TRANSPARENCY / MANAGED IT

A clearer standard. For managed IT.

18 policies. Defined responsibilities. Evidence people can inspect.

NovaSoft publishes this framework so prospective and current clients can inspect the expectations, responsibilities and evidence behind an MSP engagement. Public documents describe the approach; client-specific configuration, credentials, findings and records remain in authorised private channels.

PUBLIC FRAMEWORK - DRAFT FOR ADOPTION

Prepared for review on 1 October 2026. Version 1.0 is a draft for adoption. Publication does not confirm that every described control is implemented or independently assessed. The authorised NovaSoft and client owners must approve applicable requirements and record service-specific arrangements before operational use.

Apply this framework to the systems and activities included in the written engagement. Record applicable laws, required controls, owners, timeframes and approved exceptions in the client service schedule. A public document does not change a signed agreement or any right or obligation imposed by law.

Questions and proposed changes: contact@novasofttechnologies.com. Use the agreed client channel for service requests or incident reporting. This public enquiry address does not define response coverage.

THE COMPLETE COLLECTION

Find the right policy.

Client service & transitions

MSP-01 Service governance & shared responsibility 3
MSP-02 Client onboarding & service transition 6
MSP-03 Client offboarding & secure handover 9

Cybersecurity & access

MSP-04 Identity, access & staff lifecycle 12
MSP-05 Endpoint, mobile & BYOD security 15
MSP-06 Network security & remote administration 18
MSP-07 Cybersecurity risk & control management 21
MSP-08 Cyber incident & data breach response 24

AI, privacy & data

MSP-09 AI security & responsible use 27
MSP-10 Privacy, confidentiality & data handling 30
MSP-11 Records retention & secure disposal 33
MSP-12 Acceptable use & security awareness 36

Technology & continuity

MSP-13 Technology assets & software lifecycle 39
MSP-14 Patching & vulnerability management 42
MSP-15 Change, release & configuration management 45
MSP-16 Backup, recovery & business continuity 48
MSP-17 Cloud, email & supplier security 51
MSP-18 Logging, monitoring & operational reporting 54

CLIENT SERVICE & TRANSITIONS

Service governance & shared responsibility

Establish who can request work, approve decisions and own the systems covered by a managed IT engagement.

DOCUMENT	PREPARED	STATUS
MSP-01	1 October 2026	Draft for adoption

Scope & application

Managed services, support requests, service reviews and co-managed arrangements. A signed service schedule identifies included systems, responsibilities, coverage and commercial terms.

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 the service boundary

Record managed assets, supported services, exclusions, dependencies and the division of work between NovaSoft, client personnel and vendors. Discovery does not automatically bring an asset into managed scope.

02 Approve work through named contacts

Keep an authorised-contact register. Verify unusual or sensitive requests through a known channel before changing access, payment-related settings or business-critical services.

03 Record service expectations

Agree support hours, time zones, request channels, severity definitions, response targets and escalation. Distinguish initial response from resolution and human coverage from automated assistance.

04 Keep requests traceable

Assign a reference, impact, owner and next action to work. Record approval, material changes, communications and completion. Use a secure transfer method for confidential attachments.

05 Review performance and risk

Discuss open work, recurring faults, capacity, lifecycle issues and accepted risks at the agreed service review. Explain dependencies and delays rather than promising outcomes outside the scope.

06 Handle concerns consistently

Document a service concern, confirm the requested outcome and route it to the engagement lead. Escalate unresolved matters through the agreed complaints process and preserve applicable consumer rights.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Confirm the service schedule and authorised contacts.

02 Agree ticket intake, severity and escalation arrangements.

03 Record work and provide status through the agreed channel.

04 Review results, unresolved risks and proposed improvements.

Agree with the client

- Systems and services included
- Human support hours and targets
- Approval limits and contact changes
- Review and complaint escalation route

Evidence to retain

- Service schedule and responsibility matrix
- Request records and approval history
- Service-review actions and risk 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 each agreed service review and after a material scope or ownership 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

ASD/ACSC - Managed service provider guidance

NovaSoft public policy library and application notes

CLIENT SERVICE & TRANSITIONS

Client onboarding & service transition

Move into managed support with verified ownership, a documented baseline and explicit acceptance of the starting environment.

