LONCAR LYON JENKINS

Information Security Policy

Loncar Lyon Jenkins maintains administrative, technical, and operational safeguards designed to protect firm systems, website information, consultation submissions, client communications, and law-firm records.

Document owner	Loncar Lyon Jenkins Administration
Approval authority	Firm management
Version	1.0
Effective date	August 28, 2026
Review cycle	At least annually and after a material legal, security, operational, or technology change
Classification	Public trust and compliance information

1. Purpose and scope

This policy describes how the firm protects the confidentiality, integrity, and availability of information used to operate the law firm and website. It applies to firm personnel, contractors, approved vendors, and systems used for intake, communications, marketing, case support, records management, payment, analytics, and security operations.

This policy is not legal advice, does not create an attorney-client relationship, and does not change any engagement agreement, court order, privilege obligation, or professional responsibility requirement.

2. Security principles

- Limit access to the minimum information needed for an approved role or service.
- Protect attorney-client, prospective-client, medical, financial, and personal information according to its sensitivity.
- Use layered safeguards including authentication, encryption, monitoring, vendor review, backups, secure configuration, and incident response.
- Collect and retain only information needed for legal, operational, security, communication, compliance, or business purposes.
- Review security risks after material system, vendor, legal, or operational changes.

3. Information handling

Restricted information includes authentication credentials, security secrets, privileged legal communications, medical records, financial details, case materials, and sensitive identifying information. Confidential information includes intake submissions, client contact records, support communications, marketing preference records, internal procedures, and vendor records. Public information includes approved website content and public legal notices.

Restricted and confidential information must be handled through approved firm systems, shared only for authorized legal or business purposes, and protected from public posting, unapproved storage, or unnecessary disclosure.

4. Identity and access management

- Firm and vendor accounts should be individually assigned where practical.
- Administrative access is limited to approved personnel and reviewed when duties change.
- Strong passwords and multi-factor authentication are used where supported for administrative, email, hosting, analytics, payment, and security tools.
- Access is removed or changed when employment, contract status, vendor need, or business purpose ends.
- Credentials, API keys, and tokens are not placed in public pages, ordinary support replies, or source files intended for public distribution.

5. Website, intake, and communications security

The firm uses HTTPS for website traffic and reasonable safeguards for online forms, analytics, advertising tools, email, SMS, and telephone intake workflows. People should not submit urgent legal deadlines, emergency requests, passwords, payment card details, or highly sensitive documents through ordinary website forms unless specifically instructed by the firm.

6. Vendor and service-provider oversight

The firm uses third-party providers for hosting, email, analytics, advertising, forms, phone and SMS services, payment, document handling, backups, and security. Vendors are expected to process information only for authorized purposes and to use safeguards appropriate to their role.

7. Monitoring, backup, and incident response

The firm may monitor systems, logs, form activity, email security, authentication events, and website traffic to maintain service availability, investigate abuse, detect security issues, and protect firm rights and client interests. Backups and recovery processes are maintained for business continuity. Suspected security incidents are triaged, contained, investigated, and escalated as appropriate.

8. Exceptions and review

Exceptions require approval by firm management or an authorized system owner and may include compensating controls. This policy is reviewed at least annually and after material changes.