



Data Protection and Privacy Policy

Fusion Finance Limited

Attention: The information contained within this document is the property of Fusion Finance Limited and is issued in confidence and must not be reproduced in whole or in part or used in tendering or manufacturing purpose or given or communicated to any third party.

Code:	DPP
Version:	1.0
Date of version:	31/10/2020
Created by:	Mr. Sachin Singh Rana, Mr. Asish Das
Reviewed by:	Mr. Naveen Mangle
Approved by:	Board
Distribution List:	All fusion
Confidentiality level:	Internal
Review Frequency	Yearly

Document History

Ver No.	Date	Created /Modified By	Authorized/Approved By	Modification Details
V.1.0	9/12/2021	Sachin Singh Rana	Board	Review
V.1.0	28/11/2022	Sachin Singh Rana	Board	Review
V.1.1	6/11/2023	Asish Das	Board	Reviewed & abbreviation of company name from FMPL to FMFL
V.1.2	06/05/2024	Asish Das	Board	Added clauses 4.1 to 4.4 to cater to UIDAI guidelines
V.1.3	06/08/2024	Asish Das	Board	Reviewed & Changes in Company name

Contents

1. Definition and Acronyms	4
Definition.....	4
Acronyms	4
2. Scope	5
3. Purpose	5
4. Policy Statement	5
5. ISMS Control Reference	6
6. Enforcement	6

1. Definition and Acronyms

Definition

Term	Explanation
Asset	Anything that has value to the Organization
Information Security	Preservation of Confidentiality, Integrity and Availability; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
Information Security Management System	The system designed, implemented and maintained for assuring coherent suite of processes and systems; for effectively managing information accessibility, thus ensuring the confidentiality, integrity and availability of information assets and minimizing information security risks
FFL Employee	The person hired to perform a job or service for FFL, and one who is directly employed or hired on a contract basis
Customers	All the clients of Fusion FFL, who avail services provided by FFL.
Supplier	All third parties which include, but are not limited to vendors, volunteers, contractors, consultants, temporaries, and others who have access to, support, administer, manage, or maintain FFL's information or physical assets
External Storage Media	All storage devices like USB drives CDs, DVDs, camera phones, external hard disks, or any other device which has the ability to capture, storing or transporting data
Ethics	It applies to all aspects of business conduct and is relevant to the conduct of individuals and business organizations as a whole
Users (of the Information system of FFL)	The meaning of Users in this policy refers to all employees of FFL, temporaries, third parties, contractors, vendors, consultants, volunteers, interns, etc who use or deal with information assets or other assets of FFL.
Authorized Persons	Are defined as people who have established a need and received the necessary authorization from FFL.

Acronyms

Acronym	Full Name
FFL	Fusion Finance Limited
AR	Asset Register
ISMS/ISS	Information Security Management System/ Information Security System
IT	Information Technology
ISMF/ISF	Information Security Management Forum/ Information Security Forum
PDCA	Plan – Do – Check – Act (the Deming cycle)

2. Scope

All information concerning individuals including employees, third party users and clients are covered in the scope of this policy.

3. Purpose

Data protection and privacy policy of FFL deals with the process through which information concerning individuals including employees, third party users and client is obtained and disclosed. FFL respects the confidentiality of this information and strives to protect the privacy of individuals by regulating the collection, maintenance and disclosure of personal information.

4. Policy Statement

1. FFL is committed to compliance with all relevant data protection policies.
2. PII information can be named, phone no, gender, email, account no., address etc.
3. Personal data can be classified as per classification levels defined in the Information Labelling and Handling Policy.
4. The policy applies to all personal data held by the company, including on wireless notebook computers, personal digital assistants, mobile telephones etc.
5. All Employees/Staff will be provided training to ensure that they understand FFL's policies and procedures to implement them. Also, responsibility for handling PII should be allocated to the users.
6. The disciplinary process will be invoked in circumstances where this policy may have been transgressed.

4.1 Transparency and Consent:

- **Notice at Authentication:** During Aadhaar authentication, FFL will inform the Aadhar information holder about:
 - The specific PII (Aadhaar details) shared with UIDAI upon authentication.
 - The intended purposes for using the information received during authentication.
 - Any available alternatives to submitting your PII.
- **Language Accessibility:** FFL will provide this information in your local language for clear understanding.
- **Visually/Auditory Impaired Users:** FFL will ensure consent-related information is accessible to visually or audibly challenged individuals through appropriate methods.
- **Obtaining Consent:** FFL will obtain your explicit consent for Aadhaar authentication, preferably in electronic form, and maintain a record of your consent.

4.2 Data Minimization and Retention:

- FFL will only collect and share the minimum PII (including Aadhaar details) necessary for Aadhaar authentication.
- FFL will maintain logs of authentication transactions for a period of two (2) years. The Users have the right to access these logs during this period.
- After two (2) years, logs will be archived for a minimum of five (5) years, or for a longer period as required by law. After this period, logs will be deleted, except for those required for legal proceedings or pending disputes.

4.3 Revocation of Consent:

The Users have the right to revoke your consent at any time for a Knowledge Provider/User Agency (KUA) to store your encrypted e-KYC data or share it with third parties. Upon such revocation, the KUA will delete your e-KYC data and cease further processing.

4.4 Privacy Incidents and Reporting:

- FFL will promptly report any privacy incidents affecting your PII (including Aadhaar details) to UIDAI within 24 hours.
- FFL will fully cooperate with UIDAI or any authorized agency during investigations, incidents, claims, and complaints related to security and privacy breaches.

5. ISMS Control Reference

- A.18.1.4 Privacy and protection of personally identifiable information
- A.18.1.5 Regulation of cryptographic controls

6. Enforcement

Necessary disciplinary action will be taken against any employee not following the policies and procedures laid down by the FFL. Similarly, action will be taken against those employees encouraging/observing such activity and not reporting the same to the concerned authority. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

-END OF DOCUMENT-