DOCUMENT	PREPARED	STATUS
MSP-02	1 October 2026	Draft for adoption

Scope & application

New MSP clients, incoming-provider transitions and additions to an existing managed environment. Access and tooling require client authority before installation or connection.

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 Authorise the transition

Identify the client decision-maker, outgoing provider, business owners and transition contacts. Record permission to discover systems and the date responsibility for each service changes.

02 Discover without disrupting

Inventory accounts, devices, networks, applications, licences, backups and dependencies. Use read-only discovery first where practical. Record unknown ownership and unsupported assets for resolution.

03 Exchange access securely

Use an approved vault or secure handover channel. Verify ownership before granting delegated administration. Separate client environments and avoid copying another client's permissions or credentials.

04 Check the baseline

Review access, MFA, endpoint protection, updates and recovery arrangements. Record observed evidence and gaps; a checklist alone does not establish that a control is operating effectively.

05 Introduce management tooling

Agree agent installation, permissions, telemetry, remote access, support notices and removal arrangements. Test a limited deployment before expanding to the agreed inventory.

06 Accept the service start

Agree outstanding remediation, accepted risks, included assets and escalation details. Confirm backup and restoration responsibilities before removing existing protection or ending an outgoing service.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Approve discovery and obtain the existing documentation.

02 Validate inventory, ownership, access and recovery dependencies.

03 Deploy agreed tooling in stages and test essential functions.

04 Sign off the baseline, outstanding actions and service start.

Agree with the client

- Transition dates and outgoing-provider coordination
- Tool permissions and data collection
- Remediation priorities and funding
- Acceptance of unresolved risks

Evidence to retain

- Discovery inventory and handover receipt
- Baseline findings with evidence
- Tool deployment and service acceptance record

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 onboarding, when adding a major service, and at the first scheduled service review.

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

ASD/ACSC - Essential Eight maturity model

NovaSoft public policy library and application notes

CLIENT SERVICE & TRANSITIONS

Client offboarding & secure handover

Provide a controlled exit that transfers authorised material, removes provider access and preserves continuity responsibilities.

DOCUMENT	PREPARED	STATUS
MSP-03	1 October 2026	Draft for adoption

Scope & application

Termination, partial service transfer and transition to another provider. Contract terms determine notice, deliverables, fees and retention; this framework adds no new termination charge.

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 the exit plan

Verify the client owner and receiving party. Identify service end dates, transfer milestones, continuing support and records the client is entitled to receive under the agreement.

02 Prepare a useful handover

Provide agreed inventories, configuration documentation, client-owned exports, licence information and open issues. Separate reusable provider tools, third-party rights and restricted material from client deliverables.

03 Confirm recovery ownership

Record who will manage backups, restore keys and recovery procedures after handover. Confirm export compatibility, completion and any agreed restoration checks before retiring existing jobs.

04 Remove all access paths

Revoke delegated roles, remote agents, VPN access, service accounts, OAuth grants, API keys and integrations as applicable. Coordinate credential rotation and test removal without disabling client-owned identities.

05 Transfer through approved channels

Encrypt or otherwise protect sensitive handover material. Verify the recipient and record receipt. Keep secrets out of ordinary tickets, public links and unverified email attachments.

06 Close retention and responsibility

Apply the agreed retention schedule, legal holds and deletion process to remaining copies. Record inaccessible or supplier-held data and residual expiry dates. Confirm when NovaSoft's operational responsibility ends.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Confirm the authorised exit request and transition scope.

