BHANIX FINANCE AND INVESTMENT LIMITED

DATA PRESERVATION & DISPOSAL POLICY FOR PERSONALLY IDENTIFIABLE INFORMATION (PII) DATA

Board Approval Date	Prepared by	Reviewed by	Version No	Last Review Date
October 16, 2025	Head of Technology	Chief Executive Officer (CEO)	5	March 21, 2025

Table of Contents

1. PURPOSE

The purpose of this procedure is to provide details on how to identify and handle Personally Identifiable Information (PII), the process of securely storing any PII that the organization is required to maintain, and what to do in the event of a disclosure of PII.

Bhanix Finance & Investment Limited (BFIL) employees, in the course of their normal job responsibilities, will encounter Personally Identifiable Information (PII). Employees need to understand their roles in the collection and storage of PII.

2. SCOPE

This policy applies to all staff, employees and entities working on behalf of BFIL who are using BFIL-owned or personally-owned computers or workstations that are connected to the BFIL network.

3. IDENTIFYING PII

There are two (2) types of Personally Identifiable Information (PII) and identification of each type will dictate the actions needed to ensure its safety and integrity.

Public PII:

This is information that is available in public sources such as telephone books, employee directories, public websites, etc. The following information can be considered Public PII:

- First and the last name
- Address
- Telephone Number
- Email Address

Protected PII:

This is defined as any information which, if lost, compromised or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. It includes any one or more of the types of information that are outlined below:

- Username and password
- Passport number
- Bank account number
- Credit card number
- Banking information
- Biometrics

3.1 Maintaining PII

During normal job responsibilities, employees may encounter either Public or Protected PII, either already existing in the BFIL network, or as a part of a business process. Because Protected PII requires special handling due to the potential risk associated with its disclosure, it is important to verify the need for the existence of PII in the BFIL network and ensure that the information is properly secured.

- Verifying the need to collect PII: Best practice dictates that an organization only collects the least amount of information to follow standard business procedures. Caution should especially be taken when collecting Protected PII. The need to collect the information should be periodically reviewed, and if deemed unnecessary, the procedures should be altered to reflect the change.

- Collection Procedures: If PII does need to be collected, employees have certain responsibilities in making sure the data is secured. Any written information must be destroyed via shredding. Physical files that contain PII should be locked in a secure cabinet or room when not being actively viewed or modified. Any PII data collected should not be stored on the local workstation but would need to reside in OneDrive/centralized storage, where it is encrypted and backed up.

- Verifying the need to store PII: Whenever PII is found residing in the BFIL network, a determination needs to be made regarding whether the information is needed for an existing business practice, or if it can be securely disposed. If the information does need to be retained, please contact the IT department for guidance on the best means to secure or dispose the information properly.

- Authorized dissemination of PII: In the event an outside entity needs to have any data that includes Protected PII, the said entity would need to confirm that they understand the sensitivity of the information, and the need to properly safeguard it. Once it leaves the BFIL network, BFIL/ the IT team cannot guarantee its security. Transport of data should be done through secure means–encryption or secured transport is necessary.

- Unauthorized dissemination of PII: In the event of unauthorized disclosure or access of PII, the following steps mentioned below need to be followed:
    - Report the incident to your Direct Supervisor/ Line Manager
    - Send an email to [support@email.com]
        - Do NOT forward any compromised information in the email.
        - Include the location of the information (email or network location)
        - If email, include the sender and subject (unless the subject contains the PII).

- Include any other relevant details, such as the location and contact phone number
- Comply with the instructions from the Incident Response team

4. NON- PERSONALLY IDENTIFIABLE INFORMATION (NON-PII):

Non-personally identifiable information (NON-PII) is data that cannot be used on its own to trace or identify a person. Non-PII is call logs call records or any other information which is not PII. The said data is usually collected by businesses to track and understand the digital behaviour of their consumers. this in turn can help them improve the consumer's online experience and engagement.

Examples of Non-PII include, but are not limited to:

- Call recordings between the BFIL agent and the customer
- Call recordings between the collection agency's agent and the customer
- Email communication between the BFIL agent and the customer

Non-PII data cannot be used to distinguish or trace an individual's identity such as their name, date and place of birth, bio-metric records etc but includes data collected by browsers and servers using cookies. As a result, this data does not require encryption before it is transmitted as no scope for misuse would result in harm to any individual/customer. The amount of information sent depends on the settings you have on your web browser. All such information will be used for providing effective services to the Customers.

The Non-PII statistical data is interpreted in its continuing effort to present the Website/app content that visitors are seeking in a format they find most helpful and to make our Website/app more user-friendly.

5. DATA RETENTION:

Personal Data shall be retained to support a specific business activity or legal/ regulatory/ statutory requirements (if any). The Personally Identifiable Information (PII) and Non-Personally Identifiable Information (Non-PII) shall not be retained for longer than is required for usage as per the requirement of law and shall be deleted after the expiry of the 10 years, except for court orders or pending disputes.

6. SECURE STORAGE AND DISPOSAL OF PII DATA ON THIRD-PARTY VENDORS AND SAAS PLATFORMS

Secure Storage and Encryption

- All PII data stored on third-party systems must be encrypted at rest and in transit using industry-approved cryptographic standards (e.g., AES-256, TLS 1.2/1.3).
- Vendors must certify compliance with ISO 27001, SOC 2, or equivalent security standards.

Access Control

- Access to PII data must be restricted on a need-to-know basis and enforced through role-based access control (RBAC) and Multi-Factor Authentication (MFA).
- Regular access reviews must be performed, and unused or temporary accounts must be deactivated promptly.

Data Retention Periods

- PII data must be retained on third-party systems only for the duration required by business and regulatory needs.
- Retention timelines must be clearly documented and communicated to the vendor.

Secure Data Disposal

- Upon expiry of the retention period or termination of the vendor contract, vendors must securely delete PII data following NIST SP 800-88 or equivalent data sanitization standards.
- A certificate of data destruction must be obtained and archived for audit purposes.

Contractual Obligations

- Vendor contracts must include explicit clauses requiring secure data storage, retention, and disposal in compliance with regulatory requirements.
- Contracts must mandate immediate notification in case of any data breach or unauthorized access.

Periodic Compliance Verification

- Conduct annual vendor security reviews or request compliance reports to verify adherence to data protection and disposal requirements.

7. INCIDENT REPORTING

The IT Head must be informed of a real or suspected disclosure of Protected PII data within 3 working days after discovery, e.g. misplacing a paper report, loss of a laptop, mobile device, or

removable media containing PII, accidental email of PII, possible virus, or malware infection of a computer containing PII.

8. ENFORCEMENT

Violation of this procedure could be reported to the appropriate supervisor and could be subject to potential disciplinary action– up to and including termination.

9. RECORD DISPOSAL

- Records containing PII data are to be disposed so as to prevent inadvertent compromise of data. Paper records are disposed by shredding or other approved methods.
- The disposal method will render all PII data unrecognizable and beyond reconstruction.

10. POLICY REVIEW

This policy shall be reviewed by the Committee/Board as and when any changes are to be made to the policy or at such intervals as may be considered necessary to ensure compliance with any regulatory or statutory requirement from time to time. Any changes or modifications to the policy as recommended by the committee shall be presented to the board for their approval.

Version Control

Sr. No.	Version Control No.	Date created/ updated
1.	Version 1	April 21, 2022
2.	Version 2	October 31, 2023
3.	Version 3	March 21, 2024
4.	Version 4	March 21, 2025
5.	Version 5	October 16, 2025