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