TeleSeal Remote Online Notarization (RON) Standard Operating Procedure (SOP)

Version: 1.0
Effective Date: 2025-07-27
Review Cycle: Annual
Owner: Head of Operations

---

1. Purpose

This SOP defines the step-by-step workflow for conducting Remote Online Notarizations (RON) in Arizona, fully compliant with A.R.S. Title 2, Chapter 12, Article 13. It covers session setup, identity proofing, document handling, signing, sealing, journaling, and recording.

2. Scope

Applies to all TeleSeal-commissioned notaries, internal staff coordinating RON sessions, and technical systems (Authenticate.com, Twilio, AWS, PDF/X.509 signing).

3. Roles & Responsibilities

Role	Responsibility
Notary	Conduct RON session per this SOP; sign & seal
Session Host	Schedule session; prepare documents; monitor AV
Tech Support	Ensure platform availability & troubleshoot
Compliance	Audit recordings, journals, and adherence

---

4. Pre-Session Preparation

1. **Session Scheduling**
   - Client or staff books via `TeleSeal` portal.
   - Confirm client email & appointment time; send "Join Session" link.
2. **Document Intake & Validation**
   - Client uploads PDF(s) to secure portal.
   - Verify PDF format, ensure fillable fields for signature/seal.
   - Store upload metadata in confidential database.
3. **Notary Onboarding Verification**
   - Confirm notary's commission is valid in Arizona.
   - Ensure notary has Teleseal-provisioned hardware token for X.509 in-browser signing.

---

5. Session Initiation

1. **Authenticate User & Notary**

- Client clicks "Join Session" → Twilio Video room launches.
- Notary joins; both parties authenticate to platform with MFA.

2. **Identity Proofing (Authenticate.com)**
   - **Credential Analysis:** Client uploads government ID images.
   - **Liveness Check:** Face match plus anti-spoofing.
   - If identity proof fails:
     - Offer **Knowledge-Based Questions (KBA)** fallback (5-question quiz).
     - If KBA fails, offer **Credible Witness** (per A.R.S. § 2-12-1305).
3. **Session Record Start**
   - Automatically begin A/V recording (encrypted Twilio HLS).
   - Generate unique session ID; display on screen for audit.

---

6. Document & Signing Workflow

1. **Document Control**
   - Load PDF in in-browser viewer.
   - Restrict client navigation to current page; disabled print/download.
2. **Signing Events Tracking**
   - Capture "click" events when client places signature or initials.
   - Log timestamps, page numbers, field names in the electronic journal.
3. **Notary Certificate & Seal**
   - Notary completes statutory text via template (R2-12-1307).
   - Platform inserts certificate block at designated location.
   - Notary applies digital seal using user-provided X.509 certificate:
     - Private key operation occurs client-side (in-browser HSM or token).
     - Public certificate metadata stored with document.

---

7. Journaling & Recording

1. **Electronic Journal Entry**
   - For each act (identity proof, signing event, seal application), record:
     - Date/time (UTC)
     - Session ID & participant IDs
     - IP addresses, device info
   - Journal stored in tamper-evident AWS RDS (AES-256 + Object Lock).
2. **Audio-Video Recording**
   - Store raw and segmented recordings in AWS S3 (SSE-KMS).

- After 30 days move to Glacier Deep Archive (Immutable lock for 5 years).

---

8. Session Closure

1. **Client Confirmation**
   - Notary asks client to review final PDF.
   - Client verbally confirms acceptance; Notary logs confirmation.
2. **Stop Recording & Export**
   - Terminate Twilio stream; consolidate A/V files.
   - Generate final signed PDF; store in S3 and make available for client download.
3. **Finalize Journal**
   - Complete outstanding journal entries.
   - Lock journal record; no further edits permitted.

---

9. Post-Session Actions

1. **Quality Review**
   - Compliance team reviews random sessions monthly for adherence.
   - Check identity proof logs, A/V clarity, journal completeness.
2. **Client Delivery & Notifications**
   - Email client: link to final PDF and journal summary.
   - Send notary copy of journal entry via secure internal portal.
3. **Retention & Disposal**
   - Maintain records per Data Retention Policy (minimum 5 years).
   - After retention period, purge in accordance with Object Lock and Disposal SOP.

---

10. Exceptions & Escalations

- **Technical Failures:** If Twilio session fails, switch to backup WebRTC channel; log incident.
- **ID Proof Failures:** Refer client to in-person notarization or credible witness process.
- **Policy Deviations:** Notaries must escalate to Compliance immediately and document rationale.

---

11. References

- Arizona RON Rules: A.R.S. Title 2, Ch. 12, Art. 13
- TeleSeal Policies: Information Security, Access Control, Data Retention

---

End of RON SOP

TeleSeal Access Control & Multi-Factor Authentication (MFA) Policy

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

---

1. Purpose

This policy ensures that access to TeleSeal systems, data, and applications is appropriately restricted and protected by multi-factor authentication (MFA). The policy aligns with Arizona RON requirements and sets a path toward SOC 2 Trust Services Criteria compliance as TeleSeal grows.

