DATA HANDLING AND PRIVACY POLICY

Of

CHAITANYA INDIA FIN CREDIT PRIVATE LIMITED

Document No	CIFCPL-INT-ISMS-DHP-PO1
Version No	1.1
Originally adopted Date of Policy	May 24, 2023
Date of approval of amendment	October 30, 2023
Policy owner	Information Technology Head
Approved by	Board of Directors
Signature	

DATA HANDLING AND PRIVACY POLICY

Document No: CIFCPL-INT-ISMS-DHP-P01

Version No: 1.0

Originally adopted date: 24-Feb-2023

OBJECTIVE

Our Data handling and privacy policy indicates that we are dedicated to and responsible for processing the information of our employees, customers, stakeholders, and other interested parties whoever it concerns with absolute caution and confidentiality. This policy describes how we collect, store, handle, and secure our data fairly, transparently, and with confidentiality. This policy ensures that CIFCPL follows good practices to protect the data gathered from its customers, employees, and stakeholders. The rules outlined in this document apply regardless of whether the data is stored electronically, on paper, or on any other storage device.

WHAT DATA IS COLLECTED

Chaitanya as Lender/Employer collects certain information, some of which is sensitive personal information. We have detailed what data and the manner in which this data is collected.

We collect the data provided to us to ensure the service is provided in the best manner possible. Chaitanya uses this data to underwrite/ assess the risk associated with the source(customer/employee). The data being asked, helps us to provide services in a robust and user-friendly manner. We have detailed the manner in which Chaitanya collect data below:

DATA CUSTOMERS/EMPLOYEES SHARE IN THE COURSE OF SIGNING UP/USING CIFCPL SERVICES

We and our affiliates or our authorized Agents collect the data when customers apply for a loan/application is received for employment.

- Identification Information like Name, gender, residential / correspondence address, telephone number, date of birth, marital status, email address, or other contact information.
- KYCs like Voter ID, PAN, Signature Photograph, etc.
- Bank account or other payment instrument details.
- Nature of employment, official employment email address, and name of employer, monthly income.
- Detail which may be required by us for providing services to customer or co-applicant/s if any.

We or our Lending Partner may require the customer/employee to share further information at a later date to confirm the veracity of the information or pursuant to any additional features.

Note: Customer/Employee terminology shall be used for both Potential as well as Onboarded.

OTHER DATA SOLICITED

Geolocation data: Chaitanya collects the location data wherever it is applicable pertaining to the nature of the requirement.

Personal Information data: Demographic, email addresses, mobile numbers, etc., may be collected from customers/employees to provide further information to Chaitanya for the purposes of processing loan/employment applications. Such additional information may include (without limitation) bank statements, goods and services tax returns, salary and income statements, and title documents for the property being financed. This data shall be supplied to our Affiliates or our Authorized Agents through us. Customer/Employee

may also be required to provide this information to us, via physical documents, e-mail or other digital and offline methods.

We may (subject to applicable law) also combine and link personal information with information we obtain from other sources. This could occur, for example, in circumstances where we receive New, Updated, or Additional information from customers/employees or our affiliates and Associates Partners. We may use the performance information we collect to analyze usage, habits, and further need for sourcing.

Information we receive from other sources: We may also be working closely with third parties (including, for example, credit information bureaus, business partners, partner banks and financial institutions, technical sub-contractors, analytics providers, search information providers, title deeds, property verification service providers and valuers) and may lawfully receive information about Customer/Employee and co-applicant (in-case customer for sourcing) from such sources. Such data may be shared internally and combined with data collected. We may also use the content which is shared publicly, including on third-party platforms or applications, to promote our Services (including by quoting Customer/Employee content, reviews, and/ or recommendations, or displaying screenshots of Customer/Employee content, reviews and/ or recommendations).

