

Specimen — illustrative example

Aldergrove Legal is a fictional organisation. This document comes from the scenario described on riskwoven.com/examples, and is not an assessment of any real entity. It is advisory output to support your own decisions: not legal advice, not a certification, and not an audit.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

Information Security Policy

Aldergrove Legal

Document type	policy	Version	1.0 Draft
Owner	Director of Practice Operations	Customer decision role	Managing Partner
Effective date	Upon customer release	Review cycle	Annual
Framework basis	RiskWoven AI practical best practices		
Jurisdiction	Ontario, Canada		
Prepared for	Aldergrove Legal	Industry	Legal services
Organization size	26-100	Locations	Not specified

Advisory draft for accountable-owner and professional review. Validate legal, regulatory, contractual, technical and operational requirements before customer release. This is not legal advice, a certification, or a compliance determination.

1. Purpose

This policy sets Aldergrove Legal's mandate for protecting the information, systems and services on which the firm and its clients depend. It establishes what must be true, why it

matters, and who is accountable for making it so.

Aldergrove Legal holds privileged client communications, matter files, discovery sets, trust account records and employee data. The confidentiality, integrity and availability of that information is a professional and ethical obligation, not only a technical one. A failure to protect it can harm clients, expose the firm to regulatory action and damage the trust on which the practice depends.

This policy applies to every person who accesses Aldergrove Legal information or systems: lawyers, clerks, administrative staff, the IT Manager, managed service provider personnel and any other third party granted access. It applies regardless of the device or location from which access occurs.

2. Scope

This policy covers all information assets owned or held by Aldergrove Legal, including:

- The on-premises document management system holding privileged matter files, located in the Toronto office.
- The discovery review platform.
- The trust accounting system.
- Microsoft 365 mail and calendars, hosted in the Canadian region.
- Lawyer and clerk laptops issued by the firm.
- Any other system, service or data store that collects, processes, stores or transmits Aldergrove Legal information.

Client material must not be stored or processed on personal devices. This prohibition is absolute and applies to all staff regardless of seniority.

This policy does not duplicate the detailed requirements set out in the firm's existing instruments. Where a sibling document owns a topic — access control, data classification, records retention, third-party risk, privacy, business continuity or incident response — this policy states the mandate and defers the specifics to that instrument.

3. Definitions

Information asset. Any data, record, system, application, device or service that Aldergrove Legal owns, operates or is responsible for protecting. This includes digital and physical records, licensed software, cloud services and the hardware on which they run.

Control owner. The individual accountable for ensuring that a specific security control is implemented, operating as intended and reviewed on schedule. The control owner is named in the asset inventory or the relevant standard. Accountability cannot be delegated away, though operational tasks may be assigned to others.

Security incident. Any event, or credible suspicion of an event, that has compromised or may compromise the confidentiality, integrity or availability of Aldergrove Legal information or systems. This includes unauthorised access, data loss, ransomware, system outage affecting client services, and any breach of privilege. Suspected incidents must be treated as confirmed until investigation shows otherwise.

Risk acceptance. A documented decision by the Managing Partner to tolerate a known security risk rather than remediate it, on the basis that the cost or impact of remediation outweighs the residual risk. Risk acceptance is time-limited, recorded and subject to review. It does not extinguish the risk or the firm's obligations.

4. Accountability and Governance

Managing Partner holds ultimate accountability for information security at Aldergrove Legal. The Managing Partner reviews and endorses this policy annually, accepts residual risks that exceed the IT Manager's authority, and is notified without delay when a security incident may affect privilege.

Director of Practice Operations owns this policy. The Director ensures the policy is implemented, that control owners are assigned, that the annual review occurs, and that material control failures are escalated to the Managing Partner. The Director also serves as the primary escalation contact for security incidents.

IT Manager is responsible for the day-to-day operation of security controls: maintaining the asset inventory, executing vulnerability management, coordinating with the managed service provider, and acting as the first point of contact for reported incidents. The IT Manager escalates to the Director of Practice Operations in accordance with the Security Incident Response Procedure.

Responsible lawyer on each matter is accountable for the security of information held on that matter, including ensuring that access is limited to those with a legitimate need and that any concern about the security of privileged material is reported immediately.

All staff must comply with this policy, complete required security awareness training, report suspected incidents promptly, and not circumvent controls.

