Data Breach Response Plan

This data breach response plan is essential for effectively managing and mitigating the impact of a data breach. The plan provides a step-by-step guide into handling any personal data breach.

The plan is in relation to personal data breach, which is defined under the Data Protection Act as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Unless otherwise specified, this plan is generally written from the context of the Company as a data controller.

Data Breach Response Plan

1. Preparation

- **The Incident Response Team (IRT):**
  Data breaches shall be handled by a management committee made up of the following members and any other that they may co-opt:

Person	Role
The DPO	Secretary and Advisor
The Chief Technology Officer	Chairperson
Chief Operations Officer	Member
Human Resource & Admin Manager	Member
Publishing Manager	Member

2. Detection and Analysis

- **Monitoring and Security Information & Event Management Systems:** Implement intrusion detection systems (IDS), intrusion prevention systems (IPS), security information & event management (SIEM) and other monitoring tools to detect suspicious activities. At present, the following tools have been implemented:
  a) Fortinet firewall to prevent intrusion and web filtering. It comes with the following features:
     - **FortiAnalyzer (Log Management & Threat Intelligence)** which provides centralized logging and reporting for security events. It uses threat intelligence from **FortiGuard Labs** to detect advanced persistent threats (APTs). This helps with forensic analysis and compliance reporting.
     - **FortiGate Next-Generation Firewall (NGFW):** Which comes with an Intrusion Prevention System (IPS) for detecting malicious network traffic. It's also Integrated with FortiAnalyzer for centralized logging and reporting events.
  b) Microsoft office 365 Business premium

- Utilizes AI-driven analytics for detecting, investigating, and responding to security incidents.
- The platform also provides real-time correlation of security events.
- The package comes with Microsoft Purview (Compliance & Risk Management) which provides a platform to monitor and audit user activity across Office 365 applications. It provides data loss prevention (DLP) and information protection mechanism. This platform ensures compliance with regulations such as GDPR.

- **Incident Identification:** Our established criteria for identifying a data breach includes:
  - **a) Unauthorized Access:**
    - Detection of unauthorized access to sensitive data or systems.
    - Unusual login patterns, such as access from unfamiliar locations or devices.
  - **b) Data Exfiltration:**
    - Large volumes of data being transferred outside the organization.
    - Unusual data transfer activities, especially to external IP addresses.
  - **c) Malware Detection:**
    - Evidence of malware or ransomware on systems.
    - Alerts from antivirus or endpoint detection and response (EDR) tools.
  - **d) System Anomalies:**
    - Unexpected system behavior, such as unexplained crashes or performance issues.
    - Unplanned system reboots or shutdowns.
  - **e) User Reports:**
    - Reports by employees or customers about suspicious activities or potential breaches.
    - Phishing attempts reported by users.
    - Users should make their reports without delay to the DPO.
  - **f) Security Alerts:**
    - Alerts from intrusion detection systems (IDS) or security information and event management (SIEM) tools.
    - Detection of known attack patterns or signatures.
  - **g) Data Integrity Issues:**
    - Unexplained changes to data or configurations.
    - Missing or corrupted data files.
  - **h) Access Control Violations:**
    - Attempts to access restricted areas or data without proper authorization.

- Multiple failed login attempts or account lockouts.

i) **Network Anomalies:**
   - Unusual network traffic patterns, such as spikes in data transfer or connections to suspicious IP addresses.
   - Detection of network scanning or probing activities.

j) **Compliance Violations:**
   - Detection of activities that violate regulatory or compliance requirements.
   - Unauthorized sharing or exposure of personal data.

Staff members should be regularly trained on these signs to ensure any breach is detected or reported early.

- **Initial Assessment:** Quickly assess the nature and scope of the breach to determine its impact.

3. Containment and Mitigation

- **Immediate Containment:** Promptly take steps to contain the breach and prevent further data loss (e.g., isolating affected systems). The IRT should consider applying both short-term mitigation and rapid response. Short term mitigation involves implementing temporary measures to secure systems and data while a full investigation is conducted. Rapid Response involves immediate steps to contain the breach, such as isolating affected systems or disabling compromised accounts.
- Other measures may include:

a) **Network Segmentation:**
   - **Isolate Affected Systems:** Segment the network to isolate compromised systems and prevent the spread of the breach.
   - **Restrict Access:** Limit access to sensitive data and critical systems to only essential personnel.

b) **Endpoint Security:**
   - **Quarantine Infected Devices:** Immediately quarantine any devices suspected of being compromised to prevent further infection.
   - **Deploy Patches:** Apply security patches and updates to all affected systems to close vulnerabilities.

c) **Data Encryption:**
   - **Encrypt Sensitive Data:** Ensure that sensitive data is encrypted both in transit and at rest to protect it from unauthorized access.
   - **Use Strong Encryption Protocols:** Implement robust encryption standards to enhance data security.

d) **User Account Management:**

- **Disable Compromised Accounts:** Temporarily disable accounts that may have been compromised to prevent unauthorized access.
- **Enforce Multi-Factor Authentication (MFA):** Require MFA for accessing critical systems and data to add an extra layer of security.