HOW DATA IS USED

We use personal information collected from Customer/Employee for various reasons, which includes the following

- To Loan Processing/employment consideration; KYC Authentication
- To Tell Customers/Employees about the products and services offered by us, our referral partners, our Affiliates, and our associate agents
- To respond to Customer/Employee queries, notify Customer/Employee of changes to our policies
- To provide Customers/Employees with information on the Products and Services, Employment.
- To Access Customer eligibility for the Microfinance Loan or to improve our existing products and services
- To conduct Surveys, Webinars, Podcasts, Teleconferences or Seminars, and Microfinance Programs by us or our affiliates and associate partners
- To any Legal Compliance and Requirements.

For enabling and servicing of our Affiliates or our Authorized Agents: Our Affiliates or our Authorized Agents use the data to analyze your creditworthiness, loan eligibility, KYC documents, current employment verification and, and the terms of loans. Customer/Employee hereby grants our Affiliates or our Authorized Agents explicit consent to fetch KYC (Know Your Customer) details from the Central KYC Records Registry using the details provided by Customer/Employee. Our Affiliates or our Authorized Agents also use the data for underwriting, to track disbursement and repayment of loan.

For Enabling Customer Support: We use the information to provide customer support, including to resolve concerns from the use of the Services, and train our customer service executives.

For Research and Development: We may use the data so collected for research, analysis, and product development to improve Customer/Employee Experience.- This also helps us develop automated actions to be triggered in certain events, such as when we need to identify if photographs uploaded are not clear, fraud takes place, IFSC is incorrect etc.

For Marketing and Outreach: We may use the data we collect to market our Services. This includes sharing Customer/Employee feedback, ratings and screen names for purely promotion and marketing purposes. Even if the name appears in the Do Not Call or Do Not Disturb Register, we may contact through e- mails, telephones, messages, SMS, WhatsApp or any other available modes for marketing schemes, various financial or investment products or any other aspect pertaining to any loan availed herewith.

For Legal Compliance and Requirements: We may use the data we collect to investigate or address claims or disputes relating to use of our Services, or as otherwise allowed by applicable law, or as requested by regulators, government entities, and official inquiries.

For Product Innovation: We may use the data we collect to offer new products and services.

Sharing with third parties: We work with third-party service providers to execute various functionalities and we may share your information with such service providers to help us provide required information.

Some of these functionalities may include:

- Analyzing transaction behavior and cash flows via Customer/Employee SMSs, bank statements, goods and services tax returns, salary and income statements, income tax returns, basis on which loan offer is generated.
- Validating and authenticating the official verification documents provided by Customer/Employee.
- E-signing of the loan agreement or sanction letter, populating the loan agreement or the sanction letter. The information shared with these service providers is retained for auditing of the agreements.
- eNACH set-up to enable autopay.
- Cloud services.
- Validating and authenticating employment status, employment information, and employment duration.

Third Party Services: Customer/Employee may connect with other websites, products, or services that we don't have control over (for example, if we allow payment through an external wallet facility then we will have to share your usage information with the facility provider). However, usage of such third-party services is subject to their privacy policies and not within our control. We recommend that Customer/Employee have a look at their privacy policies before agreeing to use their services.

Change in Control: While negotiating or in relation to a change of corporate control such as a restructuring, merger, or sale of our assets, we may have to disclose the databases and information we have stored in the course of our operations.

Sharing with the Co-Lending Partner: We work with identified banks and financial institutions to provide co-lending products in Chaitanya and we may share your information with such Co-Lending Partner(s).

Sharing with law enforcement when needed: If any governmental authority or law enforcement officers request or require any information, we think disclosure is required or appropriate in order to comply with laws, regulations, or a legal process.

HOW CUSTOMER/EMPLOYEE DATA IS PROTECTED

While none of the Customer/Employee data is sold, it is shared with third parties on a contractual basis. This data is shared for processing of information and ensuring that Customer/Employee receives the Services.

We are very protective of Customer/Employee data. We may enter into data-sharing agreements or disclose the collected data in order to provide the Services and new product offerings.

LINK TO THIRD-PARTY

We ensure that our third-party service provider takes security measures in order to protect personal information against loss, misuse or alteration of the data.

