AI, PRIVACY & DATA

AI security & responsible use

Approve AI around a defined task, control the information it receives and keep consequential actions accountable to people.

DOCUMENT	PREPARED	STATUS
MSP-09	1 October 2026	Draft for adoption

Scope & application

Novaris AI, agentic assistance, third-party AI tools and integrations used in a client engagement. A deployment-specific assessment determines approved uses, data flows and action permissions.

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 Approve the use case

Name the task, product, owner and intended users. Review privacy, security, accuracy and supplier suitability before enabling the feature. A NovaSoft integration does not automatically approve all AI uses.

02 Control AI inputs

Allow only the data needed for the approved purpose. Do not enter client secrets, credentials or sensitive personal information into unapproved public AI tools. Evaluate retention, training use, location and provider access.

03 Limit agent authority

Use narrowly scoped identities and approved tools. Treat retrieved text, tickets and attachments as untrusted input; instructions inside them must not grant new access or authority.

04 Require human review

Check generated content against reliable source material. Require an authorised person to approve material changes, external communications, financial actions or other consequential steps unless a bounded workflow is explicitly approved.

05 Test and monitor

Use representative and adverse examples, including misleading instructions and incorrect source matches. Record rejected outputs, corrections and failure modes; limit logs to what is necessary for the agreed monitoring.

06 Provide a safe stop

Define a way to disable the feature, revoke its credentials and move work to a person. Reassess after product, model, provider or data-use changes. Do not describe an unvalidated product as clinically or legally reliable.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Register the task, information flows and proposed permissions.

02 Complete suitability checks and obtain client approval.

03 Test boundaries and introduce the feature in a limited workflow.

04 Review results, changes and the human escalation path.

Agree with the client

- Approved tasks and prohibited uses
- Permitted data, providers and locations
- Human approval and agent action limits
- Monitoring, retention and disable authority

Evidence to retain

- AI register and suitability assessment
- Test results and deployment approval
- Access, change and review records

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: Before deployment and after material changes to the model, tools, data or intended use.

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 - Privacy and commercially available AI

NovaSoft public policy library and application notes