Data Breach Reporting and Response Framework

AWAKEN ENERGY

To ensure compliance with data protection laws, including the **Privacy Act 1988 (Cth)** and the **Notifiable Data Breaches (NDB) scheme**, our business has established a detailed framework for reporting and addressing data breaches.

Definition of a Data Breach

A data breach occurs when personal or sensitive information is accessed, disclosed, lost, or otherwise handled in an unauthorized manner. Examples include:

- Unauthorized access to systems or databases.
- Accidental loss of physical documents containing sensitive information.
- Cyberattacks such as phishing, malware, or ransomware.
- Sending personal information to the wrong recipient.

Steps for Addressing a Data Breach

Step 1: Identification and Containment

- **Immediate Identification**:
  - Detect and assess the breach promptly.
  - Verify whether the breach involves personal or sensitive information.
- **Containment**:
  - Stop unauthorized access by disabling affected systems, accounts, or servers.
  - Retrieve lost or disclosed information, if possible.

Step 2: Assessment and Risk Evaluation

- Conduct a quick but thorough assessment to determine:
  - The type of data involved (e.g., financial details, health records).
  - The scope and impact of the breach.
  - Whether the breach is likely to result in serious harm to individuals.
- Document the findings, including evidence of the breach and mitigation actions.

Step 3: Notification (If required)

Under the **NDB Scheme**, notification is required if a breach is likely to cause serious harm. This involves:

- **Notifying Affected Individuals**:
  - Inform affected individuals of the breach, outlining:
    - The nature of the breach.
    - The type of information compromised.
    - Recommended steps to mitigate harm (e.g., changing passwords, monitoring accounts).
- **Notifying the Office of the Australian Information Commissioner (OAIC)**:
  - Submit a formal notification to the OAIC, including:
    - A description of the breach.
    - The information compromised.
    - The steps being taken to mitigate harm.
    - Contact details for further information.

Step 4: Mitigation and Remediation

- Implement measures to minimize the impact of the breach, such as:
  - Resetting system passwords or disabling compromised accounts.
  - Providing support to affected individuals (e.g., credit monitoring services).
  - Engaging cybersecurity experts to assess and strengthen defenses.

Step 5: Documentation and Review

- Maintain a comprehensive record of:
  - How the breach occurred.
  - The response actions taken.
  - Recommendations for improvement.
- Conduct a post-incident review to:
  - Identify vulnerabilities.
  - Implement corrective actions to prevent similar breaches in the future.

Reporting Channels

- **Internal Reporting**:
  - Employees must report suspected data breaches immediately to the **Data Protection Officer (DPO)** or designated compliance team.
- **External Reporting**:
  - If required, notify the OAIC and affected individuals in accordance with the NDB Scheme.

Training and Awareness

- Regular training sessions for staff on:
  - Recognizing and reporting potential breaches.
  - Implementing best practices for data security.
- Awareness campaigns to reinforce the importance of safeguarding sensitive information.

Continuous Monitoring and Improvement

- Implement data breach simulations (e.g., penetration testing) to test response readiness.
- Regularly update policies and systems to stay aligned with evolving threats and regulatory changes.

This structured approach ensures that our business can address data breaches effectively while maintaining compliance with legal obligations and protecting stakeholders' trust.