Our third-party service provider(s) employ separation of environments and segregation of duties and have strict role-based access control on a documented, authorized, need-to-use basis. The stored data is protected and stored by application-level encryption. They enforce key management services to limit access to data.

Furthermore, our registered third-party service provider(s) provide hosting security – they use industry-leading anti-virus, anti-malware, intrusion prevention systems, intrusion detection systems, file integrity monitoring, and application control solutions.

HOW WE WORK WITH OUR GROUP COMPANY

As part of our Policy, we (i.e., Chaitanya) and the Affiliates receive information from, and share information with each other. We may use the data we have collected for:

- Product research and development, marketing outreach and advertising relevant products;
- Tailoring product offerings for your benefit;
- Improving infrastructure and delivery systems of our services;
- Understanding and driving analytics on how our services are used;
- Promoting safety, security and integrity of our services, e.g., securing systems and fighting spam, threats, abuse, or infringement activities; and
- Improving our services, our Affiliates' services and Customer/Employee experiences using them, such as making suggestions for Customer/Employee, personalizing features and content, helping complete purchases and transactions.

GENERAL

Customer/Employee may reach out to the Grievance/HR dpt. to enquire about the treatment of Customer/Employee data. Customer/Employee may contact on any aspect of this policy or for any discrepancies/grievances with respect to the personal data, by writing to our grievance officer/HR representative.

WHAT IS CUSTOMER/EMPLOYEE RIGHT REGARDING THE DATA

We have identified Customer/Employee rights in the table below and the manner in which Customer/Employee may exercise these rights.

It is important for us that the Customer remains in control of the data. Customers can write to us at customer.care@chaitanyaindia.in if customer wish to exercise any of the rights under the Policy. Employee/Customer shall have the following rights:

Right to rectification: In the event that any personal data provided is inaccurate, incomplete, or outdated then the customer/employee shall have the right to provide us with the accurate, complete, and up-to-date data and have us rectify such data. It may take up to 10 days to process the request. We urge you to ensure data is accurate and correct for better use of our Services in an uninterrupted fashion.

Right to withdraw consent: Customer/Employee has the right to withdraw specific consents Customer/Employee has provided under this Policy by writing to us. However, if the Customer/Employee has availed any services/facilities or employment from Chaitanya or Affiliates or our Authorized Agents, we shall have the right to continue processing the information. However, we shall not retain the data and information if it is no longer required by us and there is no legal requirement to retain the same. Do note that multiple legal bases may exist in parallel, and we may still have to retain certain data and information at any time.

WHAT ARE OUR DATA SECURITY PRACTICES

We aspire to keep the data and information as secure as possible and to that effect, we have used state-of-the-art software.

We use requisite technical and organizational security measures to ensure a level of protection for personal data appropriate to the nature, scope, and purpose of processing personal data, the risks associated with such

processing, and the likelihood and severity of the harm that may result from such processing. The transfer of personal data between the Customer/Employee end device and us is carried out via best-in-class encryption protocols. If the Customer/Employee communicates with us by email, access by third parties cannot be ruled out. In the case of confidential information, we recommend using the mail, i.e., post or encrypted e-mail communication (PGP).

CONSENT MECHANISM

By applying for a loan/employment, Customer/Employee has consented to all our data privacy practices.

Customer/Employee agrees to processing, storage, usage, and sharing of the data provided pursuant to this Policy. By availing Services/facilities/employment in Chaitanya or Affiliates or our Authorized Agents, Customer/Employee hereby consent to our accessing your credit information from credit information companies to make personalized product offerings to Customer/Employee. If Customer/Employee does not agree with any of the terms of this Policy or the Terms or wish to revoke any consent Customer/Employee has provided to us, please write to us. However, please note that if Customer/Employee revokes any mandatory permissions or revokes the consent to process and store information such as Customer/Employee data, Financial and KYC Information, and/or any other information needed to facilitate Customer/Employee loan facility/employment, then we may have to cease the provision of Services to Customer/Employee. Customers/Employees cannot withdraw mandatory consents once they have availed services/loan facility/employment till they have closed all services/loan facility/employment with us and our Affiliates.

