



HL-DAT-170
28 AUGUST 2026

DATA HANDLING SECURITY AND SYSTEM OWNERSHIP

CONTRACTUAL POLICY FOR CLIENT DATA SYSTEMS AND ACCESS

VERSION 1.7

EFFECTIVE 28 AUGUST 2026

IMAGINE | BUILD | INSPIRE

DOCUMENT OVERVIEW

Version	1.7
Effective date	28 August 2026

Policy owner: Hamilton Lockhart Approved by: Joshua Ernest Hamilton

1. Purpose and application

This policy explains how Hamilton Lockhart handles Client information, systems, credentials and technology environments while delivering consulting, design, development, integration, automation, AI-agent, monitoring, maintenance and support services. It establishes the information Hamilton Lockhart may handle, the purposes for which that information may be used, data-handling and security requirements, responsibilities for Client-controlled and Hamilton Lockhart-controlled environments, requirements for AI, cloud and third-party providers, data retention, deletion and handover arrangements, ownership of Client information and system materials, and the process used to respond to security and data incidents.

This policy applies where it is incorporated into an accepted Engagement Document. Where an Engagement Document contains requirements specific to a particular project, those requirements apply to that project.

2. Definitions

Term	Definition
Approved Provider	A third-party AI, cloud, hosting, software, API or support provider approved for use in delivering the Services.
Background IP	Hamilton Lockhart's pre-existing or reusable systems, methods, software, code, templates, prompts, frameworks, designs and technical knowledge.
Business Day	A day other than a Saturday, Sunday or public holiday in New South Wales.
Client	The individual, business or organisation identified in the Engagement Document.
Client Data	Information, records, files, credentials and other material supplied by the Client or accessed through Client-controlled systems.
Client Environment	A system, device, account, network, storage service, software platform or technology environment owned, controlled or administered by the Client or its provider.
Confidential Information	Non-public business, operational, commercial, technical, financial or personal information disclosed in connection with the Services.
Deliverable	An item expressly identified for delivery to the Client in an Engagement Document.
Engagement Document	The accepted proposal, quote, agreement, statement of work or other written document describing the Services.
Hamilton Lockhart Environment	A device, account, system, repository, development environment or technology platform controlled or administered by Hamilton Lockhart.
High-Impact Action	An action that may materially affect a person's employment, finances, legal rights, safety, access to services, regulatory position or other significant interests.
High-Impact Output	AI-generated or automated output intended to inform, recommend, initiate or support a High-Impact Action.
Material Incident	A Security Incident that causes, or is reasonably likely to cause, significant harm, operational disruption, legal exposure or urgent protective action.

Term	Definition
Personal Information	Information or an opinion about an identified individual or an individual who is reasonably identifiable.
Security Incident	A suspected or confirmed event involving unauthorised access, disclosure, loss, alteration, misuse or compromise affecting Client Data, credentials, systems or Deliverables.
Sensitive Information	Personal Information treated as sensitive under applicable law, including health, biometric, racial, religious, political, sexual-orientation and criminal-record information.
Services	The work described in the Engagement Document.
Threat Actor	A person, group or automated system that attempts to gain unauthorised access to, manipulate, disrupt or extract value from a system, account or dataset without authorisation.

3. Information Hamilton Lockhart may handle

The information handled during an engagement depends on the agreed Services and may include:

- business workflows, procedures and operational records;
- documents, forms, emails, calendars and knowledge bases;
- employee, contractor, supplier and customer information;
- financial, invoice, payroll and transaction information;
- source code, configurations, logs and technical documentation;
- usernames, access tokens, API keys and other credentials;
- test data and generated outputs;
- system-performance and usage information; and
- engagement, support and billing records. Hamilton Lockhart will limit access to information reasonably required to deliver the Services. The Client will identify information that is legally privileged, highly confidential, safety-critical, regulated or subject to specific access, storage or residency requirements. Hamilton Lockhart may pause processing where information creates a legal, privacy or security risk requiring further safeguards or clarification.

3.1 Unsolicited information

Where Hamilton Lockhart receives Personal Information that was not requested, Hamilton Lockhart will assess whether the information could lawfully have been collected and whether it is reasonably necessary for the Services or Hamilton Lockhart's functions. If it is not reasonably necessary or cannot lawfully be retained, Hamilton Lockhart will, where lawful and technically practicable, return it, securely delete or destroy it, or de-identify it. Hamilton Lockhart may request a reduced or appropriately masked version and may preserve a limited record where required for security, evidence or legal compliance.

3.2 Sensitive and regulated information

Sensitive Information will be handled only where it is reasonably necessary for the Services, the handling has been expressly approved, any required notice, consent or legal authority has been established, and appropriate access, provider, retention and security arrangements have been agreed. Health information may be subject to Commonwealth, State or Territory health-record laws, including the Health Records and Information Privacy Act 2002 (NSW).

The Client is responsible for obtaining any consent, authority or approval required from affected individuals unless Hamilton Lockhart has expressly agreed to perform that function. Hamilton Lockhart may decline to receive or process information where adequate safeguards cannot be established.

3.3 Tax file number information

Hamilton Lockhart will handle an individual's tax file number only where the collection, recording, use or disclosure is permitted by law and required for an expressly agreed Service. The Client will remove or mask tax file numbers before providing payroll, employee or financial records where the tax file number is unnecessary for the agreed purpose.