e) **Backup and Recovery:**
- **Restore from Backups:** Use clean backups to restore affected systems and data, ensuring they are free from malware.
- **Regular Backup Testing:** Regularly test backup and recovery procedures to ensure they work effectively during an incident.

f) **Threat Intelligence:**
- **Leverage Threat Intelligence Feeds:** Use threat intelligence feeds to stay informed about emerging threats and vulnerabilities.
- **Share Information:** Collaborate with industry peers and information-sharing organizations to exchange threat information.

g) **Incident Response Tools:**
- **Deploy Forensic Tools:** Use forensic tools to analyze the breach and gather evidence for further investigation.
- **Automate Response Actions:** Implement automated response actions to quickly contain and mitigate threats.

h) **Communication Protocols:**
- **Establish Clear Communication Channels:** Set up dedicated communication channels for incident response to ensure timely and accurate information sharing.
- **Regular Updates:** Provide regular updates to stakeholders about the status of the breach and response efforts.

i) **Legal and Compliance:**
- **Consult Legal Counsel:** Work with legal counsel to understand regulatory requirements and ensure compliance with data breach notification laws.
- **Document Actions:** Maintain detailed records of all actions taken during the response to demonstrate compliance and support legal proceedings.

j) **Data Subject Support:**
- **Provide Support Resources:** Offer resources and support to data subjects affected by the breach, including counseling and identity protection services.
- **Conduct Awareness Training:** Educate data subjects about the breach and reinforce best practices for data security.

4. Investigation and Analysis

- **Root Cause Analysis:** Investigate the breach to determine how it occurred and identify the root cause.
- **Impact Assessment:** Evaluate the extent of the data compromised and the potential impact on the organization and affected individuals.

5. Notification and Communication

- **Internal Communication:** Immediately inform key stakeholders within the organization about the breach and the response plan.
- **External Notification:** External communication may be to the affected individuals or regulatory bodies (ODPC) and must be in writing. A breach is externally notifiable if it relates to:
    - the data subject's full name, identification number, financial information, health information, sensitive personal information and any other information specified under the Second Schedule to The Data Protection (General) Regulations.
    - the data subject's account identifier, such as an account name or number; or
    - any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

- The external notifications shall follow the following protocols:
    - The ODPC should be notified within 72 hours of becoming aware of the breach. If the notification cannot be made within 72 hours, it must be made as soon as possible thereafter, and reasons for the delay provided to ODPC. Notification to the ODPC shall state:
        - the date on which and the circumstances in which the data controller or data processor first became aware that the data breach had occurred;
        - a chronological account of the steps taken by the data controller or data processor after the data controller or data processor became aware that the data breach had occurred, including the data controller or data processor's assessment that the data breach is a notifiable data breach;
        - details on how the notifiable data breach occurred, where applicable;
        - the number of data subjects or other persons affected by the notifiable data breach;
        - the personal data or classes of personal data affected by the notifiable data breach;
        - the potential harm to the affected data subjects as a result of the notifiable data breach;
        - information on any action by the data controller or data processor, whether taken before or to be taken after the data controller or data processor notifies the ODPC of the occurrence of the notifiable data breach to eliminate or mitigate any

potential harm to any affected data subject or other person as a result of the notifiable data breach or address or remedy any failure or shortcoming that the data controller or data processor believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;
        - the affected individuals or the public that the notifiable data breach has occurred and how an affected data subject may eliminate or mitigate any potential harm as a result of the notifiable data breach;
        - contact information of an authorized representative of the data controller or data processor;
        - Reasons for not notifying the affected data subject, where a decision has been made to not notify them.

    - The affected data subject should be notified as soon as possible, provided their identity is known and their data was not encrypted. This notification may be delayed as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the relevant body concerned. The notice to the affected data subject may where necessary be sent in phases and should include:
        - description of the nature of the data breach;
        - description of the measures that the data controller or data processor intends to take or has taken to address the data breach;
        - recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;
        - where applicable, the identity of the unauthorized person who may have accessed or acquired the personal data; and
        - the name and contact details of the data protection officer where applicable or other contact point from whom more information could be obtained.
    - Where the company is a data processor, it must inform the data controller within 48 hours of becoming aware of the breach.

Public Relations: in consultation with the public relations/ marketing/ communications department, prepare a public statement and manage communication with the media to maintain transparency and trust.

6. Recovery and Restoration

- **System Restoration:** Clean or restore affected systems and data from backups, ensuring they are secure and free from vulnerabilities.
- **Continuous Monitoring:** Monitor systems for any signs of residual threats or further breaches.

7. Evaluation and Learning

- **Post-Incident Review:** Conduct a thorough review of the incident and the response to identify lessons learned.

- **Response Plan Updates:** Update the data breach response plan based on the findings from the review to improve future readiness.
- **Ongoing Improvement:** Continuously refine and enhance security measures and response procedures.

8. Documentation and Reporting

- **Incident Documentation:** Document the incident and maintain detailed records of the breach, response actions, and communications. In particular, the IRT must maintain a record of:
    - the facts relating to the breach.
    - its effects; and
    - the remedial action taken.

TEMPLATES FOR NOTIFICATION

1. **NTF001** for Notification of Data Breach – Data Subject
2. **NTF002** for Notification of Data Breach – ODPC