02 Prepare and verify the handover package and recovery arrangements.

03 Obtain receipt, transfer ownership and revoke provider access.

04 Record retained material, deletion actions and final closure.

Agree with the client

- Receiving contacts and permitted deliverables
- Continuing service and cutover dates
- Credential and integration changes
- Retention, legal holds and deletion scope

Evidence to retain

- Exit plan and handover manifest
- Access revocation and recipient receipt
- Retention/deletion record and closure confirmation

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: For every exit or partial transfer; revisit if cutover dates or recipients 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

ASD/ACSC - Managed service provider guidance

OAIC - Australian Privacy Principles guidelines

NovaSoft public policy library and application notes

CYBERSECURITY & ACCESS

Identity, access & staff lifecycle

Give people the access they need, verify sensitive changes and remove obsolete access across the full account lifecycle.

DOCUMENT	PREPARED	STATUS
MSP-04	1 October 2026	Draft for adoption

Scope & application

Client and provider identities, administrative roles, service accounts, joiners, movers, leavers and emergency access within agreed managed scope.

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 Use verified identities

Maintain named human accounts and a separate register for non-human identities. Verify joiner and access requests with the approved sponsor; never rely only on an unexpected message.

02 Apply least privilege

Grant the minimum role for the approved task. Keep everyday use separate from administration and separate client access from provider business systems. Review standing access and remove unused permissions.

03 Protect authentication

Use MFA where supported, prioritising phishing-resistant methods for privileged and important accounts. Store credentials in an approved vault and never request a password or one-time code through an unsolicited support message.

04 Control non-human access

Give service identities a named owner and defined purpose. Limit secrets, scopes and lifetime; rotate or revoke credentials on compromise or ownership change. Avoid interactive use of unattended service accounts.

05 Complete joiner, mover and leaver changes

Use an authorised start, role-change or end time. Review group memberships and delegated apps; revoke sessions, tokens and access paths. Preserve required business records before deleting an account.

06 Protect emergency access

Define break-glass ownership, secure storage, controlled use and post-use review. Test recovery without weakening normal access controls and record every emergency activation.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Verify the sponsor and the access or lifecycle event.

02 Approve roles, device needs and the required change time.

03 Apply changes and verify sessions, tokens and integrations.

04 Record the result and review remaining permissions.

Agree with the client

- Authorised sponsors and role approvals
- MFA and privileged-access requirements
- Leaver timing and business-record preservation
- Emergency access ownership

Evidence to retain

- Identity and service-account registers
- Approved lifecycle/access requests
- Access-review and emergency-use 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: On every lifecycle event, after a suspected compromise and at agreed access reviews.

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

CYBERSECURITY & ACCESS

Endpoint, mobile & BYOD security

Set a documented baseline for managed devices and make the boundary between business data and personal use understandable.

DOCUMENT	PREPARED	STATUS
MSP-05	1 October 2026	Draft for adoption

Scope & application

Supported desktops, laptops, phones and tablets, including personally owned devices expressly approved for business access. Client scope defines device types and management capabilities.

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 Know the device

Record owner, user, serial or asset identifier, operating system, support status and management state. Quarantine or restrict unknown devices according to the approved access plan.

02 Configure a baseline

Apply agreed screen lock, encryption, supported software, update and protection settings. Record exceptions and test that management does not break essential business functions.

03 Separate administration

Limit local administrator rights and unapproved software installation. Use controlled elevation for a defined task and return the device to its normal access state afterwards.

04 Explain BYOD boundaries

Obtain an approved BYOD arrangement stating collected telemetry, support limits, business-data separation and wipe scope. Personal ownership does not authorise unrestricted inspection or full-device erasure.

05 Respond to loss or compromise

Provide a known reporting route. Verify authority before locking or wiping; consider evidence preservation, business continuity and the agreed personal-data boundaries.

06 Manage retirement

Back up required business material, remove access and securely sanitise storage before disposal or reassignment. Record the method, result and any contractor handling the asset.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Confirm eligibility, ownership and device management authority.

02 Apply and verify the approved security baseline.

03 Monitor agreed management signals and act on reported issues.

04 Reassign, return or retire the device with a recorded outcome.

Agree with the client

- Supported devices and minimum settings
- BYOD collection and wipe consent
- Lost-device actions and contacts
- Device return and disposal arrangements

Evidence to retain

- Device inventory and baseline evidence
- BYOD approvals and exceptions
- Loss, wipe and sanitisation 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: On enrolment, ownership change, loss or retirement and at agreed baseline reviews.

