PCI DSS patch management policy

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

1 Purpose and scope

1.1 This policy applies to every system component in the cardholder data environment of [Company name], every system connected to it, and every system that can affect its security. The scope diagram dated [date] is kept by [role].

1.2 Third parties that host or manage in-scope components are named in [register] and are bound by clause 4.

4 Severity and patch windows

4.1 Windows for in-scope components, from vendor release:

Class	Window	Basis
Critical vulnerabilities	14 calendar days (company standard); never more than one month	PCI SSC FAQ 1597: Requirement 6.3.3, one month from release for critical vulnerabilities
Known exploited	3 days internet-facing, otherwise 14 days	Company standard (CISA BOD 26-04 tiers)
High and other	30, 90 and 180 days as in the general policy	Company standard; non-critical windows follow the entity's risk analysis (FAQ 1597)

4.2 Where the QSA or the assessor reads the requirement differently, [role] amends this clause within [10] working days and records the reason.

4.3 In-scope components that cannot meet clause 4.1 are recorded under Annex A with the requirement reference [number from your copy of the standard].

8 Reporting and metrics

8.1 The monthly report adds: in-scope components with a critical vulnerability past 14 days; oldest open critical age; scope changes.

8.2 Evidence of each patch (date installed, component, vulnerability) is kept for [period set by the assessor].