Data Confidentiality and Privacy Policy

Version Control:

Version	Date of Adoption	Change Reference	Owner	Custodian	Approving Authority
1.0	18-Feb-2016	Adoption of the Data Confidentiality and Privacy Policy as per Information Technology Act, 2000, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2001 and Credit Information Companies (Regulation) Act, 2005	IT Team	Compliance Team	Board of Directors
1.1	22-Jun-2021	Updated the Data Confidentiality and Privacy Policy with the following: - updation of Information Technology Act, 2000, Information Technology (Reasonable Security	IT Team	Compliance Team	Board of Directors

		Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 reference and - From join authority of CEO and COO, authority to CEO is modified w.r.t. for waiving off the requirement for sharing customer's personal data based on compelling business/ compliance logic but within the principles laid down under this policy.			
1.2	29-May-2023	Added Data Classification Policy and Review period of the Policy	IT Team	Compliance Team	Board of Directors
1.2	30-May-2024	Annual Review. No change	IT Team	Compliance Team	Board of Directors

1.3	12-Nov-2024	Addition of a section listing the right of the customer to view/ edit his/ her data and request for deletion in alignment with Digital personal Data Protection Act, 2023	IT Team	Compliance Team	Board of Directors

Data Confidentiality and Privacy Policy

1.0 Purpose

The purpose of this data classification policy is to provide a system for protecting information that is critical to the organization.

Ashv Finance Limited (erstwhile Jain Sons Finlease Limited) (hereinafter referred to as "Ashv Finance") is governed by the Information Technology Act, 2000, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and Credit Information Companies (Regulation) Act, 2005. These acts regulate Ashv Finance's handling of 'personal information', which means information or an opinion that identifies an individual/company or allows their identity and other details to be readily worked out on the basis of such information

2.0 Scope

ASHV All employees who come into contact with confidential information are expected to familiarize themselves with this data classification policy and shall constantly follow the same.

This policy (together with the Terms and Conditions and any other documents referred to in it) sets out the basis on which any personal data collected from companies or their agents, or that provided by companies or their agents, which will be processed, stored and/or shared with other parties by Ashv Finance. Such information may be provided by Customers (including actual customers and potential customers or any of their employees, directors, agents, or appointed nominees) to Ashv Finance by any means, with the intention of establishing a relationship, of whatsoever nature, with Ashv Finance. Under this Privacy Policy, Ashv Finance shall receive, store, and process data received (Company Information) from its Customers to whom it may consider giving a loan. This Policy shall also deal the manner in which Ashv Finance shall share the Company Information with other parties. In addition to the information that the Ashv Finance elicits from its Customers, the Customers are free to volunteer any other information that they feel that the Ashv Finance needs to know, but the security and confidentiality under this Policy is limited only to information that the Ashv Finance directly asks from Companies.

Ashv Finance may use the Company Information for, among other things, customer verification, provision of products and services, personalization of products or services, marketing or promotion of its financial services or related products or that of our associates and affiliates; analysis or credit scoring, enforcement of company's obligations, any other purpose that will help Ashv Finance in providing companies with optimal and high-quality services.

Ashv Finance will give access to Company Information to only authorized employees. Employees who violate this Privacy Policy shall be subject to disciplinary process as per the internal guidelines of Ashv Finance. Any employee who withdraws from the employment of Ashv Finance will have to undertake to abide by this Privacy Policy and keep all Company Information secure and confidential.

3.0 Responsibility

ASHV All Employees

Policy

- The data classification system has been designed to support the need to know, so that, information will be protected from unauthorized disclosure/use/modification/deletion.
- Consistent use of this data classification system will facilitate business activities and help us to minimize the cost of information security.
- Without the consistent use of this data classification system, there will be risks of loss of customer relationships, loss of public confidence, internal operation disruption, excessive costs, and competitive disadvantages and affect regulatory compliance.
- Since the business is handling confidential data like KYC is important to meet the regulatory requirements.
- Data has been classified as public, internal, confidential, and secret
- Clear labeling will be done on the left-hand top corner in case of internal, confidential, and secret data
- Department-wise details about the different parameters for various classes of data
- Retention schedule details of the various records in the company

Ashv Finance may disclose the Company Information to any person, without any limitation and the Customers hereby give their irrevocable consent for the same, provided such disclosure is to:

- To comply with legal requirements, legal processes, legal or regulatory directives/ instruction; or
- To enforce the terms and conditions of the products or services or any other existing agreements; or
- To protect or defend rights, interests, and property of Ashv Finance or that of its associates and affiliates, or that of our or our affiliate's employees, consultants, etc.; or
- For fraud prevention purposes; or

- As permitted or required by law;