2. Scope

This policy applies to:
- All TeleSeal accounts (human and service).
- All environments used to process or store sensitive data (production, staging, support).
- All privileged access and integrations.

3. Roles & Responsibilities

Role	Responsibility
CISO	Owns this policy, approves exceptions, performs reviews
Developers	Follow secure access practices, use MFA, report issues
Vendors	Comply with contractual access and MFA requirements

4. Policy Statements

4.1 Access Control Principles

- **Least Privilege:** Grant the least privilege required for each account.
- **Need-to-Know:** Access to sensitive data (notary journals, A/V recordings, certificates) is restricted to authorized roles only.
- **Separation of Duties:** Avoid shared or generic accounts.

4.2 Account Provisioning & Deprovisioning

- New accounts are created by the CISO based on role.
- Accounts are disabled within 1 business day of termination or role change.
- Service accounts are only used for automation, tied to a clear owner, and reviewed annually.

4.3 Authentication Requirements

- **Unique IDs:** Every user and service account must have a unique login—no shared or generic accounts.
- **Password Policy:**
  - Minimum length: 12 characters

  - Complexity: mix of uppercase, lowercase, numbers, symbols

- **Account Lockout:** After 5 failed login attempts, lock account for 15 minutes and alert Security Team.
- **MFA:** MFA is required on all accounts (see Section 5).

4.4 Authorization & Role-Based Access

- **RBAC Model:** Use predefined roles (e.g., Notary, Administrator, Developer).
- **Periodic Review:** Access is reviewed annually to confirm least-privilege.

4.5 Session Management

- **Session Timeout:**
  - Web portal sessions expire after 15 minutes of inactivity.
  - Administrative consoles expire after 5 minutes of inactivity.

4.6 Remote & Privileged Access

- **VPN / Jump Box:** All SSH or RDP access to internal systems must occur over company-managed VPN or bastion host.
- **Privileged Accounts:**
  - Privileged (admin/root) access tracked via dedicated console (e.g., AWS IAM roles, Azure PIM).
  - MFA mandatory before privilege elevation.

4.7 Logging & Monitoring

- Record all authentication attempts, access grants, and privilege escalations.
- Retain logs for a minimum of 1 year.
- Integrate with SIEM to detect and alert on suspicious access patterns.

---

5. Multi-Factor Authentication (MFA)

5.1 MFA Requirement

- **All human users** (employees, contractors, notaries) **must enroll in MFA**.
- **Administrative & privileged accounts** require **two distinct factors** (e.g., password + hardware token).
- **Customer portal users** (document signers) must complete MFA when accessing personal data or signing events.

5.2 Approved MFA Methods

- **Authenticator Apps** (e.g., Google Authenticator, Authy)
- **Hardware Tokens** (e.g., YubiKey, FIDO2 security keys) for privileged users
- **SMS or Voice OTP** only as a backup when no other factor is available (logged and monitored)

5.3 MFA Implementation

- Leverage an identity provider (e.g., AWS Cognito, Okta, Azure AD) to enforce MFA policies.
- Configure "step-up" authentication for sensitive actions (e.g., certificate import, journal access).
- Disable fallback methods if not strictly necessary; enforce app/hardware tokens for all employees.

5.4 Exception Handling & Risk Mitigation

- Temporary exceptions (e.g., lost token) require:
  1. Manager approval
  2. Business justification documented
  3. Implementation of compensating controls (e.g., IP restrictions, shortened session timeouts)
- Exceptions expire automatically within 24 hours unless renewed.

---

6. Policy Exceptions

- Any exception to this policy must be:
  1. Documented in the Exception Register
  2. Approved by the CIS

TeleSeal Electronic Journal & Audio/Video Handling SOP

Version: 1.0
Effective Date: 2025-07-27
Review Cycle: Annual
Owner: Head of Operations

---

1. Purpose

Define the procedures for creating, storing, securing, and retrieving the electronic journal and audio/video (A/V) recordings of Remote Online Notarization (RON) sessions, in compliance with Arizona RON rules (A.R.S. § 2-12-1308, § 2-12-1309) and TeleSeal policies.

2. Scope

Covers all RON sessions conducted via TeleSeal, including:
- Electronic journal entries
- Synchronous A/V recordings
- Secure storage, retention, and disposal

Applies to Notaries, Compliance Team, IT/DevOps, and any staff interacting with journal or A/V data.

