

## Serve Legal External Information Security Policy v1.0

Effective Date: 21 September 2026

Next Review: September 2027

**PUBLIC – Unclassified**

**Serve Legal**

# External Information Security Policy

## Document Control

|                                |                                 |
|--------------------------------|---------------------------------|
| <b>OWNER</b>                   | Operations Manager / ISMS Owner |
| <b>APPROVER</b>                | Senior Management Team          |
| <b>CLASSIFICATION</b>          | Public                          |
| <b>DATE OF ISSUE</b>           | 21 September 2026               |
| <b>ISSUE</b>                   | v1.0                            |
| <b>REASON FOR ISSUE/UPDATE</b> | First issue                     |
| <b>NEXT REVIEW</b>             | September 2027                  |
| <b>DISTRIBUTION</b>            | Unclassified                    |

## Version History

| <b>VERSION</b> | <b>AUTHOR</b>  | <b>SUMMARY OF CHANGES</b> | <b>DATE</b>       |
|----------------|----------------|---------------------------|-------------------|
| 1.0            | Alex Blackwell | First issue               | 21 September 2026 |

**Document Release:** This document is intended for external publication and may be shared with clients, suppliers, prospective clients and other interested parties. It provides a high-level description of Serve Legal information security expectations and does not disclose confidential security configurations or operational security details.

## Objective

Serve Legal is committed to protecting the confidentiality, integrity and availability of information entrusted to us by our clients, employees, auditors, suppliers and other interested parties. This policy provides a public overview of the information security principles applied by Serve Legal and the minimum-security expectations that apply to suppliers and third parties who access, process, store, transmit or otherwise support Serve Legal information or services.

## About Serve Legal and Scope

Serve Legal provides auditing, mystery shopping, compliance monitoring, and related services. Our activities are supported by technology, cloud services, suppliers, and a predominantly remote-working operating model. Information security is managed through an Information Security Management System aligned to ISO/IEC 27001:2022.

This policy applies to external organisations and individuals where their services, access or activities may affect Serve Legal information, systems, clients, personnel or service delivery. Security requirements are applied proportionately according to the nature and risk of the relationship.

## Information Security Principles

Serve Legal applies a risk-based approach to information security. Security decisions consider the confidentiality, integrity and availability of relevant information and services, together with applicable legal, regulatory and contractual requirements.

- Confidentiality - information is available only to authorised persons and organisations.
- Integrity - information is protected from unauthorised or inappropriate alteration.
- Availability - information and services are available when required for authorised business purposes.

- Risk management - information security risks are identified, assessed, treated and reviewed.
- Continual improvement - incidents, audits, supplier reviews, risk reviews and other assurance activities are used to improve the ISMS.

## **Governance and Accountability**

Serve Legal maintains defined information security responsibilities and governance arrangements. Information security performance, risks, objectives, incidents, supplier assurance and improvement actions are reviewed through appropriate management and assurance processes. Significant changes to services, suppliers, technologies or information processing are considered through risk assessment and governance activities.

## **Information Handling and Access**

Serve Legal information is handled according to its sensitivity and business purpose. Access is granted on a role-based and need-to-know basis and should be limited to the minimum access required for the authorised activity. Approved authentication controls, including multi-factor authentication where appropriate, are used to protect access to systems and information.

Suppliers and third parties must only access Serve Legal information or systems where authorised and must not use, copy, disclose or retain information for purposes outside the agreed service or legal obligation.

## **Acceptable Use, Devices and Remote Working**

Serve Legal requires information and systems to be used securely and for authorised purposes. Personnel and authorised third parties are expected to use approved systems, protect credentials, maintain device security, avoid unauthorised software or storage methods and protect information when working remotely or in shared locations.

Serve Legal uses approved cloud and electronic transfer methods for normal business activity. Unauthorised removable storage media must not be used with Serve Legal-managed systems. Any exceptional use must be specifically authorised and appropriately protected.

