TeleSeal Information Security Policy

Version: 1.0
Effective Date: 2025-08-20
Review Cycle: Annual
Owner: Chief Information Security Officer (CISO)

---

1. Purpose

This policy defines how TeleSeal identifies, protects, detects, responds to, and recovers from information security risks in support of our Remote Online Notarization (RON) service. It is designed to meet Arizona RON requirements (A.R.S. Title 2, Ch. 12, Art. 13) and align with industry best practices (SOC 2 Trust Services Criteria) as TeleSeal grows.

2. Scope

This policy applies to all TeleSeal employees, contractors, vendors, and systems that process, store, or transmit sensitive data, including but not limited to:

- Notary journals & audit trails
- Audio-video session recordings
- User identity data (via Authenticate.com)
- PDF documents and electronic seals (X.509 certificates)
- Infrastructure services (AWS, Twilio, Email & Communication Systems)

3. Roles & Responsibilities

Role	Responsibility
CISO	Policy ownership, risk assessments, incident response
Developers	Secure coding, code reviews, vulnerability remediation
Vendors (Authenticate, Twilio, AWS)	Adhere to security requirements in SLA/contracts

4. Policy Statements

4.1 Risk Assessment & Management

- Conduct formal risk assessments **annually** and upon material change.
- Identify threats, vulnerabilities, business impacts, and mitigation strategies.
- Maintain a Risk Register, reviewed by the CISO and executive team.

4.2 Asset Management

- Maintain an **inventory** of all cloud services, data stores, and critical code repositories.
- Classify data (Confidential, Internal, Public) and apply handling rules (e.g., encryption).

4.3 Access Control

- Apply **least privilege**: users and services receive only necessary access.
- Enforce **Multi-Factor Authentication** (MFA) for all privileged accounts.
- Review access rights at least **annually**;

4.4 Cryptography

- Protect data **in transit** using TLS 1.2+ for all web, API, and video connections (Twilio).
- Protect data **at rest** using AES-256 (AWS S3 server-side encryption + KMS).
- Require use of customer-provided X.509 certificates for PDF sealing; private keys must remain client-side.

4.5 Physical & Environmental Security

- All production servers reside in **SOC 2–certified** data centers.
- Sensitive data is not stored on personal or local devices.

4.6 Operations Security

- **Change Management**: all changes must follow documented procedures, include review & rollback plans.
- **Patch Management**: apply security patches within 30 days of release; critical patches within 7 days.
- **Malware Protection**: endpoint and server anti-malware tools deployed and updated regularly.
- **Logging & Monitoring**: collect and retain logs (authentication, system, application) for at least 1 year; integrate with SIEM for alerts. Note that notary journal logs are retained for longer in accordance with state guidelines.

4.7 Communications Security

- Secure internal communications (email, chat) with TLS.
- Classify and encrypt sensitive attachments or data exchanges.
- Prohibit use of unapproved communication channels for RON sessions or data transfers.

4.8 System Development & Maintenance

- Follow secure coding practices and perform **code reviews**.
- Use automated dependency scanning and vulnerability alerts.
- Enforce separation of development, test, and production environments.

4.9 Supplier & Third-Party Security

- Rely on vendors with strong security posture (Authenticate, Twilio, AWS).
- Re-evaluate vendor risk **annually** or upon service changes.

4.10 Incident Management

- Maintain an **Incident Response Plan**: detection, containment, eradication, recovery, and post-mortem.
- Notify impacted stakeholders and regulators (including Arizona SOS) within timeline requirements.

4.11 Business Continuity & Disaster Recovery

- Replicate critical systems across availability zones.
- Document recovery procedures; test at least annually.

4.12 Compliance & Audit

- Maintain compliance with Arizona RON regulations.
- Work toward SOC 2 compliance as TeleSeal grows, starting with Type I readiness.

5. Policy Exceptions

- Any exception must be **documented**, **approved by the CISO** with a clear time limit.

6. Enforcement & Sanctions

- Violations may result in access revocation, contract termination, or other remedies.

7. Review & Updates

- This policy will be **reviewed annually** or upon significant organizational, technical, or regulatory changes.

End of TeleSeal Information Security Policy