Data Breach Incident Response Plan - Summary

Document ID: LC-DBRP-2025.01
Version: 1.0
Effective Date: 2025-11-01
Department: Legal, IT Security, Communications

1. Scope

This plan outlines the immediate and coordinated response required for any unauthorized access to NexaCore systems, loss, destruction, or unauthorized disclosure of Personal Data (PD) or Confidential Information (CI).

2. Incident Response Team (IRT)

Role	Responsibility	Backup
Incident Commander (IC)	Head of IT Security	CTO
Legal Counsel	Compliance Officer	Head of Legal
Communication Lead	Head of Marketing/Comms	Head of HR
Technical Lead	Lead Engineer (SecOps)	IT Operations Manager

3. Four Phases of Response

Phase 1: Detection and Containment (Immediate)

- **Action:** Technical Lead isolates affected systems (e.g., disconnecting network segments, changing compromised credentials).
- **Goal:** Stop the breach and prevent further data loss or system damage.
- **Notification:** IC notifies IRT members immediately.

Phase 2: Assessment and Eradication (0-48 Hours)

- **Action:** Forensic analysis to determine the root cause, scope (what data was affected, whose data), and severity.
- **Goal:** Fully understand the incident, remove the threat, and restore affected systems.
- **Legal Input:** Legal Counsel assesses regulatory notification obligations (e.g., within 72 hours under GDPR/PDPL).

Phase 3: Notification and Communication

- **Action:** Communication Lead prepares internal and external statements. Legal Counsel manages mandatory notifications to regulatory authorities (e.g., Dubai Regulator) and affected data subjects (clients/employees).
- **Rule:** All external communication must be vetted and approved by Legal Counsel and the CEO. **No public statements are permitted without approval.**

Phase 4: Post-Incident Review

- **Action:** IRT conducts a "lessons learned" review, updates security policies and controls, and documents the full incident lifecycle for audit purposes.