Ashv Finance may disclose the Company Information to third parties for the following, among other purposes, and will make reasonable efforts to bind them to the obligation to keep the same secure and confidential and an obligation to use the information for the purpose for which the same is disclosed, and companies hereby give your irrevocable consent for the same:

- For participation in any telecommunication or electronic clearing network; or
- For the purpose of audit – whether statutory or otherwise or in relation to capital raising activities by Ashv Finance; or
- For credit rating of Ashv Finance by any credit rating agency; or
- For advertising; or
- For facilitating joint product promotion campaigns; or
- For the purposes of credit reporting, verification, and risk management to/ with clearing house centers or credit information bureaus and the like; or
- For availing of the support services from third parties e.g., collecting subscription fees, and notifying or contacting you regarding any problem with, or the expiration of, any services availed by companies

Except for the above-mentioned purposes, Ashv Finance may share Company Information with any other purpose at the specific request received by the Customer or with prior approval from the Customer for any such disclosure.

Unless absolutely necessary, the company shall not disclose the names of the customers and their principals, agents, and representatives to anybody outside the employees of Ashv Finance. For submission of the above data, unless absolutely necessary, the data shall be shared on a no-name basis and could include aliases, client/ loan codes, etc. For ample clarity, the non-employees shall include non-employee affiliates of Ashv Finance, its non-employee Shareholders, Board members, etc. Specifically, to the lenders, all details pertaining to the loan book hypothecated to respective lenders will be shared with them and the rest will be shared with aliases/ codes. CEO of Ashv Finance can waive off the above requirement based on compelling business/ compliance logic but within the principles laid down under this policy.

The customer has the following rights regarding the management of personal/financial data by the company:

1. To request revocation of consent in cases where the loan applications have not been processed
2. To request to review, and correct/edit personal data provided such changes do not change or impact any loan underwriting parameters
3. To request permanent deletion of data unless retention of the same is necessary for a specified purpose or for compliance with any law for the time being in force.

Ashv Finance reserves the right to modify this Privacy Policy from time to time in order that it accurately reflects the regulatory environment and its data collection principles. Upon each change to the Policy, Ashv Finance shall allow access to such changes / revised Policies to all concerned stakeholders by way of display of this Privacy Policy on its official website.

Operations Team

1. General Information				
2. Data Classification Levels	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Definition	Information that is freely and without reservation is made available to the public.	Information that should be controlled to protect third parties.	Information that contains confidential data related to the customer.	Information that typically is excluded from the Public.
Examples		* Policies * SOPs Only internal stakeholders and sometimes partners.	* Customer KYC Documents * Customer T&C * Leads Data* (Business and Credit)	* Internal Policy Documents * Business Plan

			* Loan Documents * Collateral Documents * Customer PII Data	
Consequence of Public Disclosure	No adverse consequences	• Loss of reputation • Loss of trust	• Loss of reputation • Loss of trust • Potential regulatory penalties	• Loss of reputation • Loss of trust • Potential regulatory penalties
3. Roles and Responsibilities	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Data Custodian		Head of Operations (For Ops Policies and SOPs)	IT	IT
Data Owner		Head of Operations (For Ops Policies and SOPs)	Operations Team	Operations Team
Information Security Officer		CISO	CISO	CISO
Legal and/or Privacy Office (Public Information Officer)	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer
Managers	n/a	Team Leads (Pre-disbursement and post- disbursement)	Team Leads (Pre-disbursement and post-disbursement)	Team Leads (Pre-disbursement and post-disbursement)
Users	n/a	-	-	-

Credit and Risk Team

1. General Information				
2. Data Classification Levels	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Definition	Information that is	Information that should	Information that	Information that typically is

	freely and without reservation is made available to the public.	be controlled to protect third parties.	contains confidential data related to the customer.	excluded from the Public.
Examples	No Public data resides with Credit and Risk	* HR Related Documents * Accounts Related Documents * Third Party Agreements without Commercial Information * General Risk Policies	* Customer KYC Documents (ID and Address Proof) * ITR, Bank Statements, GST, Business Proof and Ownership Proof * Collateral Documents	* Internal Policy Documents * Product-wise scoring models * Risk Assessment Reports * Audit Reports
Consequence of Public Disclosure	No adverse consequences	• Loss of reputation • Loss of trust	• Loss of reputation • Loss of trust • Potential regulatory penalties	• Loss of reputation • Loss of trust • Potential regulatory penalties
3. Roles and Responsibilities	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Data Custodian	IT	IT	IT	IT
Data Owner	Head of Credit and Risk / Policy	Head of Credit and Risk / Policy	Head of Credit and Risk / Policy	Head of Credit and Risk / Policy
Information Security Officer	CISO	CISO	CISO	CISO
Legal and/or Privacy Office (Public Information Officer)	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer
Managers	n/a	Line Managers - Area Heads - National Heads - Head of Policy/ Analytics - Head of Credit - CRO	Line Managers - Area Heads - National Heads - Head of Policy/ Analytics - Head of Credit - CRO	Line Managers - Area Heads - National Heads - Head of Policy/ Analytics - Head of Credit - CRO

