LeaseLogic — Data & Security Policy

Last Updated: September 6, 2025
Owner/Operator: Four Leaf Clover Ventures ("LeaseLogic", "we", "us")
Security & Privacy Contact: legal@fourleafclover.io

1) Scope & Applicability

This Policy describes the technical and organizational measures LeaseLogic uses to protect information processed by our services ("Service"), including lease documents, related communications, account data, telemetry, and support artifacts. It applies to all environments, personnel, and subprocessors engaged to deliver the Service.

2) Governance, Roles & Accountability

- **Governance.** Security and privacy programs are overseen by senior leadership with defined accountability; policies reviewed at least annually.
- **Policies & Standards.** Written policies cover access control, data handling, cryptography, SDLC, vendor management, incident response, business continuity, and disaster recovery.
- **Training.** All personnel complete security and privacy training at onboarding and annually; developers receive secure-coding training.
- **Discipline & Enforcement.** Violations of this Policy may result in access revocation and disciplinary action.

3) Risk Management & Control Alignment

- **Risk Assessments.** Periodic (at least annually) and event-driven assessments inform controls and remedial actions.
- **Framework Alignment.** Controls align with recognized standards (e.g., ISO 27001 family, NIST CSF, SOC 2 control families). **This is an alignment statement, not a certification claim.**

4) Data Classification & Handling

- **Classes.** Public, Internal, Confidential, and Restricted (e.g., government IDs or banking details if users upload them).
- **Handling.** Confidential/Restricted data requires encryption in transit/at rest, least-privilege access, logging, and secure deletion.
- **Minimization.** We collect only what is necessary to operate the Service; users are encouraged to redact extraneous personal identifiers before upload.

5) Access Control & Identity Management

- **Least Privilege & RBAC.** Role-based access, granted on a need-to-know basis; quarterly access reviews.
- **Strong Auth.** MFA is required for production access; SSO/SCIM available for enterprise tenants (where applicable).
- **Privileged Access.** Time-bound elevation with approval and logging; break-glass procedures with after-action review.
- **Separation of Duties.** Conflicting roles separated to reduce fraud or error risk.

6) Cryptography & Key Management

- **In Transit.** TLS 1.2+ (prefer TLS 1.3) for service endpoints.
- **At Rest.** AES-256 (or cloud-provider equivalent) storage encryption.
- **Key Management.** Cloud KMS for key generation, storage, rotation; restricted key access; separate keys per environment.
- **Secrets.** Secrets stored in a managed secret vault; rotation on schedule and on exposure events.

7) Application Security & Secure SDLC

- **Design & Reviews.** Threat modeling for significant features; mandatory peer code review.
- **Scanning.** SAST/DAST, dependency and container image scanning; IaC and CI/CD pipeline hardening.
- **Supply Chain.** Pinned dependencies where feasible; SBOM maintained for core components.
- **Change Management.** Changes tracked, reviewed, tested, and approved before release; rollbacks available.
- **OWASP Alignment.** Controls map to OWASP Top 10/ASVS categories.

8) Infrastructure & Network Security

- **Isolation.** Separate production/non-production environments; least-privilege security groups; network segmentation.
- **Edge Protections.** WAF, rate limiting, bot/abuse controls; DDoS protections through cloud provider.
- **Endpoint Security.** EDR/antimalware on managed hosts; disk encryption; automatic patching policies.
- **Backups & Storage.** Encrypted backups, integrity checks, and restricted restore permissions.

9) Logging, Monitoring & Detection

- **Centralization.** System, application, and security logs centralized and time-synchronized.

- **Retention.** Security-relevant logs retained for a commercially reasonable period consistent with law and business needs.
- **Detection.** Alerts for auth anomalies, data exfil signals, privilege changes, and infra drift; alert response playbooks maintained.

10) Vulnerability & Patch Management

- **Scanning Cadence.** Regular automated scans plus ad-hoc scans for zero-days.
- **Remediation SLAs (targets).** Critical: 7 days; High: 15 days; Medium: 30 days; Low: 90 days. Documented exceptions require risk acceptance by leadership.
- **Verification.** Post-patch validation and rescans; tracking to closure.

