Title: Incident Response Plan & Data Breach Procedure
Owner: Security Team / DPO
Version: 2.1
Update Date: 01.11.2025
Reference: GDPR Art. 33 & 34

Document 2: Incident Response Plan (IRP)

1. Purpose

This plan outlines the steps Replenit takes to detect, respond to, and recover from security incidents. It specifically mandates the timelines for notifying clients (Controllers) and authorities.

2. Incident Response Team (IRT)

The IRT consists of:

- **Incident Commander:** CTO / Head of Engineering
- **Legal/Compliance Lead:** DPO
- **Technical Lead:** Senior DevOps Engineer

3. The Incident Lifecycle (Phases)

Phase 1: Identification & Classification

- Any employee who suspects a security incident must report it immediately to security@replen.it or via the internal Slack #security-alerts channel.
- The Incident Commander classifies the event:
    - **Sev-3 (Low):** Non-critical deviation (e.g., failed login attempt).
    - **Sev-1 (Critical):** Confirmed data leak, unauthorized access to production, or ransomware.

Phase 2: Containment & Eradication

- **Short-term:** Isolate affected systems (e.g., take offline, revoke API keys, block IP addresses).
- **Long-term:** Patch vulnerabilities, reset all compromised credentials, and restore from clean backups.

Phase 3: Breach Notification (CRITICAL)

- **Internal Assessment:** The IRT must determine within **24 hours** if the incident constitutes a "Personal Data Breach" under GDPR.
- **Client Notification (The 48-Hour Rule):**
  Strict Requirement: If a Personal Data Breach affecting Client Data is confirmed, Replenit **must notify the Client (Controller)** without undue delay, and **in no event later than 48 hours** after becoming aware of the breach.
- **Content of Notification:** The notice shall include:
    1. Nature of the breach.
    2. Categories and approximate number of data subjects concerned.
    3. Likely consequences of the breach.
    4. Measures taken or proposed to address the breach.

Phase 4: Post-Incident Activity

- A "Post-Mortem" report is generated within 5 business days.
- The Root Cause Analysis (RCA) is shared with affected Clients upon request.

4. Testing and Updates: This plan is tested annually via a Tabletop Exercise.