Managed service provider personnel operate under the terms of their agreement with Aldergrove Legal and are bound by this policy to the extent of their access. Third-party obligations are governed by the Third-Party Risk Management Policy.

5. Information Asset Inventory and Classification

Aldergrove Legal must maintain a current inventory of its information assets. Every asset in the inventory must have a named control owner and a classification.

The IT Manager maintains the inventory. The Director of Practice Operations reviews it on a cycle set by Aldergrove Legal; annually is offered as a starting point and is not derived from any cited control. This value is the organisation's to set and must be recorded in the inventory itself.

Classification governs how information is handled throughout its life. Privileged client communications, matter files, discovery sets and trust account records carry the highest sensitivity. Privileged material governs the classification of everything it touches: a document that contains or references privileged content is treated as privileged regardless of its format or location.

The detailed classification scheme, handling requirements and labelling rules are set out in the Data Classification and Handling Standard. This policy mandates compliance with that standard. Where a conflict appears between this policy and that standard, the Director of Practice Operations resolves it.

No new system, service or data store may be used to hold Aldergrove Legal information until it has been added to the asset inventory and a control owner has been assigned.

6. Access Control

Access to Aldergrove Legal information and systems must be granted on the basis of least privilege: each person receives only the access necessary for their role, and no more.

Access to privileged matter files is further restricted to the responsible lawyer and those they have specifically authorised for that matter. The IT Manager must be able to produce an access record for any matter file on request.

Access rights must be reviewed on a cycle set by Aldergrove Legal; quarterly is offered as a starting point and is not derived from any cited control. Reviews of access to privileged matter files and the trust accounting system must be conducted by the responsible lawyer or the Director of Practice Operations respectively, with the outcome recorded in the access register.

Access must be revoked or adjusted without delay when a person's role changes or their employment or engagement ends. The IT Manager is responsible for executing revocation. The Director of Practice Operations is responsible for ensuring that HR and IT processes are coordinated so that no access persists beyond the point of departure.

The detailed authentication requirements, including password standards and multi-factor authentication obligations, are set out in the Password and Authentication Standard. The detailed access control rules are set out in the Access Control Policy. This policy mandates compliance with both instruments.

7. Secure Configuration and Vulnerability Management

All systems and devices used to access or process Aldergrove Legal information must be configured securely before they are placed into use and maintained in a secure state throughout their operational life.

The IT Manager is accountable for maintaining secure configurations across the on-premises document management system, the discovery review platform, the trust accounting system, Microsoft 365 and all firm-issued laptops. The managed service provider supports this work under the terms of its agreement, but accountability remains with the IT Manager.

Vulnerabilities must be identified, assessed and remediated in accordance with the Patch Management Procedure. The IT Manager must ensure that critical vulnerabilities — those that could expose privileged client material or trust account records — are prioritised above all others. The target remediation window for critical findings is set by Aldergrove Legal and must be recorded in the asset inventory or a supporting standard; a window of 14 days is offered as a starting point and is not derived from any cited control.

Malware defences must be maintained in accordance with the System Integrity and Malware Defence Standard.

No system or device that cannot be maintained in a secure configuration may be used to access Aldergrove Legal information.

8. Monitoring and Logging

Aldergrove Legal must maintain sufficient monitoring and logging to detect security incidents, support investigation and demonstrate that controls are operating.

The IT Manager is responsible for ensuring that logs are collected from critical systems — the document management system, the trust accounting system, Microsoft 365 and firm-issued laptops — and that those logs are protected from tampering.

Logs must be retained for a period set by Aldergrove Legal and recorded in the Records Retention and Disposal Policy. That policy governs retention; this policy mandates that the retention obligation is met.

The IT Manager reviews monitoring outputs on a cycle set by Aldergrove Legal; weekly is offered as a starting point for critical systems and is not derived from any cited control. Anomalies that may indicate a security incident must be escalated in accordance with the Security Incident Response Procedure.

Monitoring of staff activity must be proportionate, disclosed to staff in accordance with applicable Ontario privacy law, and consistent with the Privacy and Personal Information Policy.

9. Information Protection Throughout Its Lifecycle

Aldergrove Legal must protect information from the point it is collected or created through to its lawful disposal.

Collection and creation. Information must be collected only for a legitimate matter or business purpose. Privileged material must be classified and handled as such from the moment it is created or received.

Use and processing. Information must be used only for the purpose for which it was collected. Access during use is governed by Section 6 of this policy.

