TECHNOLOGY & CONTINUITY

Logging, monitoring & operational reporting

Collect useful signals for agreed purposes and connect alerts with a defined owner, response route and information boundary.

DOCUMENT	PREPARED	STATUS
MSP-18	1 October 2026	Draft for adoption

Scope & application

Security and operational telemetry from managed systems, remote tools and automated assistance. The monitoring schedule specifies sources, collection, retention and human response coverage.

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 Define monitoring coverage

List included systems, signals and known blind spots. Distinguish automated collection, AI assistance and staffed review; do not equate a running agent with guaranteed continuous human monitoring.

02 Collect proportionately

Document purpose and permitted telemetry. Avoid capturing passwords or unnecessary content; establish client authority and appropriate user notice for device, session or activity monitoring.

03 Protect the records

Restrict access, preserve useful timestamps and secure transfers and storage. Define retention, deletion and incident preservation; log copies may themselves contain confidential or personal information.

04 Give alerts a route

Agree thresholds, severity, contacts, response hours and authority. Test delivery and escalation. Record suppressions or tuning so important signals are not silently lost.

05 Check the collection itself

Identify stalled agents, source gaps, failed forwarding and expired integration credentials. Record the effect on coverage and remediate or notify the client through the agreed process.

06 Report with context

Explain findings, noise, unresolved gaps and actions in service reporting. Use aggregated or de-identified material publicly; keep raw logs, client architecture and incident details in approved private channels.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Agree purposes, sources, retention and response arrangements.

02 Enable the approved collection and test alert delivery.

03 Review signals and act within the agreed authority and coverage.

04 Report outcomes, gaps and required tuning or changes.

Agree with the client

- Permitted telemetry and user notices
- Human coverage and automated functions
- Retention, access and preservation
- Alert thresholds and escalation authority

Evidence to retain

- Monitoring and log-source schedule
- Collection, alert and response records
- Coverage gaps and reporting actions

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: At service reviews and after source, tooling, contact, retention or response-coverage changes.

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

OAIC - Australian Privacy Principles guidelines

NovaSoft public policy library and application notes