DATA RETENTION

We retain Customer/Employee personal data to the extent we need to. Once the legal basis for the retention expires, we will not hold onto it.

We shall retain the information provided to facilitate smooth and uninterrupted use and (i) to provide, improve, and personalize our Services; (ii) to contact Customers/Employees about their accounts and give customer service; (iii) to personalize our advertising and marketing communications; and (iv) to prevent, detect, mitigate, and investigate fraudulent or illegal activities. We do not retain personal data for longer than required for the purpose for which the information may be lawfully used. For any other information, we may entertain the Customer/Employee's request for deletion, however, the Customer/Employee may not be able to use our Services at all after such deletion.

Communications from Us: We may from time to time contact Customers/Employees via calls, SMS, emails, and other communication channels to provide you with information pertaining to Customer/Employee Services, notifications on updates vis-à-vis our Services (when we consider it necessary to do so), educational information and promotions.

Updates To This Notice: We may update this Policy as and when required. Use of our Services after an update constitutes consent to the updated notice to the extent permitted by law. Please take the time to periodically review this Policy for the latest information on our privacy practices.

PROCEDURE ELEMENT FOR INTERNAL OPERATION

As a key part of our operations, we gather and process any information or data that makes an individual identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, etc. This information is collected only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply to our company

Our data will be

- Be precise and consistently updated
- Is collected legitimately and with a clearly stated purpose
- Be processed by the company in line with its legal and ethical binds

- Have protection measure that protects it from any unauthorized or illegal access occurring by internal or external parties

Our data will not be

- Communicated informally
- Exceed the specified amount of time stored. Therefore, the personal data of employees, customers, and affiliates who no longer use CIFCPL services is stored in a secure area.
- Be transferred to organizations, states, or countries that do not acquire proper data protection policies
- Be spread to any party unless approved by the data's owner (except for the legitimate requests demanded from law enforcement authorities)

ROLES AND RESPONSIBILITIES

Everyone who works for or with CIFCPL is responsible for ensuring that the collection, storage, handling, and protection of data is being done appropriately. The internal contact person for any escalation or concern related to the data protection process is the Cyber Security Department which can be reached at Email: Cyber_security@chaitanyaindia.in.

In addition, the following departments have key areas of responsibility: -

- Providing oversight and continuous enhancement of cyber security awareness programs and improvements in risk management
- Collaborating and leading the design, implementation, operation, and maintenance of the Security Management System
- Ensuring periodic testing is conducted to evaluate the security posture by conducting periodic reviews to ensure compliance
- Leading the design and operation of related compliance monitoring and improvement activities to ensure compliance both with internal security policies, and applicable laws and regulations
- Developing and managing controls to ensure compliance with the wide variety and ever-changing requirements resulting from laws, standards, and regulations.

IT MANAGERS RESPONSIBILITIES

- Strictly complying with all CIFCPL policies related to non-disclosure, non-competition, and confidentiality of information
- Constantly staying up to date on various web technologies and tools
- Performing networking systems hardware and software upgrades, and installing security patches when needed.
- Checking and monitoring the general health of networks and networking devices.
- Performing daily system monitoring, verifying the integrity and availability of all hardware, server resources, systems, and key processes, reviewing system and application logs, and verifying completion of scheduled jobs such as backups.
- The implementation, configuration, and maintenance of computer networks, software, and digital security.
- Ensuring that access to the personnel data of members registered on the CIFCPL Website personnel is restricted only to authorized personnel.
- Ensuring that access to the personnel data of members registered on the CIFCPL website will not be shared with or provided to unauthorized personnel.

