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