3. Roles & Responsibilities

Role	Responsibility
Notary	Create accurate journal entries; start/stop recording per SOP
Session Host	Verify recording status; ensure journal fields are completed
Compliance Team	Audit journal & A/V integrity; review tamper-evidence controls
IT/DevOps	Configure recording pipelines; enforce encryption & retention policies
CISO	Maintain policies; review audit logs; oversee integrity controls

---

4. Journal Entry Procedure

1. **Session Initialization**
   - Upon client & Notary joining, system auto-generates a **Session ID**.
   - Journal record created with Session ID, Notary ID, timestamp.
2. **Logging Events**
   For each key action, automatically record:
   - **Identity Proofing**: method (Authenticate.com credential, KBA, witness), result, timestamp
   - **Document Load**: document name/ID, pages count, timestamp
   - **Signature Event**: actor (Notary or Signer), page/field, click coordinates, timestamp
   - **Seal Application**: Notary ID, certificate serial, timestamp
   - **Session End**: timestamp, duration
3. **Tamper-Evidence**
   - Each entry chained via cryptographic hash; alterations break the chain.

4. **Access Controls**
    - Read/write limited to service account and Compliance Team via RBAC & MFA.
    - Audit trail of any journal access or export.

---

5. A/V Recording Procedure

1. **Recording Start**
    - Automatically initiate Twilio Video recording at session start.
    - Record both audio and HD video streams; link to Session ID.
2. **Monitoring**
    - Session Host verifies live recording indicator before identity proof begins.
    - System alerts if recording fails or disconnects.
3. **Pause/Resume**
    - Allow brief pause only for technical issues; record pause/resume events in the journal.
4. **Recording Stop**
    - Automatically stop upon session end.
    - Consolidate media segments into a single encrypted container.

---

6. Storage & Retention

Asset Type	Storage Location	Retention Period	Post-30-Day Transition
Raw A/V Files	AWS S3 (SSE-KMS)	30 days	Transition to Glacier Deep Archive (Immutable)
Archived A/V	AWS Glacier Deep Archive	7 years	Locked until retention expires

- **Immutable Lock** prevents deletion or modification until retention expiry.
- **Backups**: Daily snapshot of RDS and S3 bucket; encrypted and stored in separate AWS region.

---

7. Retrieval & Access

1. **Compliance Audits**
    - Compliance Team requests retrieval via ticket.
    - IT/DevOps grants time-limited, read-only access via secure link.
2. **User Requests**
    - Client downloads signed PDF via portal; A/V and journal links not exposed directly.
    - For legal requests, provide exports under NDA.
3. **Logging**
    - All retrievals (export, view, download) logged with user ID, asset ID, and timestamp.

---

8. Security & Integrity

- **Encryption In Transit:** TLS 1.2+ for all S3 and database connections.
- **Encryption At Rest:** AES-256 for S3 and RDS; AWS KMS for key management.
- **Integrity Checks:** Scheduled Lambda verifies journal hash chain; alerts on discrepancies.
- **Access Reviews:** Annual review of journal/A/V access logs by Security Team.

---

9. Exception Handling

- If recording fails irrecoverably:
  - Notary logs the failure as a journal entry.
  - Client must reschedule or revert to in-person notarization.
- Emergency data access (e.g., legal subpoena):
  - Obtain CISO approval; document in Incident Log; provide minimal required data.

---

10. Review & Updates

- Reviewed annually or upon:
  - Changes to Arizona RON regulations
  - New AWS/Twilio feature releases impacting recording/storage
  - Audit findings or security incidents

End of TeleSeal Electronic Journal & Audio/Video Handling SOP

TeleSeal Identity Proofing Checklist

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

---

1. Purpose

This checklist establishes auditable procedures to ensure compliance with Arizona Remote Online Notarization (RON) identity proofing requirements. It aligns with industry standards (e.g., NIST SP 800-63-3 IAL2/AAL2) and provides a structured approach to protect notarial integrity.

2. Scope

This checklist applies to:

- All commissioned Arizona notaries performing remote online notarizations.
- All RON platforms and providers approved for use by TeleSeal.
- All principals and credible witnesses participating in RON sessions.

3. Definitions

- **Credential Analysis:** Automated verification of a government-issued photo ID.
- **Dynamic KBA:** Knowledge-based authentication using time-limited questions.
- **MFA:** Multi-factor authentication combining at least two independent factors.
- **Personal Knowledge:** Notary's direct, long-standing familiarity with the principal.
- **Credible Witness:** A third party who identifies the principal under state rules.
- **Provider/Platform:** Approved RON technology used for identity proofing and notarization.

4. Compliance Overview (Arizona RON)

- Identity proofing must occur **before** the notarial act.
- MFA is required, typically credential analysis + dynamic KBA, unless personal knowledge or credible witness applies.
- Identity proofing outcomes must be recorded in the electronic journal and associated with the audiovisual recording.
- Only approved providers meeting Arizona RON and industry standards may be used.

5. Roles & Responsibilities

Role	Responsibility
Notaries	Perform and document identity proofing per this checklist.
CISO	Owns this checklist, approves exceptions, monitors compliance.
Vendors	Provide compliant credential analysis, KBA, and MFA tools; maintain audit trails.

---

6. Checklist Procedures

6.1 Pre-Session Readiness

- Confirm notary's physical location is within licensed state.

- Confirm RON platform/vendor is on approved list.
- Enable time sync, logging, and session recording.
- Verify principal's device supports audio/video and ID capture.