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

OAIC - Australian Privacy Principles guidelines

NovaSoft public policy library and application notes

CYBERSECURITY & ACCESS

Network security & remote administration

Keep management paths controlled and separate client networks, administration and guest use according to business need.

DOCUMENT	PREPARED	STATUS
MSP-06	1 October 2026	Draft for adoption

Scope & application

Managed routers, switching, Wi-Fi, firewalls, remote support, VPNs and network administration. Physical works and unmanaged connections require separate scope where applicable.

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 Document the boundary

Maintain an access-controlled network diagram, device ownership, permitted administration paths and external dependencies. Publish only high-level policy; keep addresses and detailed topology private.

02 Separate trust zones

Agree separation for business systems, management, guests and other higher-risk devices. Validate the required traffic paths and avoid extending one client's trust into another environment.

03 Control remote administration

Use approved authenticated access with MFA where supported, restricted source paths and accountable administrator identities. Avoid exposing management interfaces directly to the public internet.

04 Review firewall changes

Record purpose, source, destination, service, approver and expiry for a rule. Validate the required function and remove obsolete or overly broad access through change control.

05 Protect configuration

Limit who can view and edit configuration, back up approved settings and keep supported firmware. Rotate inherited or compromised secrets and validate remote recovery before making disruptive changes.

06 Record support sessions

Establish permission for attended or unattended support. Log the connection and material actions where supported, end temporary access and restrict session recordings according to the data schedule.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Confirm the management scope and required network flows.

02 Approve access paths, segmentation and configuration changes.

03 Test permitted connectivity and blocked administrative exposure.

04 Document changes and retire unnecessary access.

Agree with the client

- Remote and unattended support authority
- Network zones and necessary traffic
- Configuration backup and rollback
- Session records and retention

Evidence to retain

- Private diagram and configuration inventory
- Firewall/remote-access approvals
- Connectivity tests and support-session logs

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: After material network changes, remote-access changes and the agreed configuration review.

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

ASD/ACSC - Essential Eight maturity model

NovaSoft public policy library and application notes

CYBERSECURITY & ACCESS

Cybersecurity risk & control management

Turn identified exposure into prioritised work, documented ownership and reviewable control decisions.

DOCUMENT	PREPARED	STATUS
MSP-07	1 October 2026	Draft for adoption

Scope & application

Risk assessments and security improvement plans for managed client environments. Regulatory requirements, threat context and any desired maturity target are established for the engagement.

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 the assessment

Identify important services, information, users and business consequences. Agree the assessment boundary and evidence required, including systems NovaSoft cannot inspect or change.

02 Maintain a risk register

Record each finding, affected asset, consequence, likelihood rationale, owner and next action. Distinguish observed facts from assumptions and prioritise according to the client's operation.

03 Plan a security baseline

Use the Essential Eight as one reference where suitable, alongside additional controls required by the environment. Agree a target and implementation plan; do not infer a maturity level from this document.

04 Validate controls

Inspect configuration and perform authorised tests proportionate to the risk. Record coverage, evidence date and limitations. A purchased tool or enabled feature is not sufficient proof of effectiveness.

05 Manage exceptions

Require a named client risk owner, rationale, compensating measures and a review or expiry date. Escalate unacceptable exposure through the engagement and agree a safe path for affected services.

06 Report proportionately

Provide an understandable improvement plan and progress record. Keep detailed weaknesses and exploit information restricted; public policy publication is not a security certification or an assurance report.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Agree important assets, risk criteria and assessment scope.

