Patching Policy

> **Effective May 22, 2026. This Patching Policy supersedes and replaces all prior versions.**

This Patching Policy describes how Methodology IT ("Provider") manages the deployment of operating system and application patches across managed endpoints, servers, and network devices. It is incorporated by reference into the Service Attachment for Managed Services and the Schedule of Services. Provider may update this Policy from time to time and will publish the current version.

1. Scope

This Policy covers patches issued by software and hardware vendors for the following components in scope under Client's Order:

- Windows desktop and server operating systems
- macOS, iOS, iPadOS, and Android operating systems on managed Devices
- Microsoft 365 and Google Workspace administrative configurations (where vendor-applied updates are user-controllable)
- Third-party desktop applications managed via Provider's RMM (browsers, productivity suites, runtime frameworks, common business applications)
- Server applications under Provider's management
- Firewall, switch, and wireless access point firmware
- Provider-managed security agents (EDR, DNS filter, etc.) — typically updated by their vendor in near-real-time

Vendor-managed cloud platforms (Microsoft 365, Google Workspace, hyperscale cloud) are updated on the vendor's own schedule outside of Provider's direct control.

2. Patch classification

Provider classifies patches into the following categories:

CLASSIFICATION	DEFINITION	TYPICAL SOURCES
Critical security	Patches addressing actively exploited vulnerabilities or high-severity unpatched issues	Out-of-band vendor releases, CISA KEV catalog entries, internal threat intel
Security (routine)	Vendor-classified security patches not actively exploited	Microsoft Patch Tuesday, Apple security updates, browser security releases
Functional / quality	Non-security patches, bug fixes, feature updates	Vendor cumulative updates, monthly rollups
Firmware / driver	Updates to device-level software	Vendor firmware releases, manufacturer driver updates

3. Deployment ring model

Provider uses a tiered ring deployment model to balance risk and timeliness. Each managed endpoint or server is assigned to a ring based on its role:

RING	COMPOSITION	PURPOSE
Ring 0	Provider internal infrastructure and pilot devices	Initial validation
Ring 1	Test devices and low-risk endpoints at consenting Client sites	Broad validation
Ring 2	General population of managed endpoints	Production deployment
Ring 3	Servers, mission-critical workstations, and Devices flagged by Client	Late deployment with additional verification

4. Deployment cadence

4.1 Critical security patches

Critical security patches addressing actively exploited or high-severity vulnerabilities are deployed on an **emergency cadence** outside the standard maintenance window. Notification to Client is

provided as conditions permit; for actively exploited vulnerabilities, Provider may proceed without prior notification to limit exposure, with retrospective notification.

Target deployment timing:

RING	TARGET TIMING FROM VENDOR RELEASE
Ring 0 (internal)	Within 24 hours
Ring 1 (pilot)	Within 48 hours
Ring 2 (general)	Within 7 days
Ring 3 (servers / critical)	Within 14 days (with verification)

4.2 Security and functional patches

Routine security and functional patches are deployed on a monthly cadence aligned to vendor release schedules — typically the second and fourth Tuesday-through-Wednesday window each month, during the standard maintenance window. The deployment progresses through rings over a 7–14 day period to validate stability before broad rollout.

4.3 Firmware and driver updates

Firmware and driver updates are deployed quarterly during scheduled maintenance windows, or earlier where the update addresses a security vulnerability.

4.4 Major version upgrades

Major version upgrades to operating systems and applications (Windows 11 → next major version, macOS major releases, etc.) are planned with Client and deployed outside the routine cadence. Major upgrades may be quoted as Project Services where significant compatibility testing or migration is required.

5. Reboot management

Where patches require reboot, Provider schedules reboots during off-hours where possible and after notice to Users. Devices marked as critical (Ring 3) follow Client-specific reboot policies on the Order.

6. Deferrals

6.1 Provider-initiated deferral

Provider may defer a patch when:

- The vendor has acknowledged a regression or compatibility issue;
- Testing in Ring 0 or Ring 1 reveals a stability problem;
- The patch conflicts with Client's specific applications.

Deferrals are documented and tracked; affected systems are reviewed at each maintenance window for re-deployment as conditions allow.

6.2 Client-initiated deferral

Client may request deferral of a specific patch or maintenance window with reasonable advance notice. Client-initiated deferrals do not relieve Client of its security obligations; deferred-but-required patches contribute to the security baseline drift discussed in § 7.

7. Baseline alignment and reporting

Provider maintains a security baseline aligned to the CIS Critical Security Controls and reports patch compliance as part of the regular technology business review:

- **Core tier:** Quarterly summary of patch compliance for managed endpoints and servers
- **Complete tier:** Quarterly compliance reporting included in the technology business review
- **Total tier:** Monthly compliance reporting

Systems persistently out of patch compliance — including Client-deferred patches and unsupported software — may be flagged in compliance reporting and may affect Provider's ability to deliver the Services at agreed pricing per the Minimum Environment Standards in the Service Attachment for Managed Services.

8. Exclusions

This Patching Policy does not cover:

- Unmanaged Devices not in scope under the Order
- Custom or proprietary line-of-business applications that are not part of Provider's RMM patch catalog (these require Client coordination with the application vendor)
- Application data and configuration changes (separate from binary patches)
- Major migrations and version upgrades requiring project scoping

- Vendor-managed cloud-platform updates outside Provider's direct control