6.2 Primary Method: Credential Analysis + Dynamic KBA

Credential Analysis

- Collect front and back images of valid government ID.
- Validate security features, MRZ/barcode, tamper detection.
- Perform liveness/face match between ID and live capture.
- Confirm consistency of data (name, DOB, expiration).
- Record provider, reference ID, timestamp, pass/fail result.

Dynamic KBA

- Generate time-limited questions from reliable sources.
- Enforce minimum pass criteria and time limits.
- Allow limited attempts; rotate failed questions.
- Record provider, timestamp, pass/fail, attempt counts.

Decision Gate

- Proceed only if both credential analysis **and** KBA pass.
- If either fails, follow Failure Handling.

6.3 Alternative Methods (if permitted)

Personal Knowledge

- Notary documents basis/duration of familiarity.

Credible Witness

- One personally known witness or two unknowns per state law.
- Proof each witness with credential analysis + KBA (unless personally known).
- Record oath, name, address, contact in journal and recording.

6.4 Fraud and Risk Controls

- Confirm ID name matches session/document name.
- Screen for coercion; terminate if suspected.
- Require physical IDs, not copies/screenshots.
- Capture principal's location for certificate wording.
- Re-verify if session interrupted or rejoined.

6.5 Failure Handling

- **Credential Analysis Fail:** Allow one re-capture; escalate or reschedule.
- **KBA Fail:** Limited retry; otherwise require credible witness or reschedule.
- **Lockout:** After repeated failures, document reason and outcome.
- **Do not proceed** if identity cannot be reliably established.

6.6 Journaling & Recording

- Journal entry includes date/time, act type, doc description, principal's name, method used, provider(s), pass/fail, attempts, credible witness info, fees.
- Associate journal entry with audiovisual recording and provider transaction IDs.
- Retain journal, recordings, and metadata per state law.
- Protect PII with encryption and restricted access.

6.7 Platform & Vendor Requirements

- Automated credential analysis with liveness/face match.
- Dynamic KBA per state/industry standards (time limits, attempts, refresh).
- Auditable logs, timestamps, reference IDs.
- Compliance with SOC 2/ISO 27001 and NIST SP 800-63-3 alignment.
- Contracts cover uptime, incident response, data retention, breach notification.

6.8 Quality Assurance

- Periodically sample RON sessions for compliance.
- Review vendor pass/fail rates and anomalies.
- Remediate gaps with training and updated procedures.

6.9 Training & Access

- Notaries complete required state RON training and registration.
- Limit platform access to authorized notaries; review quarterly.

6.10 Change Management

- Monitor statutes, rules, SOS guidance; update checklist as needed.
- Communicate updates to all notaries and vendors.

---

7. Exceptions

- Exceptions must be documented in the Exception Register.
- Must be approved by the CISO.
- Must include compensating controls (e.g., additional verification, audit review).

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

TeleSeal Certificate Management Policy

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

---

1. Purpose

To establish consistent controls for the lifecycle of X.509 certificates used by TeleSeal—notary PDF-signing certificates and server TLS certificates—ensuring their secure issuance, storage, use, renewal, and revocation in support of Arizona RON requirements (A.R.S. § 2-12-1307).

2. Scope

This policy covers all digital certificates within TeleSeal:
- **Notary-provided X.509 certificates** used for document sealing
- **Platform TLS/HTTPS certificates** (e.g. `teleseal.app`, `telesealhq.com`)
- **Code-signing or API client certificates**, if any

It applies to all personnel and systems involved in certificate handling: Notaries, Developers, IT/DevOps, Security Team.

3. Roles & Responsibilities

Role	Responsibility
CISO	Policy owner; approves exceptions; oversees audits
Security Team	Define certificate standards; monitor compliance; conduct reviews
IT/DevOps	Issue, install, renew, and revoke server certificates; enforce HSM/KMS usage
Notaries (Users)	Provide valid X.509 certificates; safeguard private keys locally
Compliance Team	Verify certificate attributes against Arizona RON statute

4. Policy Statements

4.1 Certificate Standards

- **Key Algorithms:** RSA 2048+ or ECDSA P-256+
- **Signature Hash:** SHA-256 or stronger
- **Validity Period:**
  - **Notary certificates:** <= 3 years (per state commission term)
  - **TLS certificates:** <= 1 year (auto-renew via ACME)

4.2 Notary Certificate Onboarding

1. **Submission:** Notary uploads public certificate (`.pem` or `.crt`) via secure onboarding portal.
2. **Validation:**

- Confirm certificate subject DN includes Notary's legal name, commission number, and state of commission.

- Verify certificate chain to a trusted root or intermediate CA.

3. **Installation:**
   - Public certificate metadata imported into Teleseal.app PKI registry.

   - Private key **never** leaves the Notary's device/HSM.

4.3 Certificate Storage & Access

- **Public Certificates & Metadata:**
  - Stored encrypted in AWS RDS (AES-256 + KMS).