GENERAL GUIDELINES

- Access to data covered by this policy should be restricted only to those who need it for their work. Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- CIFCPL provides comprehensive training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the Data Storage guidelines specified below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorized people, either within the company or externally.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.
- HR has to take the signature from the employee related to the data handling and confidentiality clause at the time of joining

DATA STORAGE

These rules describe how and where data should be safely stored. When data is stored on paper, it should be kept in a secure place to mitigate unauthorized usage of documents. These guidelines also apply to data that is usually stored electronically but has been printed out for certain reasons,

- The paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people access them, such as on a printer, or desk.
- Data printouts should be securely shredded and disposed of when no longer required. When data is stored electronically, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts.
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated servers at CIFCPL premises, and should only be uploaded to approved cloud computing services.
- Device Data should be backed up daily. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All data entering into CIFCPL systems and websites is stored as unique and measures to prevent privilege escalation are taken.
- All data entering into the database of the CIFCPL website are protected with certificates that ensure encrypted communication when receiving and sending information is being used.

DATA ACCURACY AND ACTION

To exercise data protection, CIFCPL takes reasonable steps and is committed to.

- Restrict and monitor access to sensitive data, and keep it in as few places as necessary
- Establish effective data collection procedures
- Provide employees with online privacy and security measures training
- Build secure networks to protect online data from cyberattacks

- Establish clear procedures for reporting privacy breaches or data misuse Include contract clauses or communicate statements on how we handle data
- Update the data continuously and as mistakes are discovered

DATA HANDLING CONTROL MECHANISM

- Install firewall and protection software that prevents employees from sharing and distributing data from CIFCPL devices externally, by detecting when a large amount of data is being transferred either through email or via external drives.

Establish data protection practices (document shredding, secure locks, data encryption, frequent backup).

DATA CLASSIFICATION

Data classification is a crucial aspect of information security that helps us categorize and manage data according to its sensitivity and access requirements. Proper classification ensures that data is handled appropriately, reducing the risk of unauthorized access, disclosure, or misuse.

Data Classification Categories

Our data is classified into four main categories:

1. **Public:** The information that is openly available to the public. It is not restricted in any way, and there are no reservations about sharing it.
2. **Sensitive:** Sensitive information refers to data that could be subject to release under an open records request. However, it should be controlled to protect the interests of third parties. This means that while it might be disclosed when legally required, it is treated with extra care to safeguard individuals or entities that could be affected by its release.
3. **Confidential:**

Confidential information is typically exempted from public disclosure laws like the Public Information Act. This category includes data that is not meant to be publicly shared and requires strict controls and access restrictions. It often contains information that, if disclosed, could have significant negative consequences.

4. **Regulated/Restricted**: Information falling under this category is controlled by state or other third-party agreements. It could include data subject to specific compliance requirements, such as financial regulations or contractual agreements Compliance with these regulations and agreements is crucial, and strict controls are often in place to ensure data security and privacy.

Having such clear data classification categories is fundamental for data governance and security. It helps CIFCPL define and implement appropriate access controls, data protection measures, and compliance strategies for each type of data it handles.

The CIFCPL (Classification of Information for Data Loss Prevention) strategy outlines the actions to be taken based on data classification levels to prevent data loss and unauthorized access.

The following table summarizes the DLP strategy for each data classification level:

Classification	Pass	Alert	Quarantine	Block	Remarks
Public	☑				Accept all and deny few.
Sensitive		☑			Monitoring and Alerts for sensitive data.
Confidential			☑		Immediately quarantine confidential data upon detection of unauthorized access or sharing.
Regulated/Restricted				☑	DLP controls proactively block access or sharing of restricted data, preventing unauthorized exposure.

GRIEVANCES

CIFCPL shall address all grievances with respect to the processing of information in relation to this policy in a timebound manner. For this purpose, we hereby designate a grievance officer to redress any grievances in this regard.

Manjunath B V
Address: Brigade Software Park, 'B' Block, 8th Floor,
Banashankari Stage II, Banashankari, Bangalore 560070
Email ID: gro.cifcpl@chaitanyaindia.in
Contact No: +91- 9108002911