# BHANIX FINANCE AND INVESTMENT LIMITED

# DATA PRIVACY POLICY

| Board Approval Date | Prepared by | Reviewed By | Version No | Last Review Date |
|---|---|---|---|---|
| May 26, 2026 | Head of Technology | Chief Executive Officer (CEO) | 6 | June 30, 2025 |

Table of Contents

## 1. PURPOSE

Bhanix Finance and Investment Limited (hereafter referred to as 'the Company') is a public limited company registered under the Companies Act 2013 and licensed as a Non-Deposit Taking Non-Banking Financial Company Base Layer (NBFC-ND-BL) by the Reserve Bank of India (''RBI'') as per Master Direction – Reserve Bank of India (Non-Banking Financial Companies – Registration, Exemptions and Framework for Scale Based Regulation) Directions, 2025.

The Board of Directors of the Company has adopted the Data Privacy Policy to maintain the privacy of and protect the sensitive business data and personal information of employees, contractors, vendors, and customers of BFIL and ensure compliance with laws and regulations.

This Privacy Policy explains about the type of information of the User that Bhanix collects, its purpose, its salient features etc. as detailed below. By using our website/application and by availing various products/services from Bhanix, the User consents to the terms of this Privacy policy ("Privacy Policy") in addition to the terms of use of the mobile application, website and product documents. We encourage User to read this Privacy Policy regarding the collection, use, and disclosure of information by the User from time to time to keep itself updated with the changes & updates that we make to this Policy.

## 2. SCOPE

This policy is applicable to all BFIL employees, all customer data, personnel data, or other company data defined as sensitive according to the Data Classification Policy of BFIL. It applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with company IT services is also subjected to this policy. In particular, this policy applies to partners, suppliers, stakeholders and other associated entities.

## 3. SALIENT FEATURES

- Bhanix respects the privacy of user in accordance with prevailing Law/regulation that governs privacy and always strives to uphold the standards in protecting the same.
- Bhanix may use the information to enhance the User's experience and may make subsequent offers to the User about its products/services.

Excepting with its associates and its subsidiaries, the information shall not be shared with any external organization unless the same is necessary to enable Bhanix to provide you services, meet legal and/or regulatory compliance requirement and/or to enable the completion of a transaction, rendition of services, pursuant to applicable norms/process or pursuant to the terms and conditions applicable to such Information as agreed with Bhanix.

## 4. DATA PRIVACY POLICY

1. DEFINITIONS

For the purpose of this Privacy Policy (hereinafter referred to as the "Policy"), wherever the context so requires:

a) The term 'Company' shall mean 'BHANIX FINANCE AND INVESTMENTS LIMITED' a private limited company limited by shares and registered under the Companies Act, 2013 and having its registered office at 5th Floor, Paville House, Off Veer Savarkar Marg, Prabhadevi Mumbai –400025, Maharashtra. The Company is the exclusive licensee in Indian Territory of the website and App.

b) The term 'website' shall mean www.cashe.co.in. "App" shall mean CASHe mobile application platform, and any other application or software run under the brand name "CASHe". CASHe is owned by TSLC PTE Ltd, a Singapore-based company, which has licensed CASHe mobile application to the Company for perpetual and exclusive use in India. In turn, the Company has sublicensed CASHe mobile application to its wholly owned subsidiary, Bhanix Finance and Investment Limited (hereinafter referred to as 'Bhanix' or 'Lender'), which is an RBI registered NBFC. Activities including digital lending are undertaken via the Append this App may be used by other NBFCs as well and the App, and other activities including promotional activities may be undertaken via the App in the future.

c) The term 'You', 'Your' & 'User' shall mean any legal person or entity accessing or using the services provided on this Website and/or the App, who is competent to enter into binding contracts, as per the provisions of the Indian Contract Act, 1872.

d) The terms 'We', 'Us'& 'Our' shall mean the website/domain/append/or Bhanix and the Company (collectively referred to as the "Platform"), as the context so requires. This Policy will be applicable to the Company to the extent applicable under the IT (RSP) Rules (defined hereinafter) and the DLG Guidelines to the extent applicable.

