MSP patch management policy

MSP variant: paste over the same-numbered sections of the general policy

1 Purpose and scope

1.1 This policy governs how [MSP name] patches systems that belong to its clients under written agreements. It covers each client's endpoints, servers, network devices and cloud tenants listed in that client's schedule.

1.2 No system is patched, rebooted or excluded without the authority recorded in the client's agreement or a written instruction from the client contact named in the schedule.

2 Roles and responsibilities

2.1 Service delivery lead ([role]): owns this policy.

2.2 Client technical contact ([named in schedule]): approves the client's maintenance window and exceptions.

2.3 Technicians: patch only inside the windows in the client schedule.

3 Asset inventory

3.1 The inventory is kept per client and records who administers each asset (MSP, client, third party) and any contractual or regulatory limit on patching.

4 Severity and patch windows

4.1 Default windows are those of the general policy, section 4.3. A client may require shorter windows. A client may not lengthen them beyond the default without a signed exception that names the systems and the end date.

4.2 The window clock runs from vendor release, whoever approves. Delay waiting for client approval is recorded and reported to the client contact.

6 Maintenance windows

6.1 Each client has its own windows and blackout dates, held in the schedule. Windows are not shared across clients unless agreed.

8 Reporting and metrics

8.1 One report per client per month: assets in scope, share patched inside the window by class, mean and median days, exceptions with age, and delays awaiting client approval.

8.2 Reports are delivered by [date each month] and kept for [period] after the agreement ends.

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