CYBERSECURITY & ACCESS

Endpoint, mobile & BYOD security

Set a documented baseline for managed devices and make the boundary between business data and personal use understandable.

DOCUMENT	PREPARED	STATUS
MSP-05	1 October 2026	Draft for adoption

Scope & application

Supported desktops, laptops, phones and tablets, including personally owned devices expressly approved for business access. Client scope defines device types and management capabilities.

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 Know the device

Record owner, user, serial or asset identifier, operating system, support status and management state. Quarantine or restrict unknown devices according to the approved access plan.

02 Configure a baseline

Apply agreed screen lock, encryption, supported software, update and protection settings. Record exceptions and test that management does not break essential business functions.

03 Separate administration

Limit local administrator rights and unapproved software installation. Use controlled elevation for a defined task and return the device to its normal access state afterwards.

04 Explain BYOD boundaries

Obtain an approved BYOD arrangement stating collected telemetry, support limits, business-data separation and wipe scope. Personal ownership does not authorise unrestricted inspection or full-device erasure.

05 Respond to loss or compromise

Provide a known reporting route. Verify authority before locking or wiping; consider evidence preservation, business continuity and the agreed personal-data boundaries.

06 Manage retirement

Back up required business material, remove access and securely sanitise storage before disposal or reassignment. Record the method, result and any contractor handling the asset.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Confirm eligibility, ownership and device management authority.

02 Apply and verify the approved security baseline.

03 Monitor agreed management signals and act on reported issues.

04 Reassign, return or retire the device with a recorded outcome.

Agree with the client

- Supported devices and minimum settings
- BYOD collection and wipe consent
- Lost-device actions and contacts
- Device return and disposal arrangements

Evidence to retain

- Device inventory and baseline evidence
- BYOD approvals and exceptions
- Loss, wipe and sanitisation records

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: On enrolment, ownership change, loss or retirement and at agreed baseline reviews.

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

OAIC - Australian Privacy Principles guidelines

NovaSoft public policy library and application notes