Tax file number information will be restricted to authorised persons and systems, excluded from ordinary design, demonstration and testing, excluded from unapproved general-purpose AI services, used only for the permitted purpose, and returned or securely deleted when no longer lawfully required. A suspected compromise involving tax file number information will be treated as a priority Security Incident.

3.4 Payment-card information

Complete payment-card credentials will ordinarily be processed through an approved payment provider. Where payment-card information is included in Client material, Hamilton Lockhart may require the information to be removed, masked or redirected through an appropriate payment service.

4. Client authority and instructions

The Client is responsible for ensuring it is authorised to provide Client Data, materials and system access to Hamilton Lockhart. The Client will ensure that Client Data has been collected and supplied lawfully, all required notices have been provided, all required consents, permissions and authorities have been obtained, the agreed processing is lawful, the material does not infringe another person's rights, and Hamilton Lockhart is informed of any legal, contractual, security or residency restriction affecting the Services.

Hamilton Lockhart may refuse or suspend an instruction that appears unlawful, unsafe, materially insecure or outside the agreed Services.

5. Permitted use of Client Data

Hamilton Lockhart will not use Client Data, Confidential Information, derived confidential records, embeddings, vector representations, stored prompts, model inputs or outputs to train or improve a general-purpose or unrelated AI model without express written approval; develop an unrelated product using identifiable or Confidential Information; provide another client with Client Confidential Information; sell Client Data; or conduct unrelated advertising or marketing. This restriction does not prevent use of transient technical processing required to provide the approved Service where the relevant provider settings and terms have been assessed.

De-identified technical knowledge, general methods and reusable components may be retained and reused where they do not reveal Client Data or Confidential Information.

6. Collection notices, consent and recording

The Client is responsible for providing notices and obtaining consents relating to Personal Information collected or controlled by the Client. Hamilton Lockhart is responsible for notices relating to Personal Information collected directly by Hamilton Lockhart for its own business administration.

Where Hamilton Lockhart holds Personal Information solely for the Client, Hamilton Lockhart will provide reasonable assistance with notices, access requests and correction requests where included in the Services.

6.1 Recording and transcription

Hamilton Lockhart will record or transcribe meetings, calls or private conversations only where the recording or transcription is relevant to the Services, the participants have been appropriately informed, and any authority or consent required by law has been obtained. The Client is responsible for internal notices and authorisations relating to its employees, contractors and representatives unless otherwise agreed.

6.2 Legally privileged material

The Client should obtain legal advice before authorising legally privileged material to be processed through AI, cloud or third-party systems. Hamilton Lockhart will handle identified privileged material according to the agreed access and confidentiality requirements.

7. Data minimisation and handling

Hamilton Lockhart will apply handling controls appropriate to the sensitivity of the information and the purpose of the engagement.

- limiting information to what is reasonably required;
- using synthetic, masked, de-identified or minimised test data where practical;
- avoiding unnecessary copies and downloads;
- restricting access according to business need;
- reducing the inclusion of sensitive information in prompts, logs, screenshots and demonstrations;
- maintaining orderly Client workspaces within Hamilton Lockhart-controlled systems; and
- removing information when it is no longer required. Where Services are performed in a Client Environment, Hamilton Lockhart will use the Client's existing systems, storage structure, access controls and approved working arrangements to the extent reasonably practicable and consistent with the agreed Services, security requirements and technical design. Where Hamilton Lockhart selects or controls a service, it will select security settings appropriate to the information and intended use. Information will be treated as identifiable where individuals can reasonably be re-identified using the information and other available data.

7A. Data classification and project handling profile

Hamilton Lockhart will classify information according to the sensitivity of the information, the consequences of unauthorised access, disclosure, alteration or loss, and any legal, contractual or operational requirements applying to the engagement. Unless a different classification model is agreed, the following categories may be used:

- Public — information approved for public release and not subject to confidentiality restrictions.
- Internal — ordinary business information intended for authorised personnel and service providers, where disclosure would cause limited harm.
- Confidential — non-public business, personal, commercial or technical information requiring controlled access and approved handling.
- Restricted — information requiring enhanced safeguards because compromise may cause significant harm or trigger legal, regulatory, safety or contractual consequences, including Sensitive Information, tax file number information, credentials, payment-card information, biometric information and safety-critical records. For clarity, “Confidential” in this classification model is an operational handling category and does not limit or replace the broader defined term “Confidential Information” used elsewhere in this policy. Where proportionate to the engagement, the Engagement Document, design record or project security record will identify the highest expected classification, approved storage and processing locations, permitted providers, access requirements, testing restrictions, retention requirements and any additional safeguards. Information will be handled according to the highest applicable classification where a dataset, document or system contains information from more than one category.

8. Security controls

Hamilton Lockhart will use reasonable technical and organisational measures proportionate to the nature of the Services, the sensitivity of the information, the systems involved, the access provided and the foreseeable consequences of compromise. Controls used within relevant Hamilton Lockhart Environments may include supported operating systems and security updates, password or secrets-management systems, automatic device locking, access restricted according to business need, secure handling of passwords, tokens and recovery codes, removal of access when it is no longer required, and protection of credentials from public repositories, ordinary logs and AI prompts.

