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