  - Access limited to signing microservice and Compliance Team via RBAC & MFA.

- **Private Keys:**
  - Held **exclusively** by Notaries in a secure store (hardware token, OS keychain, or HSM).

  - TeleSeal does **not** store or transmit private keys.

4.4 Certificate Use in PDF Sealing

- Signing operations performed in-browser or in dedicated microservice called by client, invoking the Notary's private key locally.

- The platform attaches the certificate's public portion and seal metadata into the PDF per A.R.S. § 2-12-1307 certificate block requirements.

4.5 Renewal & Expiry

- **Notary Certificates:**
  - Notaries must submit renewed certificates at least **30 days** before expiry or commission renewal.

  - Expired certificates are removed from the PKI registry and any in-flight signing requests will be blocked.

- **TLS Certificates:**
  - Automated via ACME (Let's Encrypt or internal CA); monitored by IT/DevOps with alerting on < 15 days to expiry.

4.6 Revocation & Compromise

- **Revocation Triggers:**
  - Notary commission suspension or termination

  - Certificate key compromise or device loss

- **Revocation Process:**
  1. Notary or Compliance submits revocation request.

  2. Security Team marks certificate revoked in PKI registry.

3. For TLS: Remove certificate from load balancers and issue replacement.

4. Notify affected parties (e.g., clients with pending transactions).

- **CRL/OCSP:**
  - Maintain and publish an internal CRL or OCSP responder for Notary certificates.

4.7 Audit & Monitoring

- **Logging:** All certificate issuance, renewal, and revocation events logged to SIEM with 1-year retention.

- **Periodic Review:**
  - Quarterly audit of PKI registry for expired or soon-to-expire certificates.

  - Annual compliance check against Arizona RON certificate requirements.

4.8 Incident Response

- In the event of a certificate breach (e.g., private key compromise):
  1. Activate Incident Response Plan.

  2. Revoke affected certificates immediately.

  3. Issue new certificates and enforce re-authentication for Notaries.

  4. Conduct root-cause analysis and update controls.

5. Exceptions

- Any exception (e.g., extended validity for legacy code-signing certs) must be:
  1. Documented with risk assessment

  2. Approved by the CISO

  3. Reviewed within 90 days

6. Enforcement & Sanctions

- Non-compliance may result in loss of signing privileges, disciplinary action, or commission suspension.

- Security Team performs enforcement audits semi-annually.

7. Review & Updates

- Reviewed annually or upon:
  - Changes in Arizona RON statute (§ 2-12-1307)

  - PKI security incidents

  - New industry best practices or cryptographic standards

End of TeleSeal Certificate Management Policy

TeleSeal Notary Public Onboarding Guide

Version: 1.0
Effective Date: 2025-07-27
Review Cycle: Annual
Owner: Head of Operations

---

1. Purpose

To provide a clear, step-by-step process for commissioning, training, and configuring new Arizona notaries on the TeleSeal Remote Online Notarization (RON) platform, ensuring full compliance with A.R.S. Title 2, Ch. 12, Art. 13 and TeleSeal policies.

2. Scope

Applies to all individuals newly commissioned (or re-commissioned) as Remote Online Notaries on the TeleSeal platform.

3. Roles & Responsibilities

Role	Responsibility
Head of Operations	Overall onboarding program management
Compliance Lead	Verify notary commission, review background and disclosures
IT/DevOps	Provision accounts, install software, configure MFA & certs
Training Coordinator	Deliver platform & RON workflow training
Notary Candidate	Complete prerequisites, training, and acknowledgement steps

---

4. Prerequisites

1. **Active Arizona Notary Commission**
   - Provide a certificate of commission issued by the Arizona Secretary of State.

2. **Background & Disciplinary Disclosure**
   - Complete background check and disclose any disciplinary actions.

3. **Hardware Requirements**
   - Windows 10+ or macOS latest
   - USB port (for hardware token if required)
   - Webcam (1080p recommended), headset or microphone

4. **Software Requirements**
   - Google Chrome or Microsoft Edge latest
   - VPN client (if remote network access is needed)

5. **Personal X.509 Certificate**
   - Obtain or generate a personal signing certificate (minimum RSA 2048).

- Store private key in a hardware token (YubiKey) or secure HSM/policy device.

---

5. Commission Verification

1. **Submit Commission Documents**
   - Upload commission certificate PDF in the "Notary Onboarding" portal.

2. **Compliance Review**
   - Compliance Lead verifies commission validity in the Arizona SOS database.

   - Notify candidate within 2 business days of approval or required corrections.

---

6. Account Provisioning

1. **Create Platform Account**
   - IT/DevOps creates a unique TeleSeal user ID and assigns the **"Notary"** role.

2. **Assign RBAC Permissions**
   - Grant access to RON dashboard, journal management, certificate import.

3. **Email & Notifications**
   - Provide credentials via secure email.

   - Instruct on email-based password reset and MFA enrollment link.

