

ISMS 15 - HCAL – Privacy Policy
Version 1.0

Document Control

Authorization

DOCUMENT NAME	ISMS 15 - HCAL – Privacy Policy
EFFECTIVE DATE	10 th January 2024
DOCUMENT PREPARED BY:	IT Head
DOCUMENT APPROVER	Board
DOCUMENT OWNER	IT Head
DOCUMENT CLASSIFICATION	Internal
DOCUMENT VERSION NO.	1.0

Summary of Changes:

Sr. No.	Version	Summary of Change
1	1.0	Initial Release (Reviewed – January 2025)

Ownership

This document is the sole property of HDFC Capital Advisors Limited and is to be used strictly for Internal Consumption only.

Placement

The most updated copies of the document can be found on the shared path communicated with the organization employees.

Contents

1. Objective.....	4
2. Applicability	4
3. Key Definitions	4
4. Elements of Privacy Policy	5

1. Objective

The purpose of this Privacy Policy (“**Policy**”) is to maintain the privacy of and protect the personal information of employees, contractors, outsourced workforce, vendors, interns, associates, customers, Corporate Social Responsibility (CSR) partners and business partners of HDFC Capital Advisors Limited (“**Company**”) and ensure compliance with the Information Technology Act, 2000 (“**Act**”) and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (“**Rules**”).

This Policy must be read in conjunction with the Act and the Rules, as may be amended from time to time.

2. Applicability

This Policy is applicable to the Company and the Third Party (“as defined in Section 3 of the Policy”) who may receive, collect, possess, stores, deals or handle Personal information (PI)/ Sensitive personal data or information (SPDI), on behalf of the Company.

Any such Third Party is expected to have read, understood and comply with this Policy. The Company will use its best endeavors to ensure that such Third Party have read and understood the terms of this Policy and preferably having entered into a confidentiality agreement.

3. Key Definitions

- (a) “**Data subject**” is one who is the subject of personal and sensitive personal data. It may include, but is not limited to, the employees, contractors, outsourced workforce, vendors, interns, associates, customers, Corporate Social Responsibility (CSR) partners and business partners of the Company.
- (b) “**Personal information (PI)**” means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.
- (c) “**Sensitive personal data or information (SPDI)**” of a person means such personal information which consists of information relating to.
 - i. password.
 - ii. financial information such as Bank account or credit card or debit card or other payment instrument details.
 - iii. physical, physiological, and mental health condition.
 - iv. sexual orientation.
 - v. medical records and history.
 - vi. Biometric information.
 - vii. any detail relating to the above clauses as provided to body corporate for providing service; and
 - viii. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

- (d) “**Third Party**” means all external parties such as contractors, outsourced workforce, interns, summer trainees, vendors, CSR Partners and business partners who have access to Company’s information assets.

4. Elements of Privacy Policy

This Policy describes generally acceptable privacy principles for the protection and appropriate use of personal information and SPDI at the Company.

4.1 Consent

The Company shall obtain consent from the Data subject before collecting, receiving, possessing, storing, dealing or handling personal information or SPDI of the provider of such information. No PI/SPDI shall be used by the Company without the consent of the provider of the information. The consent shall be obtained (in writing or electronically) from the Data subjects before or at the time of collecting PI or SPDI.

The Data subject shall be provided with a choice to opt out and withdraw any consent previously given by way of written communication to the Company.

4.2 Collection of Personal Information

- a) The Company shall not collect PI or Sensitive personal data or information (SPDI) unless: (i) the information is collected for a lawful purpose connected with a function or activity of the Company or any person on its behalf; and (ii) the collection of the PI / SPDI is considered necessary for that purpose.
- b) While collecting PI/ SPDI directly from the person concerned, the Company or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of: (i) the fact that the information is being collected; (ii) the purpose for which the information is being collected; (iii) the intended recipients of the information; (iv) the name and address of the agency that is collecting the information; and (v) the agency that will retain the information.
- c) The Company or any person on its behalf holding PI/ SPDI shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.
- d) The PI/SPDI collected shall be used for the purpose for which it has been collected.
- e) The Company shall address any discrepancies and grievances of the provider of the PI/ SPDI in a time bound manner. For this purpose, the Company shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall use best endeavors to redress the grievances of the provider of information expeditiously within one month from the date of receipt of grievance.

4.3 Disclosure of Information

- a) Disclosure of PI/ SPDI by the Company to any Third Party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the Company and the provider of information, or where the disclosure is necessary for compliance of a legal/regulatory obligation;

Provided that the information shall be shared by the Company, without obtaining prior consent from the provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Company will use best endeavors to ensure that the Government agency sends a request in writing to the Company possessing the sensitive personal data or information stating clearly the purpose of seeking such information and stating that the information so obtained shall not be published or shared with any other person.

- b) The Company shall disclose any PI/ SPDI to any Third Party by an order under the law for the time being in force.
- c) The Company or any person on its behalf shall not publish the PI/ SPDI.
- d) The Company shall use its best endeavors (including by way of execution of appropriate non-disclosure agreements) to ensure that the Third Party receiving the PI/ SPDI from the Company or any person on its behalf shall not disclose it further.

4.4 Reasonable Security Practices and Procedures

The Company endeavors to have in place reasonable security practices and procedures in place to protect the PI/SPDI of the provider of information.

End of the Document