Data Privacy Policy

VCPL-ISP-13 -V1.0

DOCUMENT AND RECORD CONTROL

Version Control

Document Control ID	VCPL-ISP-13-Data Privacy -V1.0
Issued Date	16-September-2022
Effective Date:	16-September-2022
Owner:	ISMS

Revision Table

Date	Version	Affected Sections	Author
16-September-2022	1.0		Mr Ramesh T.P

Release Authorization

Task	Author	Title
Prepared by	Mr Ramesh T.P	Deputy Vice President

Reviewer Authorization

Name	Title	Signature	Date
Mr. Prasenjit Datta	Head of Technology	Prasenjit Datta	16-September-2022

Approval Authorization

Name	Signature	Date
Board of Directors		

TABLE OF CONTENTS

1. Purpose

The purpose of this document is to define the policy & practices to be followed for collection, use, retention, dissemination and protection of personally identifiable information (PII).

2. Scope

The Scope extends to all staff (employees and contractors), functions & activities of the organization, and all personally identifiable information (PII) belonging to the employees, customers, and contractors, suppliers and service providers of the organization.

3. Responsibility

All members of staff (employees and contractors) are responsible to follow the rules stated in this document for collection, use, retention, dissemination and protection of personally identifiable information (PII).

IS Security Officer shall be responsible and authorized for enforcement of this privacy.

4. Definitions

PII – Personally Identifiable Information

Personally Identifiable Information (PII) is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

5. Privacy Statements

Following section defines the practice(s) to be followed for personally identifiable information (PII) being collected, used, retained, and disseminated at IVY Mobility. The goal is to be complaint with all applicable privacy laws and regulations.

5.1 Authority & Purpose

- The organization shall collect, use, retain, and disseminate personally identifiable information (PII) only that is permitted by law of land.
- The organization shall describe the purpose(s) for which personally identifiable information (PII) is collected, used, retained, and disseminated.

5.2 Accountability, Audit & Risk Management

- IS Security Officer shall ensure compliance with all applicable laws and regulations regarding the collection, use, retention, dissemination and disposal of personally identifiable information (PII) by programs and information systems.
- Special consideration shall be given to personally identifiable information (PII) while conducting the risk assessment for information assets.
- Appropriate controls shall be identified & implemented for protection of personally identifiable information (PII).

- Appropriate monitoring & audit controls shall be implemented to ensure the effective implementation of security controls to protect personally identifiable information (PII).

- Role based privacy awareness programs shall be conducted to ensure personnel understand privacy responsibilities and procedures.

5.3 Data Minimization, Retention & Disposal

- Only the minimum personally identifiable information (PII) relevant and necessary to accomplish the legally authorized purpose shall be collected.

- The purpose of collecting and retaining personally identifiable information (PII) shall be described and consent taken from an individual before collection of personally identifiable information (PII).

- Scheduled reviews shall be conducted to ensure that only consented personally identifiable information (PII) is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

- Any personally identifiable information (PII) no longer required to be retained by law or purpose shall be disposed-off / destroyed / securely erased / anonymized regardless of the method of storage in a manner that prevents loss, theft, misuse, unauthorized access of personally identifiable information (PII).

5.4 Individual Participation and Redress

- Means to authorize collection, use, retention and dissemination of personally identifiable information (PII),shall be provided to individuals wherever feasible and appropriate.

- Means to understand the consequences of decisions to approve or decline the authorization of collection use, retention and dissemination of personally identifiable information (PII), shall be provided to individuals to enable them to make informed decisions.

- Whenever feasible and appropriate the consent shall be obtained from individuals prior to any new uses or disclosure of previously collected personally identifiable information (PII).

- Wherever feasible it shall be ensured to keep individuals aware of the uses of personally identifiable information (PII) not initially described while taking consent at the time of collection.

- Individuals shall be given access as appropriate to their personally identifiable information (PII) retained in organization records/systems.

- Any concerns regarding collection, use, retention and dissemination of personally identifiable information (PII) can be raised by sending an email to privacy officer.

5.5 Security of Personally Identifiable Information (PII)

- Inventory of all programs and information systems shall be established and maintained that collection, use, retention and dissemination of personally identifiable information (PII).

- Appropriate security controls shall be identified and implemented for all programs and information systems that collection, use, retention and dissemination of personally identifiable information (PII).

- Any unauthorized disclosure unauthorized modification or unexpected loss of availability shall be reported to IS Security Officer immediately upon notice of such an event.

5.6 Use Limitation

- The personally identifiable information (PII) shall be used only for lawful and authorized purpose as consented at the time of collection.

- Any other use and/or sharing of personally identifiable information (PII) shall remain strictly prohibited at all times.

---End of Document---