AI, PRIVACY & DATA

Records retention & secure disposal

Keep information for a documented reason and make deletion, legal holds and residual copies traceable.

DOCUMENT	PREPARED	STATUS
MSP-11	1 October 2026	Draft for adoption

Scope & application

Support records, client documentation, logs, exports, device storage and backup copies held within the engagement. Requirements vary by record type, legal obligation and supplier capability.

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 Agree a retention schedule

Set a period or trigger for each record class, its owner, storage location and disposal method. Avoid a blanket promise to keep everything indefinitely or delete all material immediately.

02 Apply legal holds

Suspend ordinary disposal for records subject to a valid preservation instruction or applicable obligation. Record who authorised the hold, its scope and when release may be approved.

03 Control copies and exports

Limit duplicate working copies and temporary exports. Record sensitive exports, their purpose and recipient; remove temporary material after the authorised task and required retention are complete.

04 Address backups honestly

Document backup expiry, immutable periods and supplier deletion constraints. Where selective removal is impractical, restrict the retained copy and apply the approved expiry; do not claim immediate deletion from every backup.

05 Sanitise media

Choose an appropriate sanitisation or destruction method for storage type and sensitivity. Verify completion where possible and record failed media, destruction certificates or third-party processing.

06 Keep a disposal record

Record what was removed, the authority, method and date, with any retained exceptions. Remove access and credentials as a separate step; deleting an account does not necessarily delete its data.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Classify the records and approve retention/hold requirements.

02 Identify active, temporary, backup and supplier-held copies.

03 Execute approved deletion or sanitisation after checking holds.

04 Verify outcomes and document remaining copies and expiry dates.

Agree with the client

- Retention periods and record owners
- Preservation and legal-hold authority
- Backup expiry and supplier constraints
- Approved disposal and verification methods

Evidence to retain

- Retention schedule and hold register
- Export/copy and sanitisation records
- Deletion outcomes and residual-copy 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: At schedule review, service exit and after changes to legal obligations or storage arrangements.

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 - Australian Privacy Principles guidelines

NovaSoft public policy library and application notes