2. GENERAL

a) We are committed to safeguarding your privacy and ensuring that you continue to trust us with your personal data. When you interact with us you may share personal information with us which allows identification of you as an individual. This is known as personal data.

b) This document is an electronic record in terms of Information Technology Act, 2000 and rules there under as applicable and the amended provisions pertaining to electronic records in various statutes as amended by the Information Technology Act, 2000. This electronic record is generated by a computer system and does not require any physical or digital signatures. This document is published in accordance with the provisions of Rule 3 (1) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("Intermediary Rules") that require publishing the rules and regulations, privacy Policy and Terms of Use for access or usage of the Platform. This website is owned and operated by the Company. We confirm that our privacy Policy is compliant with applicable laws, associated regulations and RBI guidelines.

c) Various non-banking financial institutions are responsible for the loan and other facilities provided through the App. You acknowledge that such non-banking financial institutions, as per the Reserve Bank of India's ("RBI") guidelines, will be responsible for their respective contents displayed on the App, loan and other facilities offered. Bhanix reserves the right, subject to prevailing RBI guidelines, in its sole discretion to remove any content or data, information or material from the App from time to time.

d) We shall periodically inform its users, at least once every year, that in case of non- compliance with rules and regulations, privacy Policy or user agreement for access or usage of the computer resource. We shall also periodically, and at least once in a year, inform its users of its rules and regulations, privacy policy or user agreement or any change in the rules and regulations, privacy Policy or user agreement, as the case may be. When we collect information from a user for registration on the computer resource, it shall retain his information for a period of 180 (one hundred and eighty days) after any cancellation or withdrawal of his registration.

Please do not host, display, upload, modify, publish, transmit, store, update or share any information on the Platform: (i) belongs to another person and to which the user does not have any right; (ii) is defamatory, obscene, pornographic, paedophilic, invasive of other's privacy including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force; (iii) is harmful to child; (iv) infringes any patent, trademark, copyright or other proprietary rights; (v) violates any law for the time being in force; (vi) deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact; (vii) impersonates another person; (viii) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation; (ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource; (x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person.

3. SCOPE AND ACCEPTANCE OF THIS PRIVACY POLICY

a) This Policy applies to the personal data and the sensitive personal data that we collect about you for the purposes of providing you with our services. Personal data or information as used in this Policy shall include sensitive personal data or information, as applicable. This Policy is formulated under the Information Technology Act 2000, the IT (RSP) Rules (defined hereinafter) and the Guidelines on Digital Lending issued by the Reserve Bank of India dated 2 September 2022("DLG Guidelines").

b) By using this website or by giving us your personal data and sensitive personal data, you accept the practices described in this Policy, its contents, and have provided your informed consent to us collecting, storing, processing, transferring and sharing your Personal Information with lenders, partners, service providers for the purposes set out in this Policy. If you do not agree to this Privacy Policy, please do not use this website or give us any personal data or sensitive personal data.

c) We reserve the right to change this Policy without prior notice. We encourage you to regularly review this policy to ensure that you are aware of any changes and how your personal data may be used.

d) Please note that this App also deals with activities part from digital lending as covered under the DLG Guidelines. Please note that with respect to digital lending under the DLG Guidelines, the following shall be applicable to the Company, Bhanix and the App: Company, Bhanix and the App shall ensure that lending service provider/App engaged by it do not store personal information of borrowers except some basic minimal data (viz., name, address, contact details of the customer, etc.) that may be required to carry out their operations. A one-time access can be taken for camera, microphone, location or any other facility necessary for the purpose of on-boarding/KYC requirements only, with the explicit consent of the borrower. Please note that separately, the aspects pertaining to DLG Guidelines as mentioned in this Policy shall only be applicable with respect to digital lending undertaking by Bhanix/App. With respect to the DLG Guidelines, respective parties shall comply with the extant RBI guidelines in this respect.

## 4. DATA COLLECTED BY US

To create an account on the App or Bhanix's website, you must provide us with the basic details and information required as part of our Customer Identification process and you agree to our User Terms and Conditions and this Privacy Policy, which governs how we treat your information. App collects basic information required to provide customized services (for example: loan offers, content, more relevant ads), including your name, mailing address, postal code, job title, family details, employer details, phone number, PAN No., employment information, salary slips, declarations, your description and details in your account, financial information such as bank account etc. Such data is stored in our systems in accordance with Rule 3(h) of the Intermediary Rules and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("IT RSP Rules").

You will register with us using your Facebook or LinkedIn account or Google identity or any other third-party website mentioned on our Platform ("Third Party Sites"). You understand that, by creating an account or by registering through Third Party Sites, we and others will be able to identify you by your profile. We will also not be liable for the photographs and data that the users might upload, which are not in accordance with applicable law. We will ask for your bank account details only for the service provided by us. Such data is stored in our systems in accordance with Rule 3(h) of the Intermediary Rules and the IT RSP Rules.

All the information that you shall provide us is voluntary, including sensitive personal information. You understand that we may use certain information of yours, which has been designated as 'sensitive personal data or information' under the IT RSP Rules for the purpose of providing you the services and for sharing the information only with affiliates such persons who are identified in this Privacy Policy who are subject to this Privacy Policy, as will be explained further below.