Storage. Client material must be stored only in the on-premises document management system or Microsoft 365 Canadian region. It must not be stored on personal devices, personal cloud accounts or any system not listed in the asset inventory.

Transmission. Privileged material must be transmitted only over encrypted channels. The IT Manager is responsible for ensuring that the firm's email and file-sharing services meet this requirement. Staff must not transmit privileged material over unencrypted or personal channels.

Retention. Retention periods are governed by the Records Retention and Disposal Policy. This policy mandates compliance with that instrument.

Disposal. Information must be disposed of in a manner that prevents recovery. Physical records must be shredded. Digital records must be deleted in a manner that renders them unrecoverable from the relevant system. The IT Manager is responsible for ensuring that disposal methods meet this standard. Disposal must be recorded.

10. Change and Risk Assessment

Aldergrove Legal must assess security risk before making material changes to technology, suppliers or business processes.

A change is material if it could affect the confidentiality, integrity or availability of information assets, alter the firm's attack surface, introduce a new supplier with access to firm systems or data, or change the way privileged material is handled.

The IT Manager identifies whether a proposed change is material and, if so, conducts or coordinates a security risk assessment before the change proceeds. The Director of Practice Operations reviews the assessment. Where the assessment identifies risks that cannot be remediated before the change, the Managing Partner must be informed and must record a risk acceptance decision before the change proceeds.

Changes involving third-party suppliers are also subject to the Third-Party Risk Management Policy. Changes involving AI tools or services are also subject to the AI Acceptable Use Policy, the AI Risk Management Standard and the AI Governance and Accountability Policy.

Emergency changes required to meet a court deadline or to contain an active incident may proceed with concurrent rather than prior assessment, provided the assessment is completed and recorded as soon as practicable and the Director of Practice Operations is notified.

11. Incident Response

Aldergrove Legal must be able to detect, contain, investigate and recover from security incidents.

All staff must report a suspected security incident to the IT Manager immediately. The IT Manager escalates to the Director of Practice Operations. Where the incident may affect privilege, the Director of Practice Operations notifies the Managing Partner without delay.

The ordered steps for responding to a security incident are set out in the Security Incident Response Procedure. All staff must be familiar with their obligations under that procedure. The IT Manager is responsible for ensuring the procedure is current and tested.

Where an incident involves a privacy breach, the Privacy Breach Response Procedure also applies. Where it involves an AI system, the AI Incident Response Procedure also applies.

After-hours incidents are escalated through the managed service provider, which must have current contact details for the Director of Practice Operations and the Managing Partner. The managed service provider's escalation obligations are set out in its agreement with the firm.

Every security incident must be recorded. The record must include the timeline, the systems and information affected, the actions taken and the outcome. The IT Manager maintains the incident record. The Director of Practice Operations reviews it.

12. Backup, Recovery and Business Continuity

Aldergrove Legal must maintain backup and recovery capabilities sufficient to restore critical systems and information following an incident.

Critical systems for this purpose are the on-premises document management system, the trust accounting system and Microsoft 365. The IT Manager is responsible for ensuring that backups of these systems are taken, tested and stored in a manner that allows recovery.

The recovery time and recovery point objectives for each critical system are set by Aldergrove Legal and must be recorded in a supporting standard or the Business Continuity Policy. This policy mandates that those objectives exist, are tested and are met. The information supplied does not supply specific RTO and RPO values; Aldergrove Legal must set them before this policy takes effect.

Backup integrity must be tested on a cycle set by Aldergrove Legal; quarterly is offered as a starting point and is not derived from any cited control. Test results must be recorded and reviewed by the IT Manager.

Business continuity obligations, including the firm's response to extended outages affecting court-deadline matters, are governed by the Business Continuity Policy. This policy mandates compliance with that instrument.

13. Third-Party and Supplier Security

Third parties with access to Aldergrove Legal information or systems — including the managed service provider — must meet security requirements consistent with this policy.

The security obligations of each third party must be set out in a written agreement before access is granted. The Director of Practice Operations is accountable for ensuring that agreements are in place.

Third-party access must be limited to what is necessary for the service being provided. The IT Manager reviews third-party access on a cycle set by Aldergrove Legal; annually is offered as a starting point and is not derived from any cited control.

