CYBERSECURITY & ACCESS

Cyber incident & data breach response

Coordinate containment, evidence, recovery and communication when an incident may affect client systems or information.

DOCUMENT	PREPARED	STATUS
MSP-08	1 October 2026	Draft for adoption

Scope & application

Suspected compromise, ransomware, unauthorised access, accidental disclosure and service-impacting security incidents. The response schedule defines contacts, authority and specialist support.

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 Report and triage

Use the contracted support or incident route. Record time, observed symptoms, affected systems and business impact. The public contact address is not a guaranteed continuously monitored emergency channel.

02 Assign incident roles

Identify the client incident lead, technical responder and privacy/legal decision-maker. Define authority for isolation, account suspension, external assistance and recovery before an emergency.

03 Contain with evidence in mind

Limit further harm using authorised actions while preserving useful logs and affected material. Avoid unnecessary deletion, reinstallation or destructive testing before evidence needs are considered.

04 Assess notification obligations

Determine the affected information, people, jurisdictions and likely harm with appropriate advice. Where applicable, follow the NDB scheme and other required deadlines; allocate who will notify authorities and individuals.

05 Recover deliberately

Remove or contain the cause, validate clean recovery, rotate affected secrets and check persistence. Confirm system ownership and business acceptance before returning services to normal.

06 Communicate and learn

Provide agreed updates using verified facts and clearly identified unknowns. Restrict incident detail to authorised recipients, preserve required records and convert lessons into owned actions.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Receive the report, triage and activate the incident contacts.

02 Contain exposure and preserve relevant evidence.

03 Assess impact, required notices and recovery options.

04 Restore, verify and complete a documented post-incident review.

Agree with the client

- Emergency contacts and containment authority
- Specialist, insurer and legal coordination
- Notification decision-maker and duties
- Recovery acceptance and update frequency

Evidence to retain

- Incident timeline and decision log
- Evidence inventory and notification assessment
- Recovery checks and lessons/action register

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: Exercise the plan at an agreed interval and review after every material incident or contact change.

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

OAIC - Data breach preparation and response

OAIC - About the Notifiable Data Breaches scheme

NovaSoft public policy library and application notes