Please note that we always ask for your permission before accessing the information on your phone. All messages are collected to ascertain the nature of the transaction. However, we store only your financial transaction SMS, names of transacting parties, transaction description and amount to perform a credit risk assessment. Such data is stored in our systems in accordance with Rule 3(h) of the Intermediary Rules and the IT RSP Rules. No personal SMS data is stored. All information requested is relevant to create a credit score which helps us make faster credit disbursals and better credit limits. You may choose not to provide the information requested. However, your credit score may be inaccurate or unavailable for your application as a result.

We hereby confirm that we do not store your personal information, except the following personal information provided in Clause 4.1 of the Policy which is necessary to carry out our business operations which may be shared with third parties. The App does not store personal information of borrowers/users except some basic minimal data (viz., name, address, contact details of the customer, etc.) that may be required to carry out business operations.

We may collect data about you from a variety of sources, including through:

a) Online and electronic interactions with us, including via the website, mobile applications, text messaging programs or through our pages on third party social networks.

b) Your interaction with online targeted content (such as advertisements) that we or service providers on our behalf provide to you via third party websites and/or applications.

4.1 DATA THAT YOU PROVIDE US DIRECTLY

This includes the types of personal or sensitive personal data that you provide us, in addition to the data mentioned in Section 4 above, with your consent for a specified purpose of providing you the services as mentioned in the Platform, including the following, under Rule 3 of the IT RSP Rules.

Some of these may be regarded as sensitive personal data or information under Rule 3 of the IT RSP Rules. We shall use the information collected by us only for the purpose for which it has been collected, for a specified purpose of providing you the services as mentioned in the Platform.

a) Personal contact information, including any information allowing us to contact you in person. It would include, but is not limited to, users' KYC details, borrowers'/users' academic information and documents, co-borrowers/users' financial documents, etc.

b) Demographic information, including date of birth, age, gender, location. We may also collect the location data, if enabled by you to do so. Geolocation includes country of access, IP address, etc.

c) User image, for us to cross check and verify the authenticity of the User and for prevention of fraud.

d) Account login information including any information that is required for you to establish a user account with us. (e.g. login ID/ email, user name, password and security question/answer);

e) Consumer feedback, including information that you share with us about your experience in using our services (e.g. your comments and suggestions, testimonials and other feedback)

f) We may collect the Usage data, including but not limited to access date and time, platform features and/or pages viewed, type of browser, hardware models, operating systems and versions, software, mobile network data, etc.

g) The data collected, as mentioned above, is solely restricted to the above-mentioned activities and will not be in further used for any other purpose. In case we use the data for any other purpose, explicit consent shall be taken from the customers.

h) We will desist from accessing mobile phone resources like file and media, contact list, call logs, telephony functions from user phone resources.

i) We will ensure that access to camera, microphone, location or any other facility necessary for the purpose of on-boarding/ KYC requirements and only with the explicit consent of the user.

j) We will ensure that biometric data is stored/collected in the systems, only in accordance with applicable law and the IT RSP Rules.

k) We will ensure that all data is stored only in servers located within India, while ensuring compliance with statutory obligations/ regulatory instructions.

l) You are provided with an option to give or deny consent for use of specific data, restrict disclosure to third parties, data retention, revoke consent already granted to collect personal data and if required, make the App (as defined under the DLG Guidelines) delete/forget the data. In case of withdrawal or modification of your consent or your amendment of any of your choices in this regard, we reserve the option not to provide the services or modify the services provided to you for which such information was sought.

4.2 DATA WE COLLECT WHEN YOU VISIT OUR PLATFORM

APP Permissions

SMS Permission: We will request permission to view all SMS messages and identify financial transactions only in order to determine your income and expense profile. Bhanix and/ or the App will only store financial SMSs sent by 6- digit alphanumeric senders from the inbox which helps us identify the various accounts held by the user and to help perform an optimal 'credit risk assessment' of the user.

The data is accessed by our machine learning models only. We will only access those messages that are relevant to this purpose and will not read / store/share irrelevant or personal messages in any form or manner. The permission is voluntary and can be revoked at any time. However, denying access may lead to an inaccurate assessment of the user's credit assessment on the platform. The data accessed by the said permission is stored in our systems in accordance with Rule 3(h) of the Intermediary Rules and the IT RSP Rules.

Phone Permission: Collect and monitor specific information about your device including your hardware model, operating system and version, unique device identifiers like IMEI and serial number, user profile information and mobile network information to uniquely identify the devices and ensure that unauthorized devices are not able to act on your behalf to prevent frauds. The data accessed by the said permission is stored in our systems in accordance with Rule 3(h) of the Intermediary Rules and the IT RSP Rules.