Additional controls may be applied where reasonably appropriate to the agreed scope, system and assessed risk, including multi-factor authentication, named user accounts, least-privilege permissions, scoped API access, separate development and production credentials, device encryption, endpoint protection, backup and recovery controls, and security and activity logging. Security controls within Client Environments remain subject to the systems, configurations and administration controlled by the Client.

9. Accounts, credentials and access

Credentials will be transferred through an approved secure method. Where access to a Client Environment is required, the Client will provide a named account where available, permissions limited to the agreed Services, temporary or time-limited access where appropriate, and access to the minimum systems and information required.

Shared administrator credentials and personal employee passwords should be avoided where a suitable alternative is available. Credentials received through an insecure channel may be rotated before use.

Each Party is responsible for removing access it controls. Hamilton Lockhart will remove or revoke Hamilton Lockhart-controlled access when it is no longer required.

The Client will remove or revoke Client-controlled access following handover, termination or notification from Hamilton Lockhart. Continuing access for support, monitoring or maintenance will be documented in the applicable engagement or support arrangement.

10. AI, cloud and third-party providers

Hamilton Lockhart may use Approved Providers to deliver the Services. Before using a material provider to process Personal Information, Sensitive Information or Confidential Information, Hamilton Lockhart will consider the information required by the provider, the provider's privacy and security terms, retention of prompts, inputs and outputs, model-training settings, access by provider personnel, available privacy and enterprise controls, data-processing locations, material subprocessors, access logging, deletion and export options, incident-notification arrangements, account control, and the Client's legal and operational requirements.

Material providers will be identified in an Engagement Document, provider schedule or another written engagement record where their use affects the Client's privacy, security, confidentiality or residency requirements. The record should identify the provider, purpose, account owner, payer, information categories processed, known processing location or region, material subprocessors where known, and material retention or model-training settings. Hamilton Lockhart will obtain written Client approval before enabling provider training on identifiable Client Data, materially changing an expressly agreed data-residency arrangement, or adopting a Hamilton Lockhart-selected replacement that materially changes the agreed privacy or security

position. Client approval does not replace any legal assessment, notice, consent or cross-border obligation that applies independently.

Where Hamilton Lockhart becomes aware that a material provider change is reasonably likely to affect an expressly agreed privacy, security, confidentiality or data-residency requirement, Hamilton Lockhart will notify the Client within a reasonable period.

10A. Privacy, security and AI risk assessment

Hamilton Lockhart will conduct a proportionate privacy, security or AI risk assessment where the proposed Services create elevated risk that is not adequately addressed by ordinary project controls. Assessment triggers may include:

- processing Sensitive Information or Restricted information at scale;
- employee monitoring, surveillance or behavioural assessment;
- use of health, biometric or children's information;
- a system that makes, recommends or materially supports a High-Impact Action;
- an AI agent with authority to access broad datasets, initiate transactions or perform irreversible actions;
- a material change in processing purpose, provider, data residency or system access;
- integration with critical operational, financial, safety or production systems; or
- another circumstance where the likely impact of failure, misuse or compromise is material. The assessment may record the intended purpose, information flows, lawful authority, affected people, providers, permissions, foreseeable misuse, human-review requirements, security controls, residual risks and approvals required before implementation. The depth and format of the assessment will be proportionate to the system and may be documented in the Engagement Document, design materials, a project risk register or a separate assessment.

10B. Approved Provider and subprocessor records

Where reasonably required by the assessed risk, applicable law or an Engagement Document, Hamilton Lockhart will maintain a proportionate record of material Approved Providers and subprocessors used in Hamilton Lockhart-controlled delivery environments. The record may identify the provider, purpose, information category, account owner, known processing location, material retention or training settings, and approval status.

Project-specific providers that materially affect privacy, security, confidentiality or residency requirements will also be identified in the Engagement Document or another written engagement record. The provider record is an operational document and may be updated without reissuing this policy, provided that any approval or notification required under clause 10 is completed.

11. Overseas processing

Client Data may be processed or stored outside Australia where an Approved Provider uses overseas infrastructure. Hamilton Lockhart will consider the location of the processing, the provider arrangement, the level of control retained, the contractual and technical protections available, and any legal or residency requirement applying to the engagement.

Where Australian Privacy Principle 8 or another cross-border requirement applies, the legally responsible Party will assess and take the steps required by law. Client approval alone does not remove a Party's independent obligations. The Client is responsible for providing notices to individuals concerning overseas processing of Client-controlled Personal Information unless that responsibility is expressly assigned to Hamilton Lockhart.

Hamilton Lockhart will provide reasonable information about material providers and processing locations relevant to the engagement.

12. Contractors and subprocessors

Hamilton Lockhart may engage contractors or subprocessors to assist with the Services. Where a contractor or subprocessor is given access to Client Data, Hamilton Lockhart will limit access to the agreed function, apply confidentiality and data-handling requirements, assess capability and access risk proportionate to the role, restrict access according to business need, and remove access when the work is complete.

Hamilton Lockhart remains responsible for the performance of the agreed Services carried out by its contractors. On reasonable request, Hamilton Lockhart will identify material contractors or subprocessors with access to Client Data, subject to privacy, confidentiality and security requirements.

