LONCAR LYON JENKINS

Access Controls Policy

This policy describes how Loncar Lyon Jenkins requests, approves, provisions, reviews, changes, and removes access to firm systems and information.

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 applies to firm employees, attorneys, contractors, administrators, approved vendors, and technical service providers with access to law-firm systems, website administration, communications platforms, case-support systems, documents, backups, analytics, advertising tools, payment tools, and hosting infrastructure.

2. Access control principles

- Access is based on approved business or legal need.
- Permissions are limited to the least privilege appropriate for the role.
- Privileged administration, payment, hosting, email, and security access require additional care.
- Material activity should be attributable to an individual or approved technical account.
- Access is changed or removed promptly when duties, affiliation, contract status, or business need changes.

3. Request and approval

Access requests should identify the person or service, requested role, system scope, business purpose, approver, and any expected end date. Administrative or vendor access requires approval from firm management or the relevant system owner.

4. Provisioning

- Accounts are assigned to approved roles and system scopes.
- Sensitive tools remain unavailable until expressly configured and authorized.
- Initial and reset credentials are delivered through approved secure flows.
- Shared credentials are avoided where a system supports individual accounts.

5. Authentication and sessions

Passwords should be stored only through approved hashing or managed identity systems. Multi-factor authentication is required or strongly preferred for administrative, email, hosting, domain, security, payment, and other high-impact services where available. Sessions may be revoked when compromise or misuse is suspected.

6. Review, transfer, and termination

When a person changes responsibilities or leaves the firm, access is reviewed and reduced or removed. Vendor access is reviewed when a project ends, a service changes, or a security concern arises. Tokens, OAuth grants, API credentials, passwords, and sessions are rotated or revoked when appropriate.

7. Client and case information

Access to client, prospective-client, medical, financial, and case-related information is limited to personnel and approved providers who need it for intake, representation, operations, support, compliance, or other authorized purposes. This policy does not override attorney-client privilege, confidentiality duties, court orders, retention obligations, or engagement agreements.

8. Logging and accountability

Where supported by the system, administrative and sensitive access events are logged or reviewable. Logs may be used to investigate errors, suspected misuse, fraud, spam, unauthorized access, or security events.