FedRAMP patch management policy

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

1 Purpose and scope

1.1 This policy applies to the cloud service offering [name], FedRAMP [Rev5 / 20x] certification class [A / B / C / D], and to all supporting systems in its authorization boundary.

1.2 Legacy authorizations: until [date] the legacy remediation requirements apply to POA&M items; from the mandatory date the Vulnerability Detection and Response (VDR) rules apply.

4 Severity and patch windows

4.1 Timeframes are maximums measured from evaluation of the vulnerability, by the Potential Agency Impact level (N5, N4, N3, N2) and the vulnerability's internet reachability and likelihood of exploitation. They are copied from the FedRAMP rules page dated [read date] into Appendix 1 and re-read at each review.

4.2 Known Exploited Vulnerabilities are remediated by the due date shown for the entry in the CISA catalog, as required by BOD 26-04 or any successor guidance.

4.3 Other vulnerabilities are mitigated or remediated during routine operations as the provider determines necessary, within the company standard of the general policy (class 4: 90 days; class 5: 180 days).

4.4 Where the SHOULD wording of a rule is not followed, the provider records the reason and the alternative (Annex A).

8 Reporting and metrics

8.1 Reports show, for each class and impact level, the vulnerabilities evaluated, the timeframe applicable, the date mitigated or remediated, and any past timeframe.

8.2 Legacy: POA&M items show scheduled completion against 30 days (critical and high), 90 days (moderate), 180 days (low), from discovery.

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