Users	n/a	• Identify and Label/ tag data, where appropriate • Properly Dispose of Data	• Identify and Label/ tag data, where appropriate • Properly Dispose of Data	• Identify and Label/ tag data, where appropriate • Properly Dispose of Data

Sales Team

1. General Information				
2. Data Classification Levels	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Definition	Information that is freely and without reservation made available to the public.	Information that should be controlled to protect third parties.	Information that contains confidential data related to the customer.	Information that typically is accepted from the Public.
Examples		Data that meets the definition of PII • Acceptable Usage Policy * BCP / DR Policy * HR Related Documents * Accounts Related Documents	* Customer KYC Documents * Financial Documents (ITR / Bank Statements) * Leads Data * Customer PII Data * In case of a secured loan (Copy of property	* Employee Records • Salary Information * Business Plan

		* Third Party Agreements without Commercial Information	documentation)	
Consequence of Public Disclosure	No adverse consequences	• Loss of reputation • Loss of trust	• Loss of reputation • Loss of trust • Potential regulatory penalties	• Loss of reputation • Loss of trust • Potential regulatory penalties
3. Roles and Responsibilities	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Data Custodian	IT	IT	IT	IT
Data Owner	National Sales Head	National Sales Head	National Sales Head	National Sales Head
Information Security Officer	CISO	CISO	CISO	CISO
Legal and/or Privacy Office (Public Information Officer)	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer
Managers	n/a	Line Managers - Area Heads - National Heads – National Sales Head - CEO	Line Managers - Area Heads - National Heads – National Sales Head – CEO	Line Managers - Area Heads - National Heads – National Sales Head - CEO
Users	n/a	• Identify and Label/ tag data, where appropriate • Properly Dispose of Data	• Identify and Label/ tag data, where appropriate • Properly Dispose of Data	•Identify and Label/ tag data, where appropriate • Properly Dispose of Data

HR Team

1. General Information

2. Data Classification Levels	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Definition	Information that is freely and without reservation made available to the public.	Information that should be controlled to protect third parties.	Information that contains confidential data related to the customer.	Information that typically is excluded from the Public.
Examples	* Social media (Jobs notifications)	• Acceptable Usage Policy * HR Related Documents * Accounts Related Documents * HR Policy Handbook (POSH, Anti-Bribe etc.)	N/A	* Employee Records * Employee KYC Documents • Salary Information * Appraisal Sheet
Consequence of Public Disclosure	No adverse consequences	• Loss of reputation • Loss of trust	• Loss of reputation • Loss of trust • Potential regulatory penalties	• Loss of reputation • Loss of trust • Potential regulatory penalties
3. Roles and Responsibilities	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Data Custodian	IT	IT	IT	IT
Data Owner	N/A	Head of HR	N/A	Head of HR
Information Security Officer	CISO	CISO	CISO	CISO
Legal and/or Privacy Office (Public Information Officer)	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer
Managers	N/A	N/A	N/A	No Access to internal employee data
Users	N/A	N/A	N/A	N/A

Treasury

1. General Information				
2. Data Classification Levels	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Definition	Information that is freely and without reservation is made available to the public.	Information that should be controlled to protect third parties.	Information that contains confidential data related to the customer.	Information that typically is excluded from the Public.
Justification: Examples	* Annual Reports * Investor Relations * STR (Suspicious Transaction Reports) * AML (Anti-Money Laundering)	* MoA, AoA, Certificate of Incorporation * Shareholding pattern	* Customer data when converted for securitization	* Internal Policy Documents * **Borrowing profiles** * **Asset Liability Management (ALM) Statement** * **Portfolio Asset Quality**

				* KYC for Ashv Finance and Leadership team * **Monthly Reports (To Ashv Lenders)**
Consequence of Public Disclosure	No adverse consequences	• Loss of reputation • Loss of trust	• Loss of reputation • Loss of trust • Potential regulatory penalties	• Loss of reputation • Loss of trust • Potential regulatory penalties
3. Roles and Responsibilities	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Data Custodian	IT	IT	IT	IT
Data Owner	N/A	Head of Treasury	N/A	* Head of Treasury * CFO
Information Security Officer	CISO	CISO	CISO	CISO
Legal and/or Privacy Office (Public Information Officer)	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer
Managers	n/a	* Senior Managers	* Senior Managers	* Senior Managers
Users	n/a			