The detailed requirements for assessing and managing third-party risk are set out in the Third-Party Risk Management Policy. The steps for reviewing third-party AI tools are set out in the Third-Party AI Review Procedure. This policy mandates compliance with both instruments.

14. Security Awareness and Training

Every person bound by this policy must understand their security obligations and be equipped to meet them.

The IT Manager, under the direction of the Director of Practice Operations, is responsible for ensuring that security awareness training is provided to all staff. Training must cover at minimum: recognising phishing and social engineering, handling privileged material, reporting suspected incidents, and the prohibition on storing client material on personal devices.

New staff must complete security awareness training before they are granted access to client matter files. Existing staff must complete refresher training on a cycle set by Aldergrove Legal; annually is offered as a starting point and is not derived from any cited control. Completion must be recorded.

The IT Manager reports training completion rates to the Director of Practice Operations as part of the annual policy review.

15. Risk Acceptance

Where a known security risk cannot be remediated, Aldergrove Legal may accept it rather than leave it unrecorded.

Only the Managing Partner may accept a security risk. The IT Manager documents the risk, the reason remediation is not being pursued, the residual exposure and the proposed acceptance period. The Director of Practice Operations reviews the documentation before it is presented to the Managing Partner.

Risk acceptance is time-limited. The acceptance period is set by the Managing Partner at the time of the decision and must not exceed a period set by Aldergrove Legal; 12 months is offered as a starting point and is not derived from any cited control. At expiry, the risk must be reassessed. Acceptance does not automatically renew.

The IT Manager maintains a register of accepted risks. The Director of Practice Operations reviews the register on a cycle set by Aldergrove Legal; quarterly is offered as a starting point and is not derived from any cited control. Risks that have passed their acceptance expiry without reassessment are a material control failure and must be escalated to the Managing Partner.

16. Exceptions

A request to depart from a requirement of this policy must be submitted to the IT Manager in writing, with a description of the proposed exception, the business reason, the duration and the compensating controls that will apply in place of the standard requirement.

The IT Manager assesses the request and makes a recommendation. The Director of Practice Operations reviews the recommendation. The Managing Partner decides whether to grant the exception.

Exceptions are time-limited. The IT Manager records every exception, its conditions, its expiry date and the name of the person who requested it. The Director of Practice Operations reviews the exceptions register on a cycle set by Aldergrove Legal; quarterly is offered as a starting point and is not derived from any cited control.

An exception that has passed its expiry date without renewal or closure is a material control failure. The IT Manager must escalate it to the Director of Practice Operations immediately.

17. Policy Review and Metrics

The Director of Practice Operations reviews this policy annually and presents any proposed changes to the Managing Partner. The Managing Partner's endorsement of the reviewed policy is recorded in the policy review record.

The annual review must consider: changes to the firm's systems or services, changes to the threat environment, the outcome of security incidents in the preceding period, the results of backup and recovery tests, and the state of the exceptions and risk acceptance registers.

The following metrics must be reported to the Director of Practice Operations on a cycle set by Aldergrove Legal; quarterly is offered as a starting point and is not derived from any cited control:

- Percentage of critical assets with assigned control owners.
- Percentage of high-risk findings remediated within the target window.
- Percentage of required access reviews completed on time.
- Number of exceptions past their expiry date.
- Number of material control failures and the status of corrective actions.

The IT Manager is responsible for producing these metrics. The Director of Practice Operations is responsible for acting on them.

18. Related Documents

This policy is supported by the following instruments. Where a conflict appears between this policy and a sibling document, the Director of Practice Operations resolves it.

- Access Control Policy
- Password and Authentication Standard
- Data Classification and Handling Standard
- System Integrity and Malware Defence Standard
- Patch Management Procedure
- Security Incident Response Procedure
- Privacy and Personal Information Policy
- Privacy Breach Response Procedure
- Records Retention and Disposal Policy
- Third-Party Risk Management Policy

- Third-Party AI Review Procedure
- Business Continuity Policy
- AI Acceptable Use Policy
- AI Risk Management Standard
- AI Governance and Accountability Policy
- AI Incident Response Procedure

SPECIMEN

19. Document Control

Policy title: Information Security Policy

Policy owner: Director of Practice Operations

Review authority: Managing Partner

Review frequency: Annual

Jurisdiction: Ontario, Canada

This policy takes effect on the date it is endorsed by the Managing Partner and supersedes any prior information security policy issued by Aldergrove Legal.

