Policy Title: Data Breach Incident & Notification Policy & Procedures
Policy Number: AFL/DBIP/002
Version: 1.0
Effective Date: Monday, September 01, 2025

Approved By: CEO/Data Protection Officer

1.0 Policy Statement

Andray Finance Limited ("the Company") is committed to protecting the confidentiality, integrity, and availability of personal data in its custody. Despite robust security measures, the risk of a data breach can never be entirely eliminated.

This policy establishes a clear framework for the timely and effective identification, containment, investigation, and notification of data breaches in compliance with the **Nigeria Data Protection Act (NDPA) 2023** and other relevant regulations. The Company prioritizes transparent communication with affected data subjects and regulators to mitigate potential harm and maintain trust.

2.0 Objectives

- To provide a clear and effective process for responding to suspected or confirmed data breaches.
- To minimize the impact of any data breach on affected individuals and the Company.
- To ensure full compliance with the legal and regulatory obligations for breach notification under the NDPA.
- To define roles, responsibilities, and escalation paths during an incident.
- To facilitate post-incident analysis to prevent future occurrences.

3.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other third parties who process personal data on behalf of Andray Finance Limited. It covers all personal data processed by the Company, in both electronic and physical formats.

4.0 Definition of a Data Breach

A data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

This includes, but is not limited to:

- **Cyberattacks:** (e.g., hacking, phishing, ransomware infection).
- **Unauthorized Access:** An employee or third-party accessing data beyond their authorization.
- **Physical Theft/Loss:** Loss or theft of devices (laptops, phones), paper records, or storage media.
- **Human Error:** Sending personal data to the wrong recipient via email or post.
- **System Misconfiguration:** Data exposed online due to incorrect security settings.

5.0 Roles and Responsibilities

- **All Staff:** Are responsible for immediately reporting any suspected data breach to their line manager and the Data Protection Officer (DPO).
- **Line Managers:** Must ensure reported incidents are escalated immediately to the DPO and Head of Department.
- **Data Protection Officer (DPO):** The central point of contact for all breach reports. Responsible for coordinating the response, ensuring regulatory compliance, and leading the investigation.
- **Incident Response Team (IRT):** A cross-functional team activated in the event of a major breach. Members typically include:
    - DPO (Team Lead)
    - Head of IT / CISO
    - Head of Legal & Compliance
    - Head of Corporate Communications/PR
    - Head of relevant business unit (e.g., Lending Operations)
- **CEO / Management:** Responsible for providing strategic direction, resource allocation, and final approval for significant actions (e.g., public notifications).

PROCEDURES

6.0 Step 1: Identification and Reporting

1. **Discovery:** Any individual who identifies or suspects a data breach must **immediately** (within the hour) notify their direct supervisor and the DPO.
2. **Initial Report:** The report should include:
    - Reporter's name and department.
    - Date and time the incident was discovered.
    - Description of the incident (what happened?).
    - Type of data involved (e.g., customer names, BVNs, bank details, loan history).
    - Potential number of data subjects affected.
    - Immediate actions already taken (if any).

Contact for Reporting:

- **Data Protection Officer:** Edidiong Paul | Email: dpo@andrayfinance.ng | Phone: 0803 234 3908

7.0 Step 2: Containment and Initial Assessment

1. **Immediate Action:** The DPO, in conjunction with the IT Department, will take immediate steps to contain the breach. This may include:
    - Disconnecting affected systems from the network.
    - Resetting passwords and revoking access privileges.
    - Retrieving mistakenly sent emails or documents.
    - Securing a physical area.
2. **Preliminary Assessment:** The DPO will conduct an initial assessment to:
    - Confirm if a breach has occurred.
    - Determine the likely cause and scope.
    - Assess the potential risk to individuals' rights and freedoms.

8.0 Step 3: Escalation and Activation

1. The DPO will immediately escalate the incident to the CEO and Head of Legal.
2. For breaches deemed to pose a **risk to individuals**, the DPO will activate the Incident Response Team (IRT). The IRT will hold its first meeting urgently to coordinate the response.

9.0 Step 4: Investigation and Evaluation

The IRT will lead a thorough investigation to:

- Identify the root cause of the breach.
- Determine the exact scope: what specific data was compromised, how many data subjects are affected, and who the affected individuals are.
- Evaluate the likely consequences and risk level (e.g., risk of identity theft, financial fraud, reputational damage).

10.0 Step 5: Notification

A. Regulatory Notification to NDPC:

- Where a breach is likely to **prejudice the rights and freedoms of data subjects**, the Company shall notify the Nigeria Data Protection Commission (NDPC) **within 72 (seventy-two) hours** of becoming aware of the breach.
- The notification to the NDPC will include:
    - The nature of the personal data breach.
    - The number of data subjects affected.
    - The likely consequences of the breach.
    - The measures taken or proposed to be taken to address the breach and mitigate its adverse effects.
    - The name and contact details of the DPO.

B. Data Subject Notification:

- If the breach is likely to result in a **high risk to the rights and freedoms of individuals** (e.g., financial loss, identity theft, discrimination), affected data subjects must be notified **without undue delay**.
- The notification will be clear, transparent, and communicated directly (e.g., by email, SMS, phone call) and will include:
    - A description of the breach in clear and plain language.
    - The likely consequences of the breach.
    - The measures taken to address the breach.
    - Advice on steps the individual can take to protect themselves (e.g., monitor bank statements, change passwords, place a fraud alert).
    - Contact details for the DPO and how they can obtain more information.

C. Exceptions to Notification: Data subject notification is not required if:

- The Company has implemented subsequent measures that ensure the high risk is no longer likely to materialize.
- It would involve disproportionate effort (in which case a public communication or similar measure will be used).

11.0 Step 6: Documentation and Post-Incident Review

- **Documentation:** Every data breach, regardless of size, must be fully documented in a **Breach Register**. This record will include the facts, effects, and remedial actions taken, and will be made available to the NDPC upon request.

- **Post-Incident Review:** After the incident is resolved, the IRT will conduct a review to:
    - Identify lessons learned.
    - Determine the root cause and evaluate the effectiveness of the response.
    - Recommend updates to security policies, procedures, systems, or staff training to prevent a similar breach from recurring.

12.0 Training and Testing

- All staff will receive annual training on this policy and their responsibilities regarding data breach reporting.
- A simulated data breach exercise will be conducted at least annually to test the effectiveness of this plan.

13.0 Policy Review

This policy and procedures shall be reviewed annually or following a significant incident or change in law to ensure its continued suitability, adequacy, and effectiveness.