Contact: We do not collect or store contact information. However, we request the users to provide us with contact references for the purpose of filling the reference details screen during the loan application stage. The data accessed by the said permission is stored in our systems in accordance with Rule 3(h) of the Intermediary Rules and the IT RSP Rules.

Location Permission: Bhanix and/or the App will request permission to capture the user's location for verification, risk analysis and operational purposes. The user's location will enable Bhanix and/ or the App to verify addresses, determine serviceability and expedite the KYC process. The data accessed by the said permission is stored in our systems in accordance with Rule 3(h) of the Intermediary Rules and the IT RSP Rules.

Apps Permission: Collect and monitor a list of installed apps on your device for credit profile enrichment Accounts Permissions Collect and monitor the list of accounts on your device for credit profile enrichment. The data accessed by the said permission is stored in our systems in accordance with Rule 3(h) of the Intermediary Rules and the IT RSP Rules.

Information Collection and Use

For a better experience, while using our service, we may require you to provide us with certain personally identifiable information, including but not limited to User info. The information that we request will be retained by us and used as described in this privacy policy.

The app does use third party services that may collect information used to identify you.

Certain third-party providers' services are used by the App including the following: (i) Google; (ii) Facebook; (iii) IOs/ Apple, (iv) LinkedIn etc.

Log Data

We want to inform you that whenever you use our service, in a case of an error in the app we collect data and information
(through third party products) on your phone called Log Data. This Log Data may include information such as your device Internet Protocol("IP") address, device name, operating system version, the configuration of the app when utilizing our service, the time and date of your use of the service, and other statistics.

Cookies

Cookies are files with a small amount of data that are commonly used as anonymous unique identifiers. These are sent to your browser from the websites that you visit and are stored on your device's internal memory.

We may set cookies to track your usage on our web application platforms. We use data collection devices such as "cookies" on certain pages of the App and Website to help analyze our web page flow, measure promotional effectiveness, and promote trust and safety.

These are used to enhance your experience with our App. We use cookies to help us identify who you are, so your login experience is smooth each time. Cookies also allow us to collect Non-Personally Identifiable Information from you, like which pages you visited and what links you clicked on. Use of this information helps us to create a more user-friendly experience for all visitors. In addition, we may use Third Party Advertising Companies to display advertisements on our App. By using the app, you signify your consent to our use of cookies.

Please note that if you decline or delete these cookies, some parts of the App may not work properly.

Service Providers

We may employ third-party companies and individuals due to the following reasons:

- To facilitate our service.
- To provide the service on our behalf.
- To perform service-related services; or
- To assist us in analyzing how our service is used.

We want to inform users of this service that these third parties have access to your personal information. The reason is to perform the tasks assigned to them on our behalf. However, they are obligated not to disclose or use the information for any other purpose.

Security

We value your trust in providing us your Personal Information, thus we are striving to use commercially acceptable means of protecting it. But remember that no method of transmission over the internet, or method of electronic storage is 100% secure and reliable, and we cannot guarantee its absolute security.

You can access your personal identity details on our App through your login and password. We recommend that you do not share your password with anyone. In addition, your personal details are stored on a secure server located in India that only selected personnel contractors and authorised Agencies have access to on a need- to- know basis. We encrypt certain sensitive information using Secure Socket Layer (SSL) technology to ensure that your personal details are safe as it is transmitted to us.

Protection of your privacy and your data security is a top priority for us. We encrypt your data and store it in multiple databases. There are security group and firewall checks to control the APIs with multi-level authentication, authorisation and verifications.

However, you understand and accept no data transmission over the Internet can be guaranteed to be completely secure. We cannot ensure or warrant the security of any information that you transmit to us and you do so at your own risk. Data pilferage due to unauthorized hacking, virus attacks, technical is possible and we take no liabilities or responsibilities for it, except to the extent permitted in law. In case such security breach happens, we take the following steps as mentioned in Para 10 of this Policy.

Links to Other Sites

This service may contain links to other sites. If you click on a third-party link, you will be directed to that site. Note that these external sites are not operated by us. Therefore, we strongly advise you to review the Privacy Policy of these websites. We have no control over and assume no responsibility for the content, privacy policies, or practices of any third-party sites or services.

