TECHNOLOGY & CONTINUITY

Patching & vulnerability management

Find relevant exposures, prioritise remediation and verify changes against the actual managed inventory.

DOCUMENT	PREPARED	STATUS
MSP-14	1 October 2026	Draft for adoption

Scope & application

Supported applications, operating systems, firmware and managed services in scope. A remediation schedule defines severity criteria, target timeframes and emergency authority.

Who does what

NovaSoft engagement lead

Scopes the work, assigns authorised personnel and maintains implementation and exception records.

Client service and risk owners

Approve access, business decisions, priorities, notices and residual risks; provide accurate scope and timely lifecycle requests.

Users and suppliers

Follow the approved arrangements, report issues and perform responsibilities assigned in the service schedule.

Draft for adoption. Confirm applicable requirements, implementation, owners and approval in the written client service schedule before operational use. Effective date is assigned on adoption.

THE POLICY IN PRACTICE

Control requirements.

01 Identify exposure

Use approved inventory, vendor advisories and scanning methods. Agree scanning boundaries and safe testing; record unauthorised or unreachable systems as coverage gaps.

02 Prioritise with context

Consider active exploitation, internet exposure, business impact and available fixes alongside severity scores. Assign an owner and target action rather than treating every scanner result as equivalent.

03 Set remediation targets

Agree timelines consistent with the required risk and control objective. Where an Essential Eight maturity target is contracted, apply its relevant requirements explicitly; this public policy does not silently set an SLA.

04 Test and deploy

Use staged rollout and a rollback or recovery plan proportionate to the change. Confirm maintenance windows and dependencies, including firmware and application compatibility.

05 Track failed or deferred work

Record the affected system, reason, interim mitigation, owner and review date. Escalate unsupported software or repeated failures for replacement, isolation or another approved treatment.

06 Verify completion

Confirm installation state, service function and whether the exposure remains. Report residual risk and coverage; a queued job or successful download is not evidence that every endpoint is patched.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Review inventory, advisories and approved scan results.

02 Prioritise exposure and agree remediation or mitigation.

03 Apply changes through staged or emergency change control.

04 Verify the result and update outstanding risk records.

Agree with the client

- Scanning and managed-system boundaries
- Risk-based remediation timeframes
- Maintenance and emergency authority
- Deferral and replacement decisions

Evidence to retain

- Advisory/scan and inventory coverage
- Deployment and validation records
- Deferrals, mitigations and exception approvals

Exceptions & review

Record the requirement, reason, affected scope, risk owner, compensating measures and expiry or review date. Seek approval before deviating, or use documented emergency authority and arrange prompt review. Exceptions cannot waive applicable legal duties.

Review trigger: During the agreed remediation cycle and when new high-priority exposure is identified.

Proposed owner: NovaSoft engagement lead with the client service/risk owner. Review at least annually, and earlier when the trigger above applies. Version changes require an approval and client-impact record.

References & related information

ASD/ACSC - Essential Eight maturity model

NovaSoft public policy library and application notes