02 Gather evidence and prioritise the findings.

03 Approve treatment, owners, funding and exceptions.

04 Validate changes and reassess residual exposure.

Agree with the client

- Risk owner and business priorities
- Assessment scope and maturity objective
- Treatment budgets and decision dates
- Accepted exceptions and review dates

Evidence to retain

- Risk register and assessment boundary
- Control evidence and remediation plan
- Risk decisions and review outcomes

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 risk review, after significant incidents and after material environment 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 - Essential Eight maturity model

ASD/ACSC - Managed service provider guidance

NovaSoft public policy library and application notes

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

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

AI, PRIVACY & DATA

Privacy, confidentiality & data handling

Handle client information for an agreed purpose, limit access and make relevant collection and sharing understandable.

DOCUMENT	PREPARED	STATUS
MSP-10	1 October 2026	Draft for adoption

Scope & application

Personal information and confidential business data in support, administration and managed services. Client notices and applicable jurisdictional requirements must be identified for the engagement.

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 Identify the information

Record categories, business purpose, sensitivity, locations and authorised users. Reduce information collected in tickets and diagnostics to what is required to investigate or deliver the task.

02 Confirm authority and notice

Check the client's authority to provide material and the required collection or use notices. Refer sensitive-data transfers to an approved secure channel rather than asking for them in a public form.

03 Restrict use and disclosure

Use client information only for the authorised work or a lawful requirement. Share with personnel and suppliers who need it under appropriate obligations; do not publish names, screenshots or results without permission.

04 Protect transfers and storage

Select appropriate access controls, encryption and secure transfer methods for the data and service. Verify recipients and document material data flows, including international processing and vendor access.

05 Support privacy requests

Verify the requester, record the request and route it to the organisation responsible for the information. Preserve relevant records and respond according to applicable duties and the agreed processing role.

06 Handle a suspected exposure

Escalate unexpected access, misdelivery or loss through the incident process. Preserve evidence and coordinate the assessment; publication of this framework does not establish every client's legal compliance.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Identify the data, purpose and client instructions.

02 Confirm approved recipients, locations and safeguards.

03 Handle the material with minimum necessary access.

04 Record requests, disclosures and changes to data handling.

Agree with the client

- Data categories and authorised purposes
- Hosting, processing and transfer locations
- Supplier roles and privacy notices
- Requests, retention and incident contacts

Evidence to retain

- Data-flow and access records
- Authorised disclosure and transfer history
- Privacy-request and incident 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: When a new data flow, supplier, location or purpose is introduced and at agreed privacy reviews.

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

OAIC - Privacy and commercially available AI

NovaSoft public policy library and application notes

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

AI, PRIVACY & DATA

Acceptable use & security awareness

Give users practical expectations for business technology, safe reporting and approved use of software and information.

DOCUMENT	PREPARED	STATUS
MSP-12	1 October 2026	Draft for adoption

Scope & application

Client users of managed devices, accounts, cloud services and approved AI tools. The client employer adopts workplace rules and gives appropriate notices about any monitoring.

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 Use authorised services

Use approved accounts, applications and licences for business activity. Do not bypass protective settings or connect unapproved tools to client data; request an assessment when a new tool is needed.

02 Protect account access

Keep credentials and recovery methods private. Use the approved password manager and MFA process; report unexpected prompts or suspected sharing through a known support route.

03 Handle messages carefully

Verify unusual requests, attachment sources and changes to payment or access details. Report suspicious activity without forwarding sensitive content widely or continuing to interact with a suspect link.

04 Respect information boundaries

Share business information only with authorised recipients and systems. Avoid personal storage, unapproved public AI and unverified transfer links for confidential material.

05 Report without delay

Provide a clear reporting route for lost devices, misdirected data and mistakes. Preserve useful context and let the response team coordinate containment rather than asking users to investigate or conceal a problem.

06 Make training practical

Include relevant guidance at induction and agreed refreshers. Adapt training for roles and accessibility needs. Simulation activity, monitoring and employment consequences require client approval and appropriate notice.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Client approves the acceptable-use rules and user notices.

02 Explain relevant practices at induction and role changes.

03 Provide accessible reporting and support instructions.

04 Review recurring questions and update practical guidance.

Agree with the client

- Permitted services and personal use
- User notices and training arrangements
- Simulation and monitoring authority
- Employer ownership of workplace decisions

Evidence to retain

- Adopted rules and notice records
- Training attendance and materials
- Reported issues and improvement 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 agreed awareness refreshers, role changes and after relevant incidents or recurring errors.

