CYBERSECURITY & ACCESS

Network security & remote administration

Keep management paths controlled and separate client networks, administration and guest use according to business need.

DOCUMENT	PREPARED	STATUS
MSP-06	1 October 2026	Draft for adoption

Scope & application

Managed routers, switching, Wi-Fi, firewalls, remote support, VPNs and network administration. Physical works and unmanaged connections require separate scope where applicable.

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 Document the boundary

Maintain an access-controlled network diagram, device ownership, permitted administration paths and external dependencies. Publish only high-level policy; keep addresses and detailed topology private.

02 Separate trust zones

Agree separation for business systems, management, guests and other higher-risk devices. Validate the required traffic paths and avoid extending one client's trust into another environment.

03 Control remote administration

Use approved authenticated access with MFA where supported, restricted source paths and accountable administrator identities. Avoid exposing management interfaces directly to the public internet.

04 Review firewall changes

Record purpose, source, destination, service, approver and expiry for a rule. Validate the required function and remove obsolete or overly broad access through change control.

05 Protect configuration

Limit who can view and edit configuration, back up approved settings and keep supported firmware. Rotate inherited or compromised secrets and validate remote recovery before making disruptive changes.

06 Record support sessions

Establish permission for attended or unattended support. Log the connection and material actions where supported, end temporary access and restrict session recordings according to the data schedule.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Confirm the management scope and required network flows.

02 Approve access paths, segmentation and configuration changes.

03 Test permitted connectivity and blocked administrative exposure.

04 Document changes and retire unnecessary access.

Agree with the client

- Remote and unattended support authority
- Network zones and necessary traffic
- Configuration backup and rollback
- Session records and retention

Evidence to retain

- Private diagram and configuration inventory
- Firewall/remote-access approvals
- Connectivity tests and support-session logs

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: After material network changes, remote-access changes and the agreed configuration review.

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 - Managed service provider guidance

ASD/ACSC - Essential Eight maturity model

NovaSoft public policy library and application notes