TECHNOLOGY & CONTINUITY

Backup, recovery & business continuity

Agree what must be recoverable, protect backup access and test a practical route back to business operation.

DOCUMENT	PREPARED	STATUS
MSP-16	1 October 2026	Draft for adoption

Scope & application

Managed backup jobs, restoration and technology recovery. Client business continuity arrangements also cover people, premises, suppliers and manual processes beyond technical recovery.

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 recovery needs

Identify important systems, data and dependencies. Agree recovery point and recovery time objectives for each service, included backup coverage and responsibilities for gaps.

02 Protect backup access

Restrict administration and separate credentials from routine user access. Use protected, isolated or immutable copies where suitable and agreed; document retention, encryption and key-recovery arrangements.

03 Monitor the jobs in scope

Define checks, alert routing and response coverage. Record failed or incomplete jobs and capacity issues. A successful job alone does not establish that the required service can be restored.

04 Test restoration

Agree representative restoration tests, acceptance criteria and frequency. Check data usability and dependencies in an appropriate isolated environment; document achieved results and limitations.

05 Plan recovery order

Record required identities, infrastructure, applications and external services. Define the authority to restore, rollback points and the business owner who accepts resumed operation.

06 Maintain continuity

Discuss communication, alternate workflows and supplier dependencies with the client. Update the plan after material changes; confirm backup ownership and remaining copies during service exit.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Agree recovery objectives, coverage and key dependencies.

02 Configure and verify the approved backup plan.

03 Monitor agreed signals and test representative restoration.

04 Record achieved recovery, gaps and continuity improvements.

Agree with the client

- RPO/RTO objectives and backup coverage
- Retention, keys and protected copies
- Test frequency and acceptance criteria
- Recovery authority and business fallback

Evidence to retain

- Backup and dependency schedule
- Job/alert and restore-test records
- Recovery playbook and accepted gaps

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 the agreed restoration exercise and after major changes, incidents or backup ownership transfers.

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