CYBERSECURITY & ACCESS

Identity, access & staff lifecycle

Give people the access they need, verify sensitive changes and remove obsolete access across the full account lifecycle.

DOCUMENT	PREPARED	STATUS
MSP-04	1 October 2026	Draft for adoption

Scope & application

Client and provider identities, administrative roles, service accounts, joiners, movers, leavers and emergency access within agreed managed scope.

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 Use verified identities

Maintain named human accounts and a separate register for non-human identities. Verify joiner and access requests with the approved sponsor; never rely only on an unexpected message.

02 Apply least privilege

Grant the minimum role for the approved task. Keep everyday use separate from administration and separate client access from provider business systems. Review standing access and remove unused permissions.

03 Protect authentication

Use MFA where supported, prioritising phishing-resistant methods for privileged and important accounts. Store credentials in an approved vault and never request a password or one-time code through an unsolicited support message.

04 Control non-human access

Give service identities a named owner and defined purpose. Limit secrets, scopes and lifetime; rotate or revoke credentials on compromise or ownership change. Avoid interactive use of unattended service accounts.

05 Complete joiner, mover and leaver changes

Use an authorised start, role-change or end time. Review group memberships and delegated apps; revoke sessions, tokens and access paths. Preserve required business records before deleting an account.

06 Protect emergency access

Define break-glass ownership, secure storage, controlled use and post-use review. Test recovery without weakening normal access controls and record every emergency activation.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Verify the sponsor and the access or lifecycle event.

02 Approve roles, device needs and the required change time.

03 Apply changes and verify sessions, tokens and integrations.

04 Record the result and review remaining permissions.

Agree with the client

- Authorised sponsors and role approvals
- MFA and privileged-access requirements
- Leaver timing and business-record preservation
- Emergency access ownership

Evidence to retain

- Identity and service-account registers
- Approved lifecycle/access requests
- Access-review and emergency-use 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 every lifecycle event, after a suspected compromise and at agreed access 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

ASD/ACSC - Managed service provider guidance

NovaSoft public policy library and application notes