4.3 DATA THAT CAN BE STORED

The Company collects and stores only the following categories of customer data, strictly limited to what is necessary for business operations:

Personal & Identity Data

- Name, date of birth, gender, photograph
- KYC documents (PAN, Aadhaar, officially valid documents)
- Contact details (address, email, mobile number)

Financial Data

- Bank account details (collected only for service provision)

- Salary slips, bank statements
- Credit bureau / CIBIL data
- Transaction data

Device & Technical Data

- Device identifiers (IMEI, serial number, hardware model, OS version)
- IP address, log data, usage data
- Financial transaction SMS (6-digit alphanumeric senders only; no personal SMS stored)

Location Data

- Collected one-time, only for KYC verification, address confirmation, and serviceability checks

App Permission Data

- Camera/microphone: one-time, for KYC/onboarding only, with explicit consent
- Installed apps list: for credit profile enrichment only

The Company explicitly does not store: personal SMS, contact lists, call logs, biometric data (unless mandated by applicable law), or any data accessed without prior explicit user consent.

All data is stored exclusively on servers located within India

5. DIVULGING/SHARING OF PERSONAL INFORMATION

a) We may share your personal information with other corporate entities and affiliates to help detect and prevent identity theft, fraud and other potentially illegal acts; correlate related or multiple accounts to prevent abuse of our services, to facilitate joint or co-branded services, where such services are provided by more than one corporate entity, or if required to do so in course of our business operations. The third parties to whom your data may be disclosed shall not disclose the data further.

b) We may disclose personal information if required to do so by law or if we in good faith believe that such disclosure is reasonably necessary to respond to subpoenas, court-orders, or other legal processes.

c) If we are involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy. Business Transfers: As we continue to develop our business, we might sell or buy business units. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any preexisting Privacy Policy (unless, of course, the customer consents otherwise). Also, in the unlikely event that Bhanix's or the Company's India's assets or substantially all of its assets are acquired, customer information maybe one of the transferred assets.

d) Third party service providers: We may employ other companies and individuals, call centres, payment gateways, banks to perform functions on our behalf. Examples include delivering e-mail, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links) and providing customer service. They have access to personal information needed to perform their functions but may not use it for other purposes. Further, they must process the personal information in accordance with this Privacy Policy and as permitted by applicable law.

e) Protection of App: We release personal information when we believe, release is appropriate to comply with the law; enforce or apply our User Terms and Conditions and other agreements; or protect the rights, property or safety of App, our users or others. This includes exchanging information with other companies, organizations, government or regulatory authorities for fraud protection and credit risk reduction.

6. USE OF PERSONAL INFORMATION

We and our affiliated partners may use the personal information submitted by you to contact you in relation to the services offered. This shall override any calling preferences, which you may have registered in the NDNC.

7. SECURITY

Transactions on the Website are secure and protected. Any information entered by the User when transacting on the Website is encrypted to protect the User against unintentional disclosure to third parties. The User's credit and debit card information is not received, stored by or retained by the Company / Website in any manner. This information is supplied by the User directly to the relevant payment gateway, which is authorized to handle the information provided, and is compliant with the regulations and requirements of various banks and institutions and payment franchisees that it is associated with.

8. THIRD PARTY ADVERTISEMENTS / PROMOTIONS

We use third-party advertising companies to serve ads to the users of the Website. These companies may use information relating to the User's visits to the Website and other websites in order to provide customised advertisements to the User. Furthermore, the Website may contain links to other websites that may collect personally identifiable information about the ser. The Company/Website is not responsible for the privacy practices or the content of any of the aforementioned linked websites, and the User expressly acknowledges the same and agrees that any and all risks associated will be borne entirely by the User. We strongly advise you to review the privacy policy of every site you visit.

9. DATA PROTECTION OFFICER AND GRIEVANCE REDRESSAL OFFICER

If you have any complaint under the Information Technology Act 2000, the IT RSP Rules or any FinTech/ digital lending related complaints/issues, the contact details of the Data Protection Officer and Grievance Redressal Officer are provided below.

The Data Protection and Grievance Redressal Officer should acknowledge the complaint within 24 (twenty-four) hours and dispose of such complaint within a period of 15 (fifteen) days from the date of its receipt.

Ms. Pushpinder Kaur
Indiana Business Centre, 5th Floor, "B" Wing,
Makwana Road, Off M. Vassanji Road, Marol Naka,
Andheri (E), Mumbai – 400059
Phone number: 022-46047350.
E-Mail ID: Grievance@bhanix.in

10. DATA SECURITY & RETENTION

10.1 DATA SECURITY

In order to keep your personal data secure, we have implemented a number of security measures including:

We value your Personal Information, and protect it on the Platform against loss, misuse or alteration by taking extensive security measures. In order to protect your Personal Information, we have implemented adequate technology and will update these measures as new technology becomes available, as appropriate. All Personal Information is securely stored on a secure cloud setup and all communication happens via secure SSL communication channels.