Finance

1. General Information				
2. Data Classification Levels	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Definition	Information that is freely and without reservation made available to the	Information that should be controlled to protect third parties.	Information that contains confidential data related to the	Information that typically is excluded from the Public.

	public.		customer.	
Justification: Examples	* Annual Reports * Quarterly Financial Reports * Publicly Available Policies as per RBI Requirements	* Management MIS * Workings for financial statements * Tally	n / a	* Salary Information * Internal Policy Documents * TDS Certificates (Employees and Vendors) * Vendor invoices
Consequence of Public Disclosure	No adverse consequences	• Loss of reputation • Loss of trust * Financial implications	• Loss of reputation • Loss of trust * Financial implications	• Loss of reputation • Loss of trust * Financial implications
3. Roles and Responsibilities	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Data Custodian	IT	IT	IT	IT
Data Owner	Accounts	Accounts	Accounts	Accounts
Information Security Officer	CISO	CISO	CISO	CISO
Legal and/or Privacy Office (Public Information Officer)	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer
Managers	n/a	Line Managers - VP Finance - CFO	NA	Line Managers - VP Finance - CFO
Users	n/a	• Identify, and Label where appropriate, Data • Properly Dispose of Data	• Identify, and Label where appropriate, Data • Properly Dispose of Data	• Identify, and Label where appropriate, Data • Properly Dispose of Data

Compliance

1. General Information				
2. Data Classification Levels	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Definition	Information that is freely and without reservation made available to the public.	Information that should be controlled to protect third parties.	Information that contains confidential data related to the customer.	Information that typically is excluded from the Public.
Justification: Examples	* Fair Practice Code * KYC & AML Policy * Nomination and Remuneration Policy * Annual Reports * RPT Policy	* Returns submitted to regulatory authorities * Company agreements * Internal Policies (Data Confidentiality, Investment Policies etc.)	Should give awareness session to all employees for keeping the data safe	* Internal Policy Documents * Incident Reports (For RBI) * Audit Reports * Board deck * Business Plan and projections
Consequence of Public Disclosure	No adverse consequences	• Loss of reputation • Loss of trust	• Loss of reputation • Loss of trust * Regulatory Penalties	• Loss of reputation • Loss of trust * Regulatory Penalties
3. Roles and Responsibilities	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Data Custodian	IT (All other online access) and Compliance (Hard copies)	IT (All other online access) and Compliance (Hard copies)	IT (All other online access) and Compliance (Hard copies)	IT (All other online access) and Compliance (Hard copies)
Data Owner	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer
Information Security Officer	CISO	CISO	CISO	CISO
Legal and/or Privacy Office	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer

(Public Information Officer)				
Managers	N/A	Line Managers - Chief Compliance Officer	Line Managers - Chief Compliance Officer	Line Managers - Chief Compliance Officer
Users	N/A	N/A	N/A	N/A

Technology

1. General Information				
2. Data Classification Levels	**Public**	**Internal**	**Customer Confidential**	**Confidential**
Definition	Information that is freely and without reservation made available to the public.	Information that should be controlled to protect third parties.	Information that contains confidential data related to the customer.	Information that typically is excluded from the Public.
Examples			Production Database	Source Code Production Database UAT Access
Consequence of Public Disclosure	No adverse consequences	• Loss of reputation • Loss of trust	• Loss of reputation • Loss of trust • Potential regulatory penalties	• Loss of reputation • Loss of trust • Potential regulatory penalties

3. Roles and Responsibilities	Public	Internal	Customer Confidential	Confidential
Data Custodian	IT team	IT team	IT team	IT team
Data Owner	CTO	CTO	CTO	CTO
Information Security Officer	CISO	CISO	CISO	CISO
Legal and/or Privacy Office (Public Information Officer)	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer	Chief Compliance Officer
Managers	N/A	Delivery Managers – Head of Engineering - CTO	Delivery Managers – Head of Engineering - CTO	Delivery Managers – Head of Engineering - CTO
Users	N/A	N/A	N/A	N/A

Retention schedule

Sl. No.	Record	Retention period	Remarks
1.	Salary statements, PF, ESI records, and other applicable statutory records	8 Years	As per law
2.	Contract Agreements	Not specified	
3.	Financial Documents/Statements	5 Years	As per law
4	Dept. Reports	As per Dept. HOD/ Management Approval	
5	Exit employee's files	2 Years	

Review of the Policy:

This policy will be reviewed on an annual basis by the Management. If there is any change to the policy, then the Management will seek Board/Committee approval.