TeleSeal Data Classification & Encryption Policy

Version: 1.0
Effective Date: 2025-07-27
Review Cycle: Annual
Owner: Chief Information Security Officer (CISO)

---

1. Purpose

To establish a consistent framework for classifying TeleSeal data and enforcing encryption controls, both in transit and at rest, to meet Arizona RON requirements (A.R.S. Title 2, Ch. 12, Art. 13).

2. Scope

Applies to all data created, received, stored, or transmitted by TeleSeal, including:
- Notary journals & audit trails
- Audio/video recordings of RON sessions
- User identity information (Authenticate.com proofs, KBA results)
- PDF documents and X.509 certificates
- Infrastructure and operational logs

3. Roles & Responsibilities

Role	Responsibility
CISO	Policy ownership; approval of classification schemes; exception approvals
IT Operations	Implement key management, encryption in AWS, Twilio, databases
Developers	Tag data flows; incorporate encryption libraries; secure coding
All Staff & Contractors	Label data appropriately; follow handling guidelines

---

4. Data Classification

TeleSeal classifies data into four categories. All users and systems must handle data according to its classification label.

Classification	Description	Examples	Handling Requirements
Public	Information intended for wide distribution or public view	Marketing copy; documentation; blog posts	• No encryption required • Can be published to public websites
Internal	Non-sensitive operational data used within TeleSeal	Internal policies; procedure guides; generic status dashboards	• Encrypt in transit (TLS 1.2+) • Optional encryption at rest • Access restricted to employees
Confidential	Personally identifiable information and proprietary business data	User identity proofs; audit logs; session metadata	• Encrypt in transit (TLS 1.2+) • Encrypt at rest (AES-256) • Access via RBAC and MFA only
Restricted	Highly sensitive or regulated data	A/V recordings; notary journals; user-provided X.509 private keys	• Encrypt in transit (TLS 1.2+) • Encrypt at rest (AES-256 with HSM or KMS) • Strict access controls; Annual review

---

5. Encryption Controls

5.1 Encryption In Transit

- **Protocol:** TLS 1.2 or higher for all HTTP(s), API calls, WebSocket, and Twilio Video streams.
- **Certificate Management:**
  - Use certificates issued by a trusted CA.
  - Rotate public certificates annually or upon key compromise.
- **Internal Services:**
  - Encrypt database connections (e.g., PostgreSQL with SSL).
  - Secure service-to-service communication with mTLS where supported.

5.2 Encryption At Rest

- **AWS S3 & Glacier:**
  - Server-Side Encryption with AWS KMS-managed keys (SSE-KMS, AES-256).
  - Enable Object Lock in Compliance mode for audit logs & A/V recordings (5-year retention).
- **Databases & Block Storage:**
  - Use AWS RDS encryption or disk-level encryption (EBS with AES-256).
- **Application Secrets & Keys:**
  - Store in AWS Secrets Manager or HashiCorp Vault.
  - Enforce automatic rotation (every 90 days) for API keys, DB credentials.

5.3 Customer-Provided X.509 Certificates

- **Private Key Handling:**
  - Private keys remain in client control; never transmitted or stored centrally.
  - PDF signing operations occur in-browser or on client's HSM.
- **Public Certificate Storage:**
  - Store only public key components metadata in a secure database (encrypted at rest).

5.4 Key Management & Rotation

- **Key Lifecycle:**
  - Generate keys with a minimum 2048-bit RSA or EC P-256 standard.
  - Rotate master KMS keys annually.
  - Deprecated keys are archived and never overwritten.
- **Access Controls:**
  - KMS key usage limited by IAM policies to designated service roles.
  - Audit all key usage via AWS CloudTrail logs.

5.5 Backup & Archive Encryption

- **Backups:**
  - All backups of databases, journals, and logs encrypted with AES-256.
  - Backup encryption keys managed by AWS KMS.
- **Archive:**
  - Glacier Deep Archive with SSE-KMS.
  - Retention policies enforce minimum retention periods; prevent early deletion.

---

6. Monitoring & Compliance

- **Automated Scans:** Regular checks for unencrypted S3 buckets or databases.
- **Audits:** Annual audits to verify data classification labeling and encryption adherence.
- **Reporting:** Encryption compliance reported to executive team.

---

7. Exceptions

- Any exceptions to encryption requirements must be:
  1. Documented with a business justification
  2. Approved by the CISO
  3. Accompanied by compensating controls (e.g., network segmentation, endpoint encryption)

---

8. Review & Updates

- Reviewed annually or upon significant technology, regulatory, or threat-landscape changes.
- Updates approved by the CISO and communicated to all stakeholders.

End of TeleSeal Data Classification & Encryption Policy