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 - Privacy and commercially available AI

NovaSoft public policy library and application notes

TECHNOLOGY & CONTINUITY

Technology assets & software lifecycle

Maintain a useful inventory and plan licences, support status and replacement before they become operational surprises.

DOCUMENT	PREPARED	STATUS
MSP-13	1 October 2026	Draft for adoption

Scope & application

Managed hardware, applications, subscriptions, certificates, domains and technology dependencies. Procurement and renewal authority are specified in the engagement.

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 Maintain the inventory

Record owner, purpose, location, support status and important dependencies. Distinguish managed assets from discovered but out-of-scope systems and record uncertainty for resolution.

02 Track licence rights

Keep entitlement, subscription owner, renewal date and permitted use. Verify licence conditions before deployment, redistribution or transfer; an inventory entry is not proof of entitlement.

03 Plan support expiry

Review vendor support dates and critical renewals for operating systems, equipment, certificates and domains. Agree replacement or migration plans and record accepted exceptions for unsupported technology.

04 Approve procurement

Use the client's purchasing authority and documented requirements. Confirm compatibility, data handling, recurring costs and support implications before introducing a new dependency.

05 Reconcile changes

Update records after onboarding, purchase, reassignment and disposal. Investigate unrecognised assets or software through an authorised process rather than automatically removing production dependencies.

06 Retire safely

Plan replacement, record transfer, remove access and sanitise storage using the disposal policy. Confirm licence and domain ownership handover where a provider relationship changes.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Discover and verify asset ownership and scope.

02 Record lifecycle, support and licence information.

03 Agree renewals, replacement and exception decisions.

04 Update the inventory after each material change.

Agree with the client

- Managed inventory and discovery authority
- Procurement and renewal approvals
- Supported technology and replacement budget
- Ownership and licence transfer requirements

Evidence to retain

- Asset, licence and dependency registers
- Renewal/replacement decisions
- Reconciliation and retirement 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: At agreed inventory reviews and before major renewals, onboarding or retirement.

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

NovaSoft public policy library and application notes

TECHNOLOGY & CONTINUITY

Patching & vulnerability management

Find relevant exposures, prioritise remediation and verify changes against the actual managed inventory.

DOCUMENT	PREPARED	STATUS
MSP-14	1 October 2026	Draft for adoption

Scope & application

Supported applications, operating systems, firmware and managed services in scope. A remediation schedule defines severity criteria, target timeframes and emergency authority.

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 Identify exposure

Use approved inventory, vendor advisories and scanning methods. Agree scanning boundaries and safe testing; record unauthorised or unreachable systems as coverage gaps.

02 Prioritise with context

Consider active exploitation, internet exposure, business impact and available fixes alongside severity scores. Assign an owner and target action rather than treating every scanner result as equivalent.

03 Set remediation targets

Agree timelines consistent with the required risk and control objective. Where an Essential Eight maturity target is contracted, apply its relevant requirements explicitly; this public policy does not silently set an SLA.

04 Test and deploy

Use staged rollout and a rollback or recovery plan proportionate to the change. Confirm maintenance windows and dependencies, including firmware and application compatibility.

05 Track failed or deferred work

Record the affected system, reason, interim mitigation, owner and review date. Escalate unsupported software or repeated failures for replacement, isolation or another approved treatment.

06 Verify completion

Confirm installation state, service function and whether the exposure remains. Report residual risk and coverage; a queued job or successful download is not evidence that every endpoint is patched.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Review inventory, advisories and approved scan results.

02 Prioritise exposure and agree remediation or mitigation.

03 Apply changes through staged or emergency change control.

04 Verify the result and update outstanding risk records.

Agree with the client

- Scanning and managed-system boundaries
- Risk-based remediation timeframes
- Maintenance and emergency authority
- Deferral and replacement decisions

Evidence to retain

- Advisory/scan and inventory coverage
- Deployment and validation records
- Deferrals, mitigations and exception approvals

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: During the agreed remediation cycle and when new high-priority exposure is identified.