11) Business Continuity & Disaster Recovery

- **Objectives.** Default targets: RPO ≤ 24 hours; RTO ≤ 24 hours for critical services (tenant-specific targets may be set by agreement).
- **Testing.** DR procedures tested at least annually; lessons learned tracked to completion.
- **Backup Strategy.** Daily incremental + periodic full backups; encryption at rest; restore tests conducted regularly.

12) Incident Response & Breach Notification

- **Process.** Detect → Triage → Contain → Eradicate → Recover → Post-Incident Review with root cause and corrective actions.
- **Records.** Incidents documented with timeline, scope, affected systems/data, and decisions.
- **Notification.** We notify affected users and regulators **as required by applicable law** and contractual commitments.
    - **Canada (PIPEDA).** Report breaches of security safeguards that pose a real risk of significant harm; notify affected individuals and keep breach records.
    - **Québec (Law 25).** Report "confidentiality incidents" to the CAI where risk of serious injury; maintain a register of incidents.
    - **United States.** State breach-notification laws apply; timelines and thresholds vary by state.
- **Communication.** Coordinated, accurate, and proportional to risk; we do not disclose exploit details that increase harm before mitigation.

13) Subprocessors & Third-Party Risk

- **Diligence.** Vendors evaluated for security/privacy posture proportional to data sensitivity and service criticality.
- **Contracts.** Written data-processing terms required; confidentiality, breach notice, and deletion/return obligations included.

- **Inventory.** A current list of subprocessors is available on request; material changes communicated per agreement.
- **Monitoring.** Periodic reassessments; corrective actions tracked.

14) Data Residency, Transfers & Government Requests

- **Regions.** Data may be processed in Canada and the United States (and other regions where providers operate) with technical/contractual safeguards appropriate to sensitivity.
- **Cross-Border.** Transfers are supported by contractual safeguards and cloud security controls.
- **Access Requests.** Government or law-enforcement requests are reviewed for legal sufficiency; we seek to narrow scope and notify customers where legally permitted.

15) Data Retention & Deletion

- **Defaults.** Personal data retained only as long as needed to provide the Service and meet legal obligations.
- **User Deletion.** Upon verified request, we delete personal data from active systems and schedule removal from backups on a rolling basis.
- **Records.** Certain records may be retained as required by law, dispute resolution, or to enforce agreements.

16) AI/ML-Specific Controls (Lease & Document AI)

- **Dataset Governance.** Input documents processed in secured compute; dataset lineage and access logs maintained.
- **PII Minimization.** Automated and manual measures to reduce or redact unnecessary personal identifiers used for model evaluation or improvement.
- **Training/Evaluation Uses.** We may use de-identified and/or aggregated data to improve models. **Users can opt out** of training/evaluation use of their uploaded content by emailing legal@fourleafclover.io. Opt-out does not affect processing necessary to provide the Service (e.g., inference).
- **Safety & Quality.** Pre-release evaluations, red-teaming, and regression testing for safety, bias, and quality; content filters and abuse monitoring in production.

17) Customer Controls & Secure Use Guidance

- **Tenant Controls.** SSO/MFA (where available), role assignments, audit exports, retention settings, and training opt-out are available to admins (plan-dependent).
- **Secure Use.** Redact unnecessary identifiers; verify outputs before acting; restrict who can upload or export data; rotate API keys; review audit logs periodically.

18) Confidentiality & NDAs

All employees and contractors are bound by confidentiality obligations. Additional NDAs and Data Processing Addenda (DPAs/Model Clauses equivalents where applicable) are available under appropriate agreements.

19) Responsible Disclosure (Vulnerability Reporting)

We welcome good-faith security reports. Email details to **legal@fourleafclover.io** with enough information to reproduce the issue. Do not access, modify, or exfiltrate data beyond what is strictly necessary to demonstrate impact. We will investigate and acknowledge receipt; safe-harbor principles applied to good-faith research.

20) Changes to this Policy

We may update this Policy to reflect legal, technical, or business changes. The **“Last Updated”** date indicates the latest revision. Material changes will be communicated via the Service or other reasonable notice. Continued use after updates indicates acceptance.

21) Contact

Security, privacy, DSRs, DPAs, subprocessor list, incident questions, or enterprise questionnaires: **legal@fourleafclover.io**