12A. Personnel security and authorised use

Hamilton Lockhart personnel and contractors with access to Client Data or Client systems will be subject to confidentiality, privacy and security requirements appropriate to their role. Controls may include:

- role-appropriate privacy and security instruction;
- secure credential and secrets handling;

- restrictions on the use of personal accounts, devices and unapproved AI or cloud services;
 - access limited according to business need;
 - prompt reporting of suspected Security Incidents, phishing and social-engineering attempts; and
 - revocation or adjustment of access following completion of work, departure or a material change in responsibilities.
- Hamilton Lockhart may require additional screening, supervision or access restrictions where a role involves Restricted information, privileged access or material production authority.

13. AI agents, automation and human review

AI systems may produce inaccurate, incomplete, inconsistent, biased or unpredictable outputs. High-Impact Output must be reviewed and verified by a suitably authorised person before it is communicated externally, relied upon for a High-Impact Action, used to initiate an irreversible action, or used to make or implement a materially consequential decision.

Unless the Engagement Document expressly assigns operational review to Hamilton Lockhart, the Client is responsible for ensuring that this review occurs during operation of the system. AI agents and automations will be designed with controls proportionate to their authority and risk.

Controls may include restricted tools and data sources, limited service accounts, human approval steps, transaction and rate limits, audit logging, testing environments, pause and shutdown mechanisms, rollback procedures, and escalation to an authorised person. Controls addressing prompt injection specifically are set out in clause 13A.2.

The Client will maintain the accuracy and completeness of Client-controlled source information. Hamilton Lockhart will apply reasonable data-quality controls within the system design where the accuracy of source information materially affects the intended result.

13.1 Employee monitoring

Systems used to monitor employee communications, computer activity, location, productivity or conduct will be implemented only after the Client has considered applicable workplace, surveillance, employment and consultation requirements. The Client is responsible for required employee notices, consultation and authorisation unless Hamilton Lockhart has expressly agreed to assist.

13.2 Logging and monitoring

Logging and monitoring may collect usernames, timestamps, IP addresses, system actions, prompts and outputs, errors, device information and performance information. Logging will be limited to information reasonably required for security, audit, support, troubleshooting and system performance.

Access to logs will be restricted and logs will be retained according to their operational, legal and security purpose.

13A. Threat landscape and attack vectors

Systems designed, built or operated by Hamilton Lockhart, and the AI models and cloud infrastructure they depend on, are exposed to a range of threats that exist independently of any specific engagement. This section describes the threat categories Hamilton Lockhart designs against and the general mitigations applied.

13A.1 Threat categories

Hamilton Lockhart considers the following categories of threat when designing and operating a system, using recognised sources such as the OWASP Top 10 for LLM Applications, the OWASP Top 10 for Agentic AI and relevant Australian Signals Directorate guidance. The Essential Eight may be used as a useful baseline for applicable enterprise controls, but this policy does not represent that Hamilton Lockhart or a Client environment has achieved a certified Essential Eight maturity level:

- Prompt injection — an attacker embeds instructions in content an AI system processes (a document, email, webpage, API response, or other untrusted input) intending to override the system's actual instructions. This may be direct (instructions typed straight into a chat interface) or indirect (instructions hidden in content the AI reads on the Client's behalf). See clause 13A.2.
- Credential and account compromise — theft, guessing, phishing or leakage of passwords, API keys, tokens or session credentials, whether targeted at Hamilton Lockhart, the Client, or a shared Approved Provider.
- Excessive agent permissions — an AI agent granted broader tool access, data access or autonomy than its task requires, increasing the impact if the agent is compromised, manipulated, or simply makes an error.
- Data exfiltration — unauthorised extraction of Client Data or Confidential Information, including through a compromised integration, an over-permissioned agent, or a prompt-injection attack that instructs an AI system to leak information it has access to.
- Supply chain and provider compromise — a vulnerability, breach or malicious update introduced through a thirdparty library, Approved Provider, subprocessor or open-source component rather than through Hamilton Lockhart's or the Client's own systems.
- Social engineering and phishing — an attacker manipulates a person (Hamilton Lockhart personnel, Client personnel, or a shared contact) into granting access, approving a fraudulent action, or disclosing credentials.

- Model and output manipulation — attempts to cause an AI system to produce biased, false, harmful or manipulated output, including through data poisoning of retrieved content or adversarial inputs designed to bypass safety controls.
- Unauthorised access to production systems — direct attempts to access Hamilton Lockhart-controlled or Client-controlled infrastructure outside approved channels, including through misconfigured permissions or exposed services.

13A.2 Prompt injection mitigation

Prompt injection is treated as a standing, unresolved risk category rather than a defect that can be permanently eliminated. Current industry guidance, including OWASP's LLM Top 10, is explicit that prompt injection cannot be fully prevented through input filtering alone, because it exploits the way language models process instructions and untrusted content in the same channel.

Hamilton Lockhart's approach is defence in depth: multiple independent layers of mitigation, so that a single bypassed control does not result in a High-Impact Action. Depending on the system and its risk level, mitigations may include:

- segregating untrusted content (documents, emails, web pages, API responses) from system instructions, so an AI system is designed to treat retrieved content as data to evaluate, not as instructions to follow;
- least-privilege tool access — an agent is only given the specific tools and data sources its task requires, so a successful injection has a limited blast radius;
- human approval steps before a High-Impact Action is executed, rather than allowing an agent to act on injected instructions autonomously;
- output validation and allowlisting, so an agent's proposed action is checked against expected parameters before it is executed;
- rate, value and scope limits on what an agent can do in a single action or time period, to reduce the impact of a compromised or manipulated session;
- logging of prompts, tool calls and outputs sufficient to detect and investigate a suspected injection after the fact; and
- periodic adversarial testing of higher-risk agents, where proportionate to their authority and the information they can access. No combination of these controls eliminates prompt injection risk entirely. Hamilton Lockhart will disclose the general mitigation approach applied to a specific agent or system on reasonable request, and will treat a suspected promptinjection compromise as a Security Incident under clause 17.