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

NovaSoft public policy library and application notes

TECHNOLOGY & CONTINUITY

Change, release & configuration management

Make technology changes deliberate, traceable and recoverable, with authority proportional to their impact.

DOCUMENT	PREPARED	STATUS
MSP-15	1 October 2026	Draft for adoption

Scope & application

Configuration, software releases, infrastructure modifications and emergency changes to managed systems. Standard change categories and approvers are recorded for each engagement.

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 Describe the proposed change

Record purpose, affected systems, dependencies, risk, expected outage and business owner. Check data-handling and access implications before implementation.

02 Assign an approval route

Define pre-approved standard changes, ordinary approvals and emergency authority. A request to investigate a fault does not automatically authorise a material service or permission change.

03 Prepare validation and rollback

Identify expected results, test steps, recovery prerequisites and who can stop the change. Confirm a suitable backup or other recovery option when the work may affect data or availability.

04 Communicate the window

Notify affected contacts through the agreed channel. Include expected impact, timing and support arrangements; coordinate with external suppliers where their systems are involved.

05 Implement and record

Use controlled access and retain relevant commands, configuration differences or deployment records without exposing secrets. Pause or roll back when the agreed stop criteria are met.

06 Close with evidence

Validate the result with the responsible owner, update documentation and monitor agreed follow-up signals. Review emergency changes retrospectively and record any unresolved impact.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Record the scope, risk and approval path.

02 Prepare testing, communications and recovery.

03 Execute the approved change and capture the outcome.

04 Validate, document and close or assign follow-up work.

Agree with the client

- Change categories and approval authority
- Maintenance windows and notices
- Testing, rollback and acceptance criteria
- Emergency and retrospective review process

Evidence to retain

- Change request and approval
- Implementation and validation evidence
- Updated configuration and review 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: For each material change, after failed changes and at agreed process reviews.

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

NovaSoft public policy library and application notes

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

TECHNOLOGY & CONTINUITY

Cloud, email & supplier security

Assess third-party services and configure cloud collaboration around clear ownership, access and information flows.

DOCUMENT	PREPARED	STATUS
MSP-17	1 October 2026	Draft for adoption

Scope & application

Managed cloud tenants, business email, SaaS, hosting and suppliers with client data or administrative access. Supplier selection and commercial commitments require client authority.

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 Assess before connection

Record the business purpose, information processed, hosting locations, access rights, incident support, export options and relevant contract terms. Review material subcontracting and integration dependencies.

02 Keep ownership clear

Identify the client tenant owner, domain owner and delegated provider roles. Use accountable administration and separate client environments; avoid creating ownership that prevents an authorised exit.

03 Configure collaboration

Agree external sharing, guest access, forwarding, consent to connected apps and privileged roles. Review risky mailbox or application changes and revoke obsolete integrations.

04 Protect business email

Configure agreed sender-domain authentication, account protection and mail-flow safeguards. Verify payment-detail changes through a known channel; authentication does not make every message trustworthy.

05 Understand availability and retention

Record supplier support, storage/retention settings and restoration capabilities. Do not assume a cloud subscription includes the backup coverage or recovery objectives the client requires.

06 Review and exit

Reassess material provider or data-use changes. Maintain a record of active suppliers and approved access; test export and revocation arrangements during a planned transition.

FROM POLICY TO DELIVERY

Operate. Record. Review.

01 Assess the supplier and obtain purchasing/access approval.

02 Document ownership, configuration and data flows.

03 Introduce the service and verify agreed protection settings.

04 Review changes, renewals and a workable exit path.

Agree with the client

- Approved providers and processing locations
- Tenant, domain and integration ownership
- Sharing, email and retention settings
- Supplier changes and exit requirements

Evidence to retain

- Supplier assessment and service register
- Tenant/access and configuration records
- Renewal, export and revocation 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 a new supplier or integration, at renewal and after material provider or data-flow 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

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