## **Data Protection, Retention and Secure Disposal**

Personal and confidential information must be processed in accordance with applicable data protection, legal and contractual requirements. Information should only be retained for as long as required by the agreed service, contractual requirements, legal or regulatory obligations, or other legitimate and documented business needs.

At the end of an agreed retention period or supplier relationship, Serve Legal information must be securely returned, deleted, anonymised or destroyed as required. Evidence of deletion or destruction may be requested where appropriate.

## **Cloud Services and Technology**

Cloud, software and technology services supporting Serve Legal are subject to proportionate security and supplier assurance. Security considerations may include access control, authentication, encryption, logging, monitoring, backup and recovery, data location, sub-processors, service continuity, international transfers and exit arrangements.

Where technology includes artificial intelligence or automation, associated privacy, confidentiality, data use, accuracy, human oversight and supplier risks must be considered before or during use as appropriate.

## **Business Continuity and Resilience**

Serve Legal maintains business continuity and incident response arrangements to support the continued delivery and recovery of important services. Third parties supporting critical services are expected to maintain proportionate continuity and recovery arrangements and to cooperate with Serve Legal during disruptions that affect our services or information.

## Information Security Incidents

Suppliers and third parties must promptly notify their Serve Legal contact of any actual or suspected information security incident that may affect Serve Legal information, systems, service delivery, legal obligations or clients. This includes loss, unauthorised disclosure, misuse, compromise, cyber incidents, material service disruption or suspected personal data breaches.

Third parties are expected to support investigation, containment, recovery, evidence preservation and corrective actions where an incident involves their service or activities. Any contractual or regulatory notification timescales remain applicable.

## Supplier and Third-Party Security Requirements

Serve Legal applies proportionate supplier assurance based on the service provided, the information and systems involved, the supplier access and the potential impact on confidentiality, integrity and availability. Depending on risk, suppliers may be asked to provide questionnaires, certifications, audit reports, trust-centre information, contractual documentation, privacy information or other appropriate assurance evidence.

Where relevant to the service, suppliers and third parties are expected to:

- Maintain appropriate information security governance, policies and responsibilities.
- Protect Serve Legal information against unauthorised access, use, alteration, loss or disclosure.
- Ensure access is authorised, appropriately authenticated, limited to business need and removed when no longer required.
- Maintain confidentiality obligations for personnel and subcontractors with access to Serve Legal information.
- Provide appropriate security awareness and role-specific training to relevant personnel.
- Maintain proportionate physical and environmental protections for locations used to process or store Serve Legal information.
- Maintain appropriate malware protection, vulnerability management, patching, security testing, logging and monitoring where relevant to the service.
- Maintain business continuity, backup, recovery and resilience arrangements appropriate to the service.
- Notify Serve Legal of material security incidents and cooperate with investigation and remediation.
- Notify Serve Legal of material changes to the service, hosting, security arrangements or sub-processors where contractually required or where the change may materially affect Serve Legal risk.
- Securely return, transfer, delete or destroy Serve Legal information and revoke access when the service or relationship ends.
- Comply with information security obligations contained in applicable contracts, service terms, confidentiality agreements, data processing agreements and service-level agreements.

## Supplier Assurance and Review

Serve Legal may assess and periodically review suppliers according to risk and material changes in the relationship. Reviews may consider service performance, incidents, independent assurance, certifications, contractual compliance, access rights, data protection, business continuity, sub-processors, hosting arrangements and outstanding security actions. Suppliers are expected to provide reasonable cooperation and evidence where required by the agreed relationship.

## Compliance and Exceptions

Suppliers and third parties must comply with the security requirements applicable to their relationship with Serve Legal. Where a requirement cannot be met, the supplier should notify its Serve Legal contact so that the risk, alternative controls and any required approval can be assessed before the exception is accepted.

A breach of agreed security requirements may result in corrective action, restriction or removal of access, reassessment of the supplier relationship, contractual remedies or other action appropriate to the risk and agreement.

## **Contact**

Questions about this policy, supplier security requirements or information security concerns should be raised with the relevant Serve Legal business contact, who will coordinate with the ISMS Owner or other appropriate role where required.