13B. AI agent security requirements, Client use and responsibility

This clause applies to AI agents and autonomous or semi-autonomous systems Hamilton Lockhart designs, configures, deploys or supports for the Client, including Executive Assistant, Personal Assistant and similarly named agents. It establishes the security guardrails for their operation, the Client's obligation to preserve those guardrails, and responsibility where the Client changes or operates a system outside its approved design.

13B.1 Hamilton Lockhart security design and operating guardrails

Hamilton Lockhart will design an agent's initial permissions, tool access, data access, autonomy, approval requirements and operating environment proportionate to its intended purpose and foreseeable risk. At handover or go-live, for each material production agent within the agreed scope, Hamilton Lockhart will provide proportionate written security and operating requirements identifying the controls that are conditions of safe and supported operation.

These may include:

- the sandbox, test environment, hosting environment or network boundary within which the agent must operate;
- the specific tools, systems, mailboxes, repositories, applications and data sources the agent may access;
- the permissions, service accounts, credentials, transaction limits, rate limits and spending limits assigned to the agent;
- actions the agent may perform autonomously and actions requiring review or approval by an authorised person;
- prohibited actions, prohibited information sources and restrictions on external communications or irreversible actions;
- logging, monitoring, escalation, pause, shutdown, rollback and incident-response controls; and
- any other configuration, safeguard or operating instruction identified as necessary for secure or supported use. A safeguard or operating requirement relied upon under this clause will be identified with reasonable specificity in the design documentation, system register, handover material, Support Guide or another written engagement record.

13B.2 Client obligations for operation and use

The Client will operate each agent and system in accordance with the documented design, security requirements and operating instructions supplied by Hamilton Lockhart. The Client will:

- keep the agent within any required sandbox, test environment, hosting boundary or other identified operating environment;
- maintain the approved permissions, tool access, data access, service accounts, transaction limits and human-approval steps;
- ensure that employees, contractors, administrators and other providers with access to the agent are informed of and comply with the applicable requirements;
- not disable, bypass or remove a security control, approval gate, logging function, monitoring control, rate limit, content restriction, pause mechanism or shutdown mechanism identified as a condition of operation;

- not connect the agent to an additional system, mailbox, tool, data source, credential or production environment, or materially increase its autonomy, without the review or approval required under the engagement;
- maintain the accuracy and security of Client-controlled systems and information on which the agent relies;
- promptly report suspected misuse, unexpected behaviour, permission drift, unauthorised changes or Security Incidents; and
- suspend or restrict the agent where Hamilton Lockhart reasonably advises that continued operation creates a material security, privacy, operational or legal risk. These requirements are conditions of the agent's safe and supported operation. The Client is responsible for controlling the persons and accounts authorised to administer or alter Client-controlled agents, systems and environments.

13B.3 Client changes and departure from guardrails

A Client-controlled change includes a change made by the Client or by an employee, contractor, administrator, technology provider or other person acting with access or authority provided by the Client. It includes an intentional or accidental change to permissions, connected systems, data access, tools, autonomy, approval requirements, operating environment, security controls or other documented guardrails.

Where the Client wishes to make a material change, the Client will request Hamilton Lockhart's review before the change takes effect where review is required by the Engagement Document, handover material, Support Guide or documented operating requirements. Hamilton Lockhart may recommend additional testing, controls, documentation or scope before approving or supporting the changed configuration.

The Client is responsible for a Security Incident, error, unintended action, data loss, unauthorised disclosure, operational disruption or other adverse outcome to the extent it is caused or contributed to by:

- operation of an agent outside the documented design or operating requirements;
- removal of the agent from an identified sandbox, test environment, hosting boundary or restricted environment;
- the grant of permissions, tools, credentials, data access or autonomy beyond the approved configuration;
- the removal, bypass or disabling of a required human-approval step or security control;
- a Client-controlled change that was not submitted for required review or was implemented contrary to Hamilton Lockhart's written advice; or
- continued operation after the Client knew, or was advised, that the agent was behaving unexpectedly or creating a material risk. Hamilton Lockhart's responsibility remains applicable to the original design, configuration and Services it supplied, including any defect or failure within that agreed scope that contributed to the outcome. Where an outcome has multiple causes, responsibility will be assessed under clause 17.8 by reference to the documented design, the applicable guardrails, the changes made, each Party's control and each Party's contribution to the outcome.

13B.4 Ongoing monitoring and permission drift

Ongoing monitoring, configuration review and detection of permission or behavioural drift are included only where expressly stated in an Engagement Document, Support Guide or ongoing support arrangement. Unless that monitoring is included, Hamilton Lockhart is not responsible for continuously detecting Client-controlled changes, altered permissions, disabled safeguards or operation outside the documented configuration.

The Client remains responsible for reporting known or suspected departures promptly.

13B.5 AI agent and system register

For each material production AI agent or autonomous system designed or operated by Hamilton Lockhart, a proportionate system record will be prepared at handover or go-live where reasonably required by the system's authority, risk or the Engagement Document. Ongoing maintenance of that record is included only where stated in an active support arrangement.