---

7. Technology Setup

7.1 Multi-Factor Authentication

- Candidate installs approved authenticator app (e.g., Authy) or configures hardware token.

- IT sends enrollment link; candidate completes MFA registration.

7.2 X.509 Certificate Installation

- Candidate imports public certificate into the browser-based HSM extension.

- Confirm private key is only accessible via hardware token; verify in demo signing flow.

7.3 Twilio Video & Platform Access

- Verify audio/video functionality in a supervised test session.

- Confirm ability to start/stop recording, share documents, and capture click events.

---

8. Training & Certification

1. **Platform Walkthrough (2 hours)**
   - UI navigation: dashboard, session scheduling, document upload.

- RON SOP demonstration: identity proofing, signing flow, sealing, journal.

2. **Arizona RON Regulation Briefing (1 hour)**
   - Key statute highlights: identity methods (A.R.S. § 2-12-1305), certificate format (§ 2-12-1307), retention (§ 2-12-1308).

3. **Mock Session & Assessment (1 hour)**
   - Conduct a complete simulated RON session with a peer/mentor.
   - Pass a checklist verifying all journal entries, A/V recording start/stop, and PDF sealing.

4. **Policy Acknowledgement**
   - Read and electronically sign: Information Security, Access Control, Data Retention, Incident Response policies.

---

9. Compliance & Agreements

- **Non-Disclosure Agreement (NDA)**
- **Platform Acceptable Use Policy**
- **Arizona RON Vendor Disclosure**
- **SOC 2 Code of Conduct**

All signed and stored in the compliance document repository.

---

10. Readiness Checklist

Item	Status	Date Completed
Commission Verified	☐	
Disclosure Form Reviewed	☐	
Platform Account & MFA Configured	☐	
X.509 Certificate Installed & Tested	☐	
Audio/Video Test Session Passed	☐	
Platform & Regulatory Training Completed	☐	
Policy Acknowledgements Signed	☐	
Mock Session Assessment Passed	☐	

---

11. Ongoing Requirements

- **Annual Re-Verification** of commission and background status.
- **Quarterly Refresher Training** on SOP changes or platform updates.
- **Continuous Compliance**: adhere to policy updates and complete any emergent training within 30 days.

---

12. Resources & Support

- **Notary Onboarding Portal:** `https://teleseal.app/onboarding`
- **Knowledge Base & How-Tos:** `https://telesealhq.com/docs`
- **Support Email:** `support@telesealhq.com`
- **Emergency IT Hotline:** (623) 244-7325

End of TeleSeal Notary Public Onboarding Guide

TeleSeal Vendor Management Policy

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

---

1. Purpose

To ensure that all third-party vendors supporting TeleSeal meet our security, privacy, and compliance requirements—including Arizona RON regulations (A.R.S. Title 2, Ch. 12, Art. 13).

2. Scope

Applies to all vendors, service providers, consultants, and contractors that:
- Process or store TeleSeal data (e.g., identity proofs, A/V streams, retention storage)
- Provide critical infrastructure or platform services (e.g., Authenticate.com, Twilio, AWS)
- Have logical or physical access to TeleSeal systems

3. Roles & Responsibilities

Role	Responsibility
CISO	Policy owner; approves vendor risk classification and exceptions
Vendor Management Team	Conduct vendor assessments; negotiate security requirements; manage ongoing reviews
Security Team	Evaluate vendor security posture; review SOC 2 reports and vulnerability scans
IT Operations	Integrate vendor services securely; enforce vendor access controls
Business Owner	Identify vendor business requirements; approve vendor selection

4. Policy Statements

4.1 Vendor Inventory & Classification

1. **Inventory:** Maintain a centralized register of all vendors, including:
   - Vendor name, service description, point of contact
   - Data domains accessed (e.g., identity data, recordings, certificates)
2. **Risk Classification:** Tier vendors into Low, Medium, or High risk based on:
   - Data sensitivity they handle (Public, Internal, Confidential, Restricted)
   - Criticality of service to TeleSeal operations
   - Regulatory or compliance impact

4.2 Due Diligence & Onboarding

- **High-Risk Vendors:**
  - Obtain and review latest SOC 2 Type II report, penetration test summary, and information-security questionnaire.

  - Conduct a security questionnaire covering data handling, encryption, incident response, and business continuity.

- **Medium-Risk Vendors:**
  - Review SOC 2 Type I report or equivalent security certification.
  - Confirm basic security posture (encryption in transit/at rest, MFA for access).

- **Low-Risk Vendors:**
  - Verify organizational details and non-disclosure agreement (NDA).

4.3 Ongoing Monitoring & Review

- **Annual Reviews:**
  - High-risk vendors: review updated SOC 2 reports and penetration test results
  - Medium-risk vendors: confirm continued certification or self-attestation

- **Quarterly Check-ins:**
  - Validate vendor performance against SLAs
  - Review security alerts or incidents involving the vendor

- **Access Reviews:**
  - Verify that vendor-issued accounts and credentials are current; revoke any unnecessary access

5. Offboarding & Termination

- **Access Revocation:** Immediately revoke all vendor access (credentials, API keys, network) upon termination.
- **Data Return/Destruction:** Ensure vendor returns or securely destroys all TeleSeal data.
- **Post-Engagement Review:** Document lessons learned and update Vendor Risk Register.