You are responsible for all actions that take place under your User Account. If you choose to share your User Account details and password or any Personal Information with third parties, you are solely responsible for the same. If you lose control of your User Account, you may lose substantial control over your Personal Information and may be subject to legally binding actions.

No data collected and allowed to be stored by us shall be stored in any server which is not located in India.

Standards for handling security breach:

(i) All suspected or reported security breaches or violations shall be logged and tracked from initiation of the preliminary analysis to determine whether there was a security breach or violation till completion of actions taken.

(ii) Appropriate contacts with relevant authorities shall be maintained to escalate to respective authorities as required, including the local cyber cell information.

(iii) Below mentioned are the steps for handling security breach:

- Move quickly to secure the systems and fix vulnerabilities that may have caused the breach.
- Switch off the servers and change the access code to prevent additional data loss.
- Mobilize the breach response team right away to prevent additional data loss.
- Additional security required will be placed.
- Securely delete personally identifiable information (PII) and other sensitive data when it no longer needed for business purposes.

(iv) if any security breach comes to our knowledge, then we may take all steps required to protect misuse of such information and may attempt to notify you electronically so that you can take appropriate steps.

(v) As per the Indian Computer Emergency Response Team ("CERT-In") cyber-security directions under Section 70B (6) of the Information Technology Act, 2000 (CERT Directions), we shall report cyber incidents (as mentioned in Annexure I of the CERT Directions) within 6 (six) hours of noticing such incidents or being brought to notice about such incidents. For incidents not covered herein, we shall report cyber security incidents within a reasonable time of occurrence or noticing the incident to have scope for timely action under Rule 12(1)(a) of the CERT Rules, any entity affected by cyber-security incidents should. We shall report the cyber security incidents if they arise to: CERT- In via an email (incident@cert- in.org.in), Phone (1800-11-4949) and Fax (1800-116969). We shall comply with the Information Technology Act 2000 and the rules thereunder with respect to the applicable cyber security standards.

10.2 RETENTION & DATA PURGING

We will only retain your personal data for as long as it is necessary for the stated purpose, taking into account also our need to answer queries or resolve problems, provide improved and new services, and comply with legal requirements under applicable laws. This means that we may retain your personal data for a reasonable period after your last interaction with us. Kindly note that we do not sell your personal data to any third party and the use of your personal data is strictly restricted to the services provided by us, as mentioned herein. Your data will be stored in our systems in accordance with the Information Technology Act, 2000, Rule 3(h) of the Intermediary Rules and the IT RSP Rules ("IT RSP Rules").

When there is no longer a business, legal, or regulatory requirement to keep the data, then the data will be purged in a secure manner.

Data Destruction Protocol :

Trigger for Destruction : Data is destroyed when there is no longer a business, legal, or regulatory requirement to retain it, or upon a valid customer account deletion request (subject to eligibility criteria).

Retention Periods Before Destruction

All data and information collected, processed, stored, or generated pursuant to the provision of services shall be retained for a period of 10 (ten) years from the date of collection, termination of relationship, closure of account, or completion of the relevant transaction or service.

Exemptions from Destruction: Data shall be retained beyond the standard period if:

- Required by an active court order, tribunal direction, or regulatory investigation
- The account is classified as fraud or defaulter, or is under active recovery
- Retention is required for audit, statutory, or tax compliance

Destruction MethodsDigital Data:

- Cryptographic erasure (preferred for cloud-stored data)

- Secure overwriting
- Full purging of databases including backups, replicated copies, and archive snapshots

Physical/Offline Media:

- Paper records: cross-cut shredding
- Magnetic media: degaussing followed by physical destruction
- CDs, DVDs, USB drives, SSDs: physical destruction via certified e-waste vendor under E-Waste (Management) Rules, 2022

Third-Party / Cloud Data:

- Formal written destruction instruction issued to processor upon contract termination or retention expiry
- Certificate of Data Destruction obtained from vendor confirming method, scope, and date
- Third-party contracts mandate destruction standards equivalent to this Policy

Account Deletion Process : Upon a valid customer deletion request, the account is deleted on the 30th day from submission. Authentication credentials, active sessions, access tokens, and app permissions are immediately revoked. Regulatory data (KYC, loan history, transaction history) is retained as required under applicable law notwithstanding account deletion.

Documentation & Audit : All destruction exercises are recorded in a Data Destruction Register maintained by the IT Security Team, reviewed by the Data Protection Officer periodically, and available to auditors upon request.

