether it is reachable from the internet; its maintenance group; any legal, contractual or outage limit on patching; and the date it was last patched.

3.2 An asset is added before it goes into production. Automated discovery runs at least [weekly].

3.3 An asset found by discovery that has no owner is given one within [5] working days or isolated.

4 Severity and patch windows

4.1 Each vulnerability takes the severity the vendor publishes. If the vendor publishes none, the policy owner assigns one from the organization's risk analysis. A vulnerability listed in the CISA Known Exploited Vulnerabilities catalog is class 1 whatever its vendor label. If two classes apply, the shorter window applies.

4.2 The window starts when the vendor releases the patch. If no patch exists, the window starts when one becomes available and the mitigation in Annex A applies meanwhile.

4.3 Windows:

Class	Window	Applies to
1. Known exploited, internet-facing	3 calendar days	Systems reachable from the internet
1. Known exploited, other	14 calendar days	All other systems
2. Critical	14 calendar days	All systems
3. High	30 calendar days	All systems [set 14 if you hold Cyber Essentials]
4. Medium	90 calendar days	All systems
5. Low	180 calendar days	All systems
Routine baseline	Every month, or more often	Operating system and application updates

4.4 A window that cannot be met is escalated to the executive sponsor before it expires and recorded under Annex A.

5 Testing and staging

5.1 Every maintenance group has a canary set of [number or percent] assets that receives each patch first.

5.2 A patch moves from canary to the full group after [2] working days with no incident, or sooner if the patch is class 1.

5.3 A rollback method is written down before deployment. If none exists, say so in the change record and name the fallback.

5.4 Test evidence (what was tested, by whom, result, date) is kept with the change record.

6 Maintenance windows

6.1 Standard windows by group: [group, day, hours, time zone]. The schedule is published [5] working days ahead.

6.2 Installation is forced after [number] days from the start of the window, by direct execution or by restricting network access of the unpatched asset.

6.3 Reboots needed to finish an install happen inside the same window. An asset that cannot reboot is handled under Annex A.

7 Emergency patching

7.1 The policy owner (or deputy [role]) may declare an emergency for named assets when a vulnerability is class 1, when a vendor issues an emergency update, or when the policy owner judges that waiting for the standard window is unacceptable.

7.2 While an emergency is declared, the standard windows and change lead times are suspended for the named assets only. The declaration records who declared it, the time, the assets and the reason.

7.3 Canary installation may run for minutes to hours; full installation follows in the hours or days the emergency allows.

7.4 When the patch is installed and verified, the declaration is closed and the standard windows resume.

8 Reporting and metrics

8.1 Each month the patch coordinator reports to the executive sponsor: the share of assets patched inside their window, by class and by asset importance; the mean and median days to patch; open exceptions with age; assets with no owner.

8.2 Evidence for every reported figure is exportable from [system] for [retention period].

9 Review and approval

9.1 The policy is reviewed at least every 12 months, and when a framework named in section 4 changes its timing.

9.2 Changes are approved by [role]. The approved version, date and approver are recorded on the cover.

Annex A Exceptions

Exceptions follow the exceptions clause ([insert clause text]).