6. Exceptions

- Exceptions to this policy must be:
  1. Documented with rationale and compensating controls
  2. Reviewed and approved by the CISO
  3. Time-bound with scheduled re-evaluation

7. Enforcement & Sanctions

- Non-compliance may result in service suspension or termination.
- Repeat failures can trigger removal of vendor from approved list and tighter oversight for future engagements.

8. Review & Updates

- Reviewed annually, or upon:
  - Major regulatory changes (e.g., Arizona RON updates)

- Findings from audits or security incidents
- Introduction of new critical vendors or services

End of TeleSeal Vendor Management Policy

TeleSeal Change Management & Patch Management Policy

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

---

1. Purpose

To ensure all changes to TeleSeal systems, applications, and infrastructure are planned, tested, approved, and documented; and that security patches are applied promptly and consistently. This policy maintains system integrity for our Remote Online Notarization platform.

2. Scope

Applies to all changes (feature releases, configuration updates, infrastructure modifications) and security patches affecting:
- Production, staging, and development environments
- Network devices, servers, databases, and cloud infrastructure (AWS, Twilio, Authenticate.com integrations)
- Application code, dependencies, and container images

3. Roles & Responsibilities

Role	Responsibility
Change Advisory Board (CAB)	Reviews and approves all non-emergency changes
CISO	Policy owner; oversees change management and patch compliance
Security Team	Classify patches, assess risk, verify security testing
DevOps / IT Operations	Submit change requests, deploy changes and patches, document outcomes
Developers	Write automated tests, perform code reviews, support rollbacks
Business Owners	Provide impact analysis and approve functional changes

---

4. Change Management

4.1 Change Classification

- **Standard Changes:** Pre-authorized, low-risk (e.g., scheduled backups, routine configuration tweaks).
- **Normal Changes:** Require CAB review (e.g., new feature deployments, major configuration updates).
- **Emergency Changes:** Critical fixes to mitigate production outages or security incidents.

4.2 Change Request & Approval

1. **Submit Request:** All changes must be recorded in the Change Management system with:
   - Change description, scope, risk assessment, rollback plan
   - Affected systems, scheduled window, and owner
2. **Risk Assessment:** Security Team evaluates impact on confidentiality, integrity, and availability.

3. **CAB Review:**
   - **Normal Changes:** Discussed in weekly CAB; approved or rejected.
   - **Emergency Changes:** Convene an ad-hoc CAB; document verbal approvals immediately.
4. **Authorization:** Change cannot proceed without documented approval.

4.3 Testing & Validation

- **Development & Staging:** All changes must be tested against functional, security, and performance criteria.
- **Automated Testing:** Unit, integration, and regression tests must pass prior to production.
- **Security Testing:** Include SAST/DAST scans for code changes; verify configuration hardening for infrastructure.

4.4 Implementation & Documentation

- **Deployment Plan:** Execute changes during approved windows (off-peak hours for production).
- **Communication:** Notify stakeholders (via Slack/email) 24 hours before, during, and after change.
- **Rollback Procedures:** If issues occur, invoke the documented rollback plan immediately.
- **Post-Implementation Review:** Document actual start/end times, deviations, incidents, and lessons learned.

4.5 Change Monitoring & Reporting

- Track change success/failure metrics monthly.
- Include change management dashboard in quarterly SOC 2 and executive reports.
- Conduct annual audit of change records for completeness and compliance.

---

5. Patch Management

5.1 Patch Classification

- **Critical Security Patches:** Remediate CVSS score >=7.0 or vendor-identified critical fixes.
- **High/Medium Patches:** CVSS score 4.0–6.9 or important bug/security fixes.
- **Low/Informational Patches:** Non-security updates or cosmetic fixes.

5.2 Patch Scheduling & Deployment

- **Critical Patches:**
  - Test in staging within 48 hours of release.
  - Deploy to production within 7 days.
- **High/Medium Patches:**

  - Test in staging within 14 days.
  - Deploy to production within 30 days.
- **Low/Informational:**
  - Deployed as part of quarterly maintenance windows.

5.3 Testing & Validation

- Verify patch compatibility with existing applications and integrations (Twilio, AWS SDKs).
- Conduct post-patch smoke tests to confirm system functionality and security.

5.4 Patch Documentation & Monitoring

- Record patch details (source, version, date applied, affected systems) in the Patch Inventory.
- Monitor patch compliance weekly; report missing or failed deployments within 24 hours.
- Include patch status in monthly security and operations reports.

---

6. Emergency Change & Patch Exceptions

- Document emergency changes/patches with business justification and CAB retrospective approval.
- Apply compensating controls if rollback is not feasible.
- Review all emergency actions in the next CAB meeting.