The record may form part of the design documentation, handover schedule or support record and will identify, where applicable:

- the system purpose and authorised business owner;
- connected tools, systems and data sources;
- service accounts, credentials or machine identities;
- approved actions, prohibited actions and transaction limits;
- High-Impact Actions and required human approvals;
- required operating environments, sandboxes and material security guardrails;
- logging, monitoring and incident-escalation arrangements;
- the party responsible for support, configuration and access administration; and
- the process for suspension, credential revocation and decommissioning. The Client will notify Hamilton Lockhart of material changes to registered information where Hamilton Lockhart provides ongoing support or monitoring that depends on the accuracy of that record.

13C. Secure development, testing and release

Hamilton Lockhart will apply development and release controls proportionate to the risk, complexity and production authority of the system. Controls may include:

- use of synthetic, masked, de-identified or minimised data during development and demonstration where practical;
- separation of development, testing and production credentials and environments where appropriate;
- review and testing of material functionality, permissions and failure conditions before production release;
- recording of material configuration, integration and permission changes;
- approval before a material production change where required by the engagement;
- rollback, recovery or disablement arrangements proportionate to the likely impact of failure; and
- restriction of direct production changes to authorised persons and approved methods. Testing reduces but does not eliminate the possibility of defects, provider changes, model variation, unexpected interactions or misuse after release.

13D. Vulnerability and dependency management

During development, any expressly agreed warranty period and any active support arrangement that includes vulnerability management, Hamilton Lockhart will manage known vulnerabilities and material software dependencies within Hamilton Lockhart-controlled Deliverables according to the agreed scope and the risk presented. Where included in the applicable scope and reasonably practicable, Hamilton Lockhart will assess known material security issues, determine an appropriate response having regard to exploitability, likely impact, available fixes, provider dependencies and Client-controlled constraints, and notify the Client where remediation requires Client action, access, downtime, approval or a provider change.

Known material unresolved vulnerabilities or unsupported dependencies identified at handover will be disclosed where they materially affect the safe or supported operation of the Deliverable. Continuous vulnerability scanning, penetration testing, security operations monitoring and third-party code auditing are included only where expressly stated in the Engagement Document or support arrangement.

13E. AI interaction transparency

The Parties will consider whether users, employees, customers or other affected people should be informed that they are interacting with an AI system or that Personal Information, communications or decisions are being processed or materially assisted by AI. Depending on the system and applicable requirements, transparency controls may include identification of an AI assistant, notice of recording or transcription, explanation of material limitations, disclosure that content is AI-generated or AI-assisted, and a practical method for escalation to an authorised person.

The Client is responsible for providing customer, employee and stakeholder notices within Client-controlled operations unless Hamilton Lockhart has expressly agreed to assist. Hamilton Lockhart will identify known system behaviour that materially affects the content of those notices.

14. Security responsibilities

14.1 Hamilton Lockhart responsibilities

- security design within the agreed scope;
- secure configuration of Hamilton Lockhart Deliverables;
- handling credentials provided for the Services;
- applying agreed access controls;
- testing Hamilton Lockhart-developed components;
- restricting AI-agent permissions according to the approved design;
- protecting Hamilton Lockhart-controlled development materials;
- responding to identified defects within the agreed scope; and
- performing the incident-response obligations in this policy.

14.2 Client responsibilities

- Client networks, devices and accounts;
- administration of Client Environments;
- employee and contractor access;
- internal backups and recovery;
- physical security;
- business continuity;
- internal security monitoring;
- accuracy and maintenance of Client-controlled data;
- required notices, consents and internal approvals;
- regulatory obligations applying to the Client's operations;
- changes made after implementation; and
- revocation of Client-controlled access.

14.3 Shared responsibilities

The Parties will cooperate in relation to access design, integration security, provider selection, testing, incident containment, investigation, recovery, regulatory assessment and communication with affected parties. Responsibilities specific to an engagement may be further described in the Engagement Document.

14.4 Business continuity, backup and recovery

Backup, restoration, continuity and disaster-recovery services are not included unless an Engagement Document expressly says they are. Where those services are included, the Engagement Document or handover material may identify the Party controlling the relevant mechanism, provider dependencies, restoration responsibility and any expressly agreed testing or downtime objective.

The existence of a backup does not guarantee restoration within a particular period or without data loss. Any recovery-time objective, recovery-point objective, availability commitment or recovery test must be expressly agreed. The Client remains responsible for business continuity, backups and recovery for Client-controlled systems unless an Engagement Document expressly allocates a responsibility to Hamilton Lockhart.

15. Data retention and deletion

Hamilton Lockhart retains Client Data only while it is reasonably required for the agreed system or Services, support or maintenance, incident investigation, legal or regulatory compliance, taxation and business records, insurance requirements, or the establishment or defence of legal rights. The Engagement Document or Deployment Approval may outline the information categories retained by a production solution and any configuration controlled by Hamilton Lockhart.

Hamilton Lockhart does not guarantee a fixed retention or deletion period unless one is expressly agreed and technically supported. Temporary and operational copies controlled by Hamilton Lockhart will be deleted, de-identified or scheduled for deletion when no longer reasonably required. Billing, contract, incident, audit and security records may be retained for their lawful or evidentiary purpose.

