Technology Solutions – Breach Notification Procedure

Department: Technology Solutions
Procedure Name: Breach Notification
Procedure ID: TS-PROC-013
Effective Date: 01/22/2026
Last Reviewed: 01/22/2026

Owner: Chief Information Officer (CIO)

Applies To: All Technology Solutions staff and leadership

1. Purpose

This procedure defines how Technology Solutions identifies, escalates, and coordinates breach notification activities in the event of a suspected or confirmed data breach or security incident.

2. Scope

This procedure applies to all suspected or confirmed breaches involving institutional systems, applications, infrastructure, or sensitive data regardless of hosting location.

3. Definitions

Security Incident: An event that may compromise confidentiality, integrity, or availability.
Data Breach: Confirmed unauthorized access or disclosure of sensitive data.

4. Guiding Principles

Assume impact until proven otherwise. Do not speculate. Contain first. Centralize decisions. Preserve evidence.

5. Initial Identification & Escalation

Any staff member identifying a suspected breach must immediately follow TS-PROC-007 and notify Technology Solutions leadership via the Incident Response channel.

6. Containment & Investigation

Containment and investigation activities prioritize preventing further exposure and preserving evidence. External communication is prohibited without CIO approval.

7. Breach Determination

The CIO, in coordination with leadership and legal counsel as required, determines whether a breach has occurred and if notification is required.

8. Notification Authority

All breach notifications require CIO approval. No staff member may independently notify individuals or external entities.

9. Notification Requirements

Notifications will be timely, factual, and compliant with applicable regulatory requirements.

10. Communication Standards

All communications must use approved messaging and align with Communications by Severity guidance.

11. Post-Breach Documentation & Review

Incident investigation reports and corrective actions are mandatory following resolution.

12. Training & Awareness

Staff must understand breach escalation responsibilities and participate in training as required.

13. Compliance & Enforcement

Failure to follow this procedure may result in corrective or disciplinary action.

14. Review Cycle

This procedure will be reviewed annually or as regulatory or institutional requirements change.