7. Enforcement & Sanctions

- Failure to follow this policy may result in disciplinary action, up to termination or contract cancellation.
- Security Team will audit adherence to change and patch processes semi-annually.

8. Review & Updates

- Policy reviewed annually or upon:
  - Significant incidents or system outages
  - Major regulatory updates
  - Findings from audits or risk assessments

End of TeleSeal Change Management & Patch Management Policy

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

TeleSeal Incident Response & Breach Notification Policy

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

---

1. Purpose

To establish a structured, timely, and effective process for detecting, responding to, containing, and reporting security incidents and data breaches. This policy aligns with Arizona RON requirements and applicable breach-notification laws.

2. Scope

Applies to all TeleSeal systems, networks, applications, data stores, and personnel (employees, contractors, third-party vendors) involved in the handling of security events or data breaches.

3. Roles & Responsibilities

Role	Responsibility
CISO	Policy owner; convene Incident Response Team; approve notifications; oversee post-mortems
Incident Response Team (IRT)	Lead detection, analysis, containment, eradication, recovery, and post-incident reviews
All Staff	Report suspected incidents immediately via designated channels

4. Definitions

- **Security Incident:** Any event that may compromise confidentiality, integrity, or availability of systems or data.
- **Breach:** Confirmed unauthorized access to or disclosure of Confidential or Restricted data.
- **Incident Response Team (IRT):** Cross-functional group charged with coordinating incident handling.

---

5. Incident Response Phases

5.1 Preparation

- Maintain and distribute a current **Incident Response Plan (IRP)**.
- Ensure IRT members have access to tools (SIEM, forensics kits, contact lists).
- Conduct annual **tabletop exercises** and update IRP based on findings.

5.2 Detection & Analysis

- **24/7 Monitoring:** Security Team uses logs, alerts, and anomaly detection to identify suspicious activity.

- **Initial Triage:** IRT assesses scope, impact, and urgency within **1 hour** of detection.
- **Classification:** Label as Incident or Breach based on data sensitivity and unauthorized access.

5.3 Containment

- **Short-Term:** Isolate affected systems (network segmentation, account suspension) to halt damage.
- **Long-Term:** Apply temporary fixes (patches, firewall rules) pending eradication.

5.4 Eradication

- Remove malicious artifacts (malware, compromised accounts).
- Apply security patches and harden configurations.
- Validate eradication through targeted scans and tests.

5.5 Recovery

- Restore systems from known-good backups.
- Monitor restored systems for anomaly recurrence.
- Return to normal operations once validated.

5.6 Post-Incident Review

- Convene IRT within **one week** of recovery.
- Document root cause, timeline, detection/response effectiveness, lessons learned.
- Update IRP, controls, and training to prevent recurrence.

---

6. Breach Notification Procedures

6.1 Internal Notification

- **Within 24 hours** of confirming a breach, IRT notifies:
  - CISO
  - Legal & Compliance
  - Executive Leadership

6.2 Regulatory & State Notification

- **Arizona RON Authorities:** Submit written notice to the Secretary of State's office within **10 business days** of breach confirmation.
- **Other Jurisdictions:** Comply with applicable data breach laws (e.g., Arizona A.R.S. § 18-571, GDPR, etc.) regarding timelines and content.

6.3 Customer & Third-Party Notification

- **"Without unreasonable delay,"** notify affected individuals via email or postal mail, including:
  - Nature of the breach
  - Data elements involved
  - Mitigation steps taken
  - Contact information for inquiries
- Offer credit monitoring or identity-theft protection as required by regulation or best practice.

6.4 Public Disclosure

- Coordinate with Communications/PR and Legal to craft public statements.
- Ensure compliance with securities, consumer protection, and privacy laws.
- Publish statement on company website and social media as appropriate.

---

7. Communication & Coordination

- Use a **central incident ticket** or collaboration channel to track all activities.
- Maintain a **notification log** recording who was notified, when, and by what method.
- Hold weekly update meetings during active incidents.

8. Evidence Preservation & Forensics

- Preserve logs, disk images, memory snapshots, and relevant artifacts in a **forensically sound** manner.
- Chain-of-custody documentation for all evidence.
- Engage external forensic experts if needed.

9. Documentation & Record-Keeping

- Maintain an **Incident Report** for every event, including timelines, actions taken, and lessons learned.
- Retain Incident Reports and notification records for **at least 7 years** in encrypted storage.

10. Training & Awareness

- Annual security training for all staff on incident identification and reporting.
- IRT members participate in quarterly drills.

11. Policy Exceptions

- Any deviation must be approved by the CISO and documented with compensating controls.

12. Enforcement

- Violations of this policy may result in disciplinary action, up to termination or contract termination.
- The Security Team will audit adherence to this policy bi-annually.

13. Review & Updates

- This policy is reviewed annually or upon:
  - Major incidents or breaches
  - Changes in regulatory requirements
  - Findings from audits or risk assessments

End of TeleSeal Incident Response & Breach Notification Policy