Deletion is limited to systems and copies within Hamilton Lockhart's administrative control and remains subject to residual backups, provider deletion cycles, immutable logs, technical limitations, legal holds and statutory requirements. Hamilton Lockhart is not responsible for deletion from Client-controlled systems or third-party systems outside its administrative control. The Client remains responsible for retention and deletion in Client-controlled systems.

16. Ownership and handover

The Client owns Client Data, Client branding, Client records, Client credentials, and Client systems and materials existing before the engagement. Hamilton Lockhart owns its Background IP.

Ownership and licensing of each Deliverable will be stated in the Engagement Document. Third-party components remain subject to the relevant provider or open-source licence terms.

Where handover is included, Hamilton Lockhart will provide the agreed material in a format reasonably available from the relevant system. The Engagement Document will identify whether material third-party accounts are Client-owned from creation, transferred to the Client at handover, or retained by Hamilton Lockhart as part of an ongoing hosted Service.

At handover, Hamilton Lockhart will provide the agreed Client-owned materials, remove or adjust Hamilton Lockhart-controlled access, transfer agreed credentials and administrative controls, document known limitations and outstanding issues, and transfer ongoing responsibilities according to the agreed handover arrangements. The Client will revoke Client-controlled temporary access and assume the responsibilities allocated to it under the handover arrangements.

16.1 Decommissioning and access closure

Where decommissioning is included, the Parties will complete the actions reasonably required to stop unauthorised or unintended continued operation of the solution. Actions may include:

- disabling agents, workflows, scheduled jobs and webhooks;
- revoking service accounts, API keys, tokens and temporary credentials;
- transferring, closing or reassigning provider accounts;
- exporting agreed Client-owned records and configuration material;
- removing Hamilton Lockhart-controlled access and integrations;
- recording unresolved dependencies, retained records and continuing responsibilities; and
- scheduling operational project copies for deletion in accordance with clause 15. On reasonable request, Hamilton Lockhart may provide written confirmation that specified Hamilton Lockhart-controlled operational copies have been deleted or scheduled for deletion, subject to residual backups, legal retention and provider limitations.

17. Incident reporting and response

Hamilton Lockhart maintains a proportionate process for suspected and confirmed Security Incidents. Included incident responsibilities are limited to notification of material incidents within Hamilton Lockhart's control, reasonable immediate containment within Hamilton Lockhart-controlled systems, preservation of relevant available evidence, cooperation with legally required assessment or notification concerning Hamilton Lockhart's conduct or systems, and correction of a qualifying defect for which Hamilton Lockhart is responsible under the applicable agreement.

Forensic investigation, data reconstruction, restoration, rebuilding, extended recovery coordination, investigation of Client-controlled accounts or systems, and investigation or remediation of Third-Party Services are additional chargeable Services unless an Engagement Document or support arrangement expressly includes them. Except for urgent protective action or a legal obligation that cannot reasonably wait, Hamilton Lockhart will obtain Client approval before material chargeable incident work begins.

17.1 Reporting

Security and privacy concerns may be reported to josh@hamiltonlockhart.com or 0412 034 742 during ordinary business hours. These channels are monitored during ordinary business operations and do not provide 24-hour monitoring or a guaranteed response time unless an Engagement Document expressly states otherwise. A report should include, where available, the affected system or information, when the issue was identified, the suspected activity, actions already taken, relevant screenshots or logs, and a person available for coordination.

The Client will report suspected incidents promptly and preserve available evidence.

17.2 Initial triage

Hamilton Lockhart will perform an initial assessment sufficient to identify urgent action and responsibility within the agreed scope. A broader assessment of cause, systems, information, credentials, provider involvement or business impact may be chargeable where it concerns Client-controlled or third-party environments or falls outside an included support arrangement.

17.3 Containment

Hamilton Lockhart may take immediate containment action within systems and access its controls. Containment may include suspending credentials, disabling integrations, pausing AI agents or automated workflows, restricting system access, isolating affected components, preserving logs, blocking malicious inputs, rotating Hamilton Lockhart-controlled secrets, and contacting an affected provider.

Where containment requires action in a Client Environment, Hamilton Lockhart will notify the Client and coordinate the required steps. Urgent protective action may be recommended before the cause or full impact has been confirmed.

17.4 Investigation and assessment

Hamilton Lockhart will investigate matters within its control to the extent reasonably required by an express responsibility, applicable remedy obligation or law. Investigation of shared, Client-controlled or third-party systems requires cooperation and may be chargeable under clause 17 unless the applicable agreement states otherwise. Any investigation will balance containment, recovery, privacy and preservation of relevant evidence.

Investigation activities will balance containment, recovery and preservation of evidence.

17.5 Client notification

Hamilton Lockhart will notify the Client without undue delay where a suspected or confirmed Security Incident may require protective action by the Client, materially affects or may materially affect Client Data, credentials, systems or operations, affects a Deliverable, or creates a material legal, regulatory or contractual risk. The initial notification may contain preliminary information and will be updated as material facts become available.

Where reasonably practicable, Hamilton Lockhart aims to provide the initial notification within one Business Day after becoming aware of a Material Incident. Urgent protective information will be communicated as soon as reasonably practicable.