Scope of Data Deletion & Retention

When a user's account deletion request is successfully submitted, the following details shall be deleted from our database:

- All stored passwords, MPINs, access tokens, refresh tokens and any other authentication credentials associated with the user's account.
- Any active session data will be cleared, and users will be logged out from all devices and platforms.
- All permissions previously granted to the CASHe App/Web platform will be revoked.
- The user shall be opted out of all communication channels.

However, for regulatory and legal compliance reasons, other details related to the user's account, including user-submitted data, loan history, transaction history, investment history, KYC and CIBIL data shall be retained as per regulatory guidelines.

10.3 RESTRICTIONS ON USE OF DATA

The Company operates under the following clear restrictions governing data use:

Purpose Limitation : Data collected is used solely for the purpose for which it was collected. It shall not be used for any other purpose without obtaining fresh explicit consent from the customer.

Third-Party Sharing Restrictions : Customer data is shared only with:

- Affiliates and group entities for fraud detection and service delivery
- RBI-registered lending partners bound by contractual confidentiality obligations
- Regulated third-party service providers (payment gateways, credit bureaus, KYC validators) under data processing agreements
- Regulatory/judicial authorities when legally mandated

Data is not sold, rented, or leased to any third party under any circumstances.

Lending Service Provider (LSP) / DLA Restrictions : In line with RBI DLG Guidelines, LSPs and DLAs engaged by the Company are prohibited from storing personal information of borrowers beyond basic minimal data (name, address, contact details) required for their operations.

Employee Access Restrictions : Access to customer data is governed by Role-Based Access Control (RBAC) and the principle of least privilege. Only personnel with a documented business need and senior management approval may access sensitive or restricted data.

Prohibition on Sensitive Resource Access : The Company does not access file/media storage, contact lists, call logs, or telephony functions from user devices. Camera, microphone, and location are accessed one-time, solely for onboarding/KYC, with explicit consent.

11. YOUR RIGHTS

As per the applicable data protection law, your principal rights are as follows. Please read this in in conjunction with the Policy, specifically Clause 4.1:

Right to withdraw consent: You have the option, at any time while availing our Services or otherwise, to withdraw your consent given to us, for processing your data. In case of withdrawal of your consent, we reserve the option not to provide the Services for which such information was sought. In case the Services are already availed and then you raise a request to withdraw consent, then we have the right to retain to stop the provision of the Services.

You have the right to exercise any of the above rights by contacting our Data Protection Officer(“DPO”) as mentioned under Clause 9 of this Policy. Once we receive your request and verify the same satisfactorily, we shall proceed with assisting you on your request.

12. APPLICABLE LAWS & DISPUTE RESOLUTION

Any controversy or claim arising out of or relating to this policy shall be decided by Arbitration in accordance with the Arbitration and Conciliation Act 1996 and the governing law shall be the laws of India. The Arbitral Tribunal shall consist of one arbitrator who shall be appointed in accordance with the Arbitration and Conciliation Act 1996.Any such controversy or claim shall be arbitrated on an individual basis and shall not be consolidated in any arbitration with any claim or controversy of any other party. Any other dispute or disagreement of a legal nature will also be decided in

accordance with the laws of India, and the Courts at Mumbai shall have exclusive jurisdiction in all such cases, subject to the foregoing.

13. REGULAR REVIEW OF PRIVACY POLICY

We keep our Policy under regular review and may update the same to reflect changes to our information related practices. We encourage you to periodically review this page for the latest information on our privacy practices, your continued use and access of our platform will be taken as acceptance of the updated policy.

## 5. PRIVACY PRINCIPLES

This Policy describes generally acceptable privacy principles for the protection and appropriate use of personal information at BFIL. These principles shall govern the use, collection, disposal and transfer of sensitive and personal information.
The key data privacy principles are:

- Data Minimization - Ensure that you are asking sensitive/personal data that you truly need and nothing more.
- Storage Limitation - Ensure that you do not keep sensitive/personal data for longer than you need it.
- Accountability - You must have appropriate measures and records in place to be able to demonstrate your compliance.
- Integrity and confidentiality - Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organisational and technical measures to prevent unauthorised access, illegal processing, or distribution, as well as accidental loss, modification or destruction.
- Restrictions to a specific purpose- Personal data can be processed only for the purpose that was defined before the data was collected. Personal data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes. Subsequent changes to the purpose are only possible to a limited extent and require justification.
- Data Anonymization - The organization shall implement data anonymization techniques where feasible to irreversibly remove personal identifiers from datasets, ensuring that individuals cannot be identified directly or indirectly. Anonymized data shall be treated as non-personal data and may be used for statistical, research, or analytical purposes in compliance with applicable laws and internal governance standards.
- Data Pseudonymization - Where full anonymization is not practical, the organization shall apply pseudonymization measures to reduce the identifiability of personal data. Pseudonymized data shall be stored separately from additional information that could re-identify individuals, and access to such linking information shall be strictly controlled and monitored.