Owner review items

The drafting process identified the following in the supplied answers. Resolve each before customer release.

Type	Detail	Where
gap	Aldergrove Legal's physical office locations beyond 'Toronto office' are not specified. If the firm operates from more than one location, the asset inventory and storage restrictions in Sections 5 and 9 must be reviewed to ensure they cover all sites.	Sections 5 and 9
gap	Recovery time objectives and recovery point objectives for critical systems are not supplied. Section 12 mandates that these exist and are tested but cannot state the values. Aldergrove Legal must set and record them before this policy is considered complete.	Section 12
gap	The Business Continuity Policy is listed as an existing document but its contents are not available. Section 12 of this policy defers to it for continuity obligations. Aldergrove Legal must confirm that the Business Continuity Policy covers the firm's after-hours and court-deadline scenarios described in the customer answers.	Section 12
gap	The Records Retention and Disposal Policy is listed as an existing document but its contents are not available. Section 9 defers retention periods to it and Section 8 defers log retention to it. Aldergrove Legal must confirm that the Records Retention and Disposal Policy covers both matter file retention and security log retention.	Sections 8 and 9
gap	The applicable Ontario privacy legislation and any sector-specific regulatory obligations (for example, Law Society of Ontario rules on client confidentiality and data handling) are not enumerated in the supplied material. This policy refers to 'applicable Ontario privacy law' without naming statutes. Aldergrove Legal's legal reviewers should confirm which instruments apply — candidates include Ontario's privacy legislation and Law Society of Ontario professional obligations — and ensure that the Privacy and Personal Information Policy and this policy together address them. This is a candidate	Section 8

gap	The discovery review platform is listed as a critical system but no detail is supplied about whether it is hosted on-premises, in a cloud environment, or by a third-party vendor. If it is third-party hosted, the Third-Party Risk Management Policy obligations apply and the asset inventory must reflect the hosting arrangement.	Section 5
vague	The customer answers describe the managed service provider as providing after-hours support but do not specify the provider's name, the scope of their access, or the contractual terms governing their security obligations. Section 13 mandates that a written agreement is in place. Aldergrove Legal must confirm this agreement exists and covers the security requirements stated in this policy.	Section 13
gap	No framework control identifiers are available in the supplied material. All requirements in this policy are stated as organisational mandates without citation to external control identifiers. If Aldergrove Legal later adopts a named framework, the policy should be updated to align terminology and cross-references.	All sections

Information the organization must supply

These values were not available from the intake and are required before this document can operate:

- Recovery time objectives (RTO) and recovery point objectives (RPO) for each critical system (document management system, trust accounting system, Microsoft 365). These must be recorded in a supporting standard or the Business Continuity Policy before this policy is considered complete.
- The review cycle for the asset inventory (Section 5). Annual is offered as a starting point.
- The review cycle for access rights (Section 6). Quarterly is offered as a starting point.
- The target remediation window for critical vulnerabilities (Section 7). 14 days is offered as a starting point.
- The monitoring review cycle for critical systems (Section 8). Weekly is offered as a starting point.
- The log retention period, to be recorded in the Records Retention and Disposal Policy and referenced from Section 8.
- The maximum risk acceptance period (Section 15). 12 months is offered as a starting point.
- The review cycle for the risk acceptance register (Section 15). Quarterly is offered as a starting point.
- The review cycle for the exceptions register (Section 16). Quarterly is offered as a starting point.

- The metrics reporting cycle (Section 17). Quarterly is offered as a starting point.
- The backup testing cycle (Section 12). Quarterly is offered as a starting point.
- The security awareness training refresh cycle (Section 14). Annual is offered as a starting point.
- The third-party access review cycle (Section 13). Annual is offered as a starting point.
- Confirmation that the Business Continuity Policy covers after-hours and court-deadline continuity scenarios.
- Confirmation that the Records Retention and Disposal Policy covers both matter file retention and security log retention.
- Confirmation that a written agreement with the managed service provider is in place and covers the security obligations stated in Section 13.
- Confirmation of the hosting arrangement for the discovery review platform, and whether it is subject to the Third-Party Risk Management Policy.
- Legal review to confirm which Ontario privacy legislation and Law Society of Ontario obligations apply, and that the Privacy and Personal Information Policy together with this policy address them.
- The effective date of this policy, to be inserted in Section 19 upon endorsement by the Managing Partner.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.