17.6 Recovery and remediation

Recovery activities may include restoring affected components, rotating credentials, correcting configurations, removing malicious content, repairing integrations, validating data integrity, retesting affected workflows and documenting safeguards where those activities fall within Hamilton Lockhart's express responsibility or are separately approved. Hamilton Lockhart will correct qualifying security defects in Hamilton Lockhart Deliverables according to the applicable agreement. Other recovery and remediation work is chargeable unless expressly included.

The Client will remediate Client-controlled systems, accounts and infrastructure. The Parties will coordinate recovery where the incident crosses both environments.

17.7 Regulatory and contractual assessment

The Parties will assess whether the incident triggers obligations under privacy, tax file number, surveillance, employment, sector-specific, contractual, insurance or other applicable requirements. Where the Notifiable Data Breaches scheme applies and there are reasonable grounds to suspect an eligible data breach, the legally responsible entity will conduct a reasonable and expeditious assessment and take all reasonable steps to complete that assessment within 30 days after becoming aware of the grounds for suspicion.

Where there are reasonable grounds to believe an eligible data breach has occurred, the responsible entity will notify the Office of the Australian Information Commissioner and affected individuals as soon as practicable, unless an exception applies. The Client is responsible for notifications concerning Personal Information collected or controlled by the Client.

Hamilton Lockhart will provide timely information and reasonable assistance required for the Client's assessment and notification. Hamilton Lockhart remains responsible for any assessment or notification it is independently required to make.

The Parties will coordinate where information is held by or on behalf of more than one entity and will not delay urgent protective action while notification responsibility is being determined.

17.8 Incident responsibility

Hamilton Lockhart is responsible to the extent a Security Incident is caused or contributed to by Hamilton Lockhart's breach, negligence, credential mishandling, failure to perform an expressly agreed security responsibility, or failure to exercise reasonable care when selecting or configuring a provider within its control. The Client is responsible for incidents arising from Client-controlled systems, accounts, access, data, infrastructure, unauthorised changes, failure to follow agreed safeguards, or failure to revoke or restrict access under its control.

Where an incident has multiple causes, responsibility will be allocated according to each Party's contribution, control, agreed scope and compliance with its responsibilities. Third-party involvement, provider conduct and the configuration of shared systems will be considered when assessing responsibility.

Liability is governed by the applicable agreement and law.

17.9 Closure and review

An incident may be closed after containment, recovery, required notifications and agreed remediation have been completed or formally transferred. Hamilton Lockhart will record material findings, actions taken, remaining risks and recommended improvements.

Following a Material Incident, Hamilton Lockhart will review relevant technical, procedural and contractual controls and update them where appropriate. The Client will be informed of material changes affecting the Client's systems, responsibilities or future use of the affected solution.

18. Privacy requests and complaints

A Client or an individual may contact Hamilton Lockhart regarding Personal Information held by Hamilton Lockhart. Where applicable, an individual may request access to or correction of their Personal Information.

A Client may request the return, correction, deletion or de-identification of Client Data held by Hamilton Lockhart, subject to the applicable agreement and legal, contractual, technical and backup limitations. Where Hamilton Lockhart holds Personal Information solely on behalf of a Client, Hamilton Lockhart may refer the request to the Client and provide reasonable assistance.

Requests may be subject to identity or authority verification. Privacy and security requests may be made through Hamilton Lockhart's usual business contact channels.

Hamilton Lockhart aims to acknowledge a privacy or security request within five Business Days and respond substantively within a reasonable period having regard to its nature and complexity. Business Day means a day other than a Saturday, Sunday or public holiday in New South Wales. This administrative target does not create 24-hour monitoring, a guaranteed response time or an incident-response service beyond the applicable agreement and clause 17. Where Hamilton Lockhart cannot comply with a request, it will explain the reason to the extent reasonably and legally permitted.

Where applicable, an individual may be entitled to complain to the Office of the Australian Information Commissioner or another relevant regulator after first raising the concern with Hamilton Lockhart.

19. Privacy status and legal application

Based on its current turnover and activities, Hamilton Lockhart may qualify for the small-business exemption under the Privacy Act 1988. The application of the Privacy Act may vary according to the information handled, the activity performed and a particular engagement. This contractual policy is not represented as a complete public-facing privacy policy or collection notice. Hamilton Lockhart will maintain or publish a separate privacy notice if and when applicable law or its operations require one.

Certain activities, information types and contractual arrangements may be subject to the Privacy Act 1988, the Australian Privacy Principles, the Notifiable Data Breaches scheme, the Privacy (Tax File Number) Rule 2015, State or Territory health-record legislation, surveillance and workplace laws, or other sector-specific privacy requirements. Hamilton Lockhart applies the safeguards in this policy as contractual standards and operational practice.

Where applicable law imposes a higher or more specific requirement, that requirement prevails.

20. Policy governance

Hamilton Lockhart intends to review this policy periodically and may review it earlier where reasonably appropriate following a Material Incident or a material change to Hamilton Lockhart's Services, systems, providers or applicable legal requirements. A failure to complete an internal review by a particular administrative date does not itself expand the Services or create an operational warranty, without limiting applicable law or an Engagement Document.

Operational registers, provider records, project handling profiles, handover schedules, development checklists and internal incident plans may be maintained separately from this client-facing policy. Their existence does not add a Deliverable or service that is not expressly included in an Engagement Document.

This policy forms part of Hamilton Lockhart's contractual documentation only when incorporated by reference in the applicable Engagement Document. Version 1.7 was approved by Joshua Ernest Hamilton and is effective 28 August 2026.