## 6. APPLICATION AND INFORMATION ACCESS

All company staff and contractors shall be granted access to the data and applications required for their job roles on a need basis. Access control applies to all networks, servers, workstations, laptops, mobile devices, web applications and websites, cloud storages, and services.

All company staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from higher management. Sensitive systems shall be physically or logically isolated to restrict access to authorized personnel only.

## 7. ACCESS TO CONFIDENTIAL, RESTRICTED INFORMATION

- Access to data classified as 'Confidential' or 'Restricted' shall be limited to authorized persons whose job responsibilities require it and as approved by the higher/senior management.
- The responsibility to implement access restrictions lies with the IT Security department.
- Bhanix has reasonable management, technical and administrative measures in place to protect information within Bhanix.

## 8. ACCESS CONTROL AUTHORIZATION

- Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions and access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

- Role-based Access Control (RBAC) shall be used to secure access to all file-based resources in Active Directory domains.

- The use of shared identities shall be permitted only where they are suitable, such as training accounts or service accounts.

## 9. NETWORK ACCESS:

- All employees and contractors shall be given network access in accordance with business access control procedures and the least-privilege principle.
- All staff and contractors who have remote access to company networks shall be authenticated using the VPN authentication mechanism only. Two-factor authentication should also be evaluated
- Segregation of networks shall be implemented as recommended by the company's network security assessment. Network administrators shall group together information services, users, and information systems as appropriate to achieve the required/adequate segregation.

- Network routing controls Shall be implemented to support the access control policy.

## 10. USER RESPONSIBILITIES

- All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.
- All users must keep their workplace clear of any sensitive or confidential information when they leave.
- All users must keep their passwords confidential and should not share them.
- Bhanix will not be liable / responsible for any breach of privacy owing to Users negligence.
- User shall only use the official application/website/links of Bhanix for availing product/services by inputting the domain information on the address bar. User is completely aware of the potential risk of data/privacy breach and User shall be solely liable for any unauthorized disclosure/ breach of personal/ sensitive personal information etc. and any direct/ indirect loss suffered by User due to User's conduct. Hence, User shall exercise utmost caution to ensure that User's personal data/ Sensitive personal data (including but not limited to any passwords, financial information, account details, etc.) are not shared/stored/made accessible through any physical means with or without User's knowledge (disclosure to any person/third-party etc.) or through any electronic mode.

## 11. RETENTION OF INFORMATION

Bhanix may retain User's Information if it is required to provide services or as long as it is required for business purposes. Retention of Information will be as per applicable law/regulatory requirements in India.
Information may be retained for an extended period:

- In case of requirement of any investigations under law or as part of any requirement before Courts/Tribunals/Forums/Commissions etc and
- To enhance/improvise the products /services of Bhanix.

By agreeing to avail of the services offered by Bhanix, the User's agrees to the collection and use of their Sensitive Personal Data or Information by Bhanix. The user always has the right to refuse or withdraw their consent to share/disseminate their Sensitive Personal Data or Information by contacting customer care. However, in the event of the User's refusal or withdrawal of personal data, the User shall not be able to avail of any services of Bhanix to the fullest extent.

## 12. ACCOUNT DELETION/DEACTIVATION

Bhanix allows users to request for their account to be deleted/deactivated from the respective Digital Lending App (DLA) with an option to initiate an app account deletion/deactivation request.

Bhanix deletes the user data associated with that app account of the User subject to the retention policy and retention of information clause as above.

## 13. ENFORCEMENT

Any user found in violation of this policy is subject to disciplinary action– up to and including termination of employment. Any third-party partner or contractor found in violation may have their network connection terminated.

## 14. POLICY REFERNCE

- Data Classification Policy
- Password Policy
- Cyber Security Policy
- Information Security Policy
- Data Integrity, Accuracy and Completeness Policy

## 15. POLICY REVIEW

This Policy shall be reviewed by the Committee/Board as and when any changes are to be made in 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 in or modifications to the Policy as recommended by the Committee shall be presented to the Board for approval.

## 16. POLICY EXCEPTION

Any exception to the policy needs to be approved by the CEO – Chief Executive Officer.

## 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 | February 28, 2024 |
| 4 | Version 4 | March 21, 2025 |
| 5 | Version 5 | June 30, 2025 |
| 6 | Version 6 | May 26,2026 |