Enterprise patch management policy

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

2 Roles and responsibilities

2.1 Policy owner ([CISO]): owns this policy and the windows. Approves changes to maintenance plans.

2.2 Patch program lead ([role]): runs the cycle across all groups and reports monthly to the [risk committee].

2.3 Group owners ([role per maintenance group]): own the maintenance plan for their group, approve outage time, and accept test results. Group owners may delegate day-to-day approval in writing to [role]; the delegation names the group, the limits, and an expiry date no later than [12] months.

2.4 Business unit heads: receive the group-level report and own late items in their units.

2.5 Change advisory board ([name]): reviews only changes that fall outside a maintenance plan. Plan-conforming patches are pre-approved.

3 Asset inventory

3.1 The inventory may be held in more than one system. The patch program lead keeps a register that names each source of record, the asset types it covers, and how often it syncs.

3.2 Each asset is assigned to exactly one maintenance group. Assets that cannot meet their group's plan move to a separate group with its own plan; they are not left as exceptions in the group.

3.3 Authenticated scanning or agent reporting is the source for installed software. Unauthenticated scans are used only for discovery.

4 Severity and patch windows

4.1 Group importance is High, Moderate or Low, set by the group owner and confirmed by the policy owner.

4.2 Windows (calendar days from vendor release):

Class	High importance group	Moderate importance group	Low importance group
1. Known exploited, internet-facing	3	3	3
1. Known exploited, other	7	14	14
2. Critical	7	14	14
3. High	14	30	30
4. Medium	60	90	90
5. Low	180	180	180

5 Testing and staging (rings)

5.1 Ring 0: [IT and security staff], first, for [3] working days.

5.2 Ring 1: [volunteer early adopters across business units], for up to [14] days for routine updates.

5.3 Ring 2 and later: remaining assets, in groups of [size].

5.4 Class 1 updates skip Ring 1 and run Ring 0 for no more than [24] hours.

8 Reporting and metrics

8.1 Reports are cut by importance of asset and class of vulnerability, not as one overall percentage. Each cell shows the share patched by deadline, the mean days and the median days.

8.2 The CISO sees all cells; group owners see their group; the board sees the cells for High importance assets and class 1 and 2 vulnerabilities.