Data Breach and Management Response Policy

This process applies to any confirmed **security incident** involving the unauthorized access, acquisition, disclosure, or loss of **Personal Information (PI)** or **Sensitive Personal Information (SPI)** held, processed, or transmitted by the Company. The primary goal is to contain the breach, eliminate the threat, recover systems, and fulfill all legal and contractual notification obligations to regulators and customers within mandated timeframes.

---

2. Data Breach Incident Response Stages

The data breach management process is divided into four stages: Preparation (Ongoing), Detection & Analysis, Containment & Remediation, and Post-Incident Activity.

Stage 1: Detection and Analysis

Step	Action	Responsibility	Timeframe
2.1.1. Triage & Confirmation	Upon initial alert, the Incident Response Team (IRT) verifies if a security incident has occurred and, if so, whether it involves PI or SPI.	**Incident Response Team (IRT)**	**Within 1 hour** of initial alert.
2.1.2. Severity & Scope	Determine the severity (High, Medium, Low) and scope (systems, data subjects, data types) of the breach. This informs subsequent notification deadlines.	**IRT Lead & CISO (Chief Information Security Officer)**	**Within 4 hours** of confirmation.
2.1.3. Activate Response Team	Mobilize the full Data Breach Response Team (DBRT) as defined in the master Incident Response Plan.	**IRT Lead**	Immediately after severity determination.

Stage 2: Containment, Eradication, and Recovery

Step	Action	Responsibility	Timeframe
2.2.1. Containment	Immediately isolate affected systems, take offline network segments, and revoke compromised credentials to stop the breach from spreading.	**Security Operations / IRT**	Immediately upon confirmation.
2.2.2. Eradication	Remove the root cause of the breach (e.g., delete malware, patch the exploited vulnerability, reconfigure systems).	**Engineering & IRT**	As rapidly as technically feasible.
2.2.3. Recovery	Restore affected systems from secure backups, validate system security, and monitor for recurrence.	**Engineering & IRT**	After root cause is fully eradicated.

---

3. Communication Roles and Notification Requirements

Defined roles and strict timeframes are critical for regulatory compliance and customer trust.

3.1. Defined Communication Roles

Role	Responsibility
Legal Counsel / Privacy Officer	**Regulatory and Legal Communication:** Oversees all communication to Supervisory Authorities (e.g., DPC, ICO, CPPA) and provides guidance on the necessity and content of customer notifications.
Chief Executive Officer (CEO) / CISO	**Executive Communication:** Decides on public statements and formally accepts the residual risk following remediation.
Customer Communications Lead (Marketing/Sales)	**Customer Communication:** Drafts, coordinates, and sends formal notifications to affected customers/clients/partners. Manages the communications hotline and FAQ.

Role	Responsibility
Forensics Lead	**Evidence & Documentation:** Ensures that evidence is collected, preserved, and detailed records are created for all investigation and remediation activities.

3.2. Regulatory Reporting Timeframes

The following timeframes represent key obligations under major privacy regulations. The most stringent applicable requirement will always be followed.

Regulation	Data Subject(s)	Required Action	Timeframe
GDPR (EU/EEA)	European Union Residents	**Notify Supervisory Authority (SA):** Required unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.	**Within 72 hours** of becoming aware of the breach.
		Notify Data Subject: Required if the breach is likely to result in a high risk to the rights and freedoms of natural persons.	**Without undue delay.**
CCPA/CPRA (California)	California Residents	**Notify Affected Consumers:** Required for breaches of unencrypted and unredacted PI.	**The most expedient time possible** and without unreasonable delay.
HIPAA (If applicable to client data)	Protected Health Information (PHI)	**Notify Secretary of HHS and Affected Individuals.**	**Without undue delay** and in no case later than **60 days** after discovery.

Policy on Timeframes: For breaches of PI, the Company shall initiate a formal legal review of all applicable notification requirements within **4 hours** of confirmation, and aim to prepare the notification draft within **24 hours**.

---

4. Record Keeping and Post-Incident Activity

4.1. Maintenance of Breach Records

All data breach incidents, whether reportable or not, shall be documented and archived in a **Breach Register**. This is essential for demonstrating accountability, fulfilling legal obligations, and for audit purposes.

The record for each incident will include:

1. **Date and Time of Discovery:** When the incident was detected and confirmed.
2. **Scope and Impact:** A description of the incident, the categories and approximate number of data subjects affected, and the types of PI/SPI involved.
3. **Containment and Remediation:** A detailed log of all actions taken to contain and recover from the incident.
4. **Root Cause Analysis:** The confirmed reason the breach occurred (e.g., system vulnerability, human error).
5. **Notification Documentation:** Copies of all communications sent to customers, regulators, and third parties, including the date and method of transmission.
6. **Lessons Learned:** Recommendations for control improvements.

4.2. Post-Incident Review and Improvement

After the breach is contained and notifications are complete, the DBRT will conduct a formal **Lessons Learned Review**. This review must identify failures in controls, processes, or training that contributed to the incident. Findings will be used to update the Risk Assessment Policy, revise security controls, and improve future incident response training. The CISO will track all resulting remediation actions to closure.