DATA PROTECTION & PRIVACY

POLICY

Ver 1.3

(Doc No: EHS/ISMS/IT/PLC-07)

Contents

1. Purpose

ECLAT may collect, use and store, disclose or transfer data and/or personal information from its employees, business partners, vendors, customers, consultants or third parties ("**Data Subjects**") in its ordinary course of business ("**Personal Information**") after taking due consent from the concerned Data Subject in this respect. Therefore, the purpose of this policy is to define the measures to be taken for protecting the Personal Information.

ECLAT collects the Personal Information as per statutory requirements under the applicable laws of India and for the purposes of its internal human resource management, and commercial operations and business. This Personal Information will be disclosed by ECLAT on need to know basis with authorized members as per statutory requirements and/or in accordance with this policy.

2. Scope

This Policy applies to all Data Subjects who share Personal information with ECLAT. The words "data", "information" and "Personal Information" may be used interchangeably in this procedure and mean the same thing.

3. Glossary

Abbreviation /Term	Full Form / Description
ISF Head	Chief Information Security Officer/Information security Forum Head
Individual Users / Employees	Employees / Users in ECLAT
Department Heads	Heads of various departments within ECLAT
ISF	Core group of people responsible for implementing and maintaining the ISMS

4. Policy

4.1 Principle of Data Protection

ECLAT complies with the below principles:

- Data should be obtained for specific and lawful purposes
- Data should be processed fairly and lawfully only for the specific purpose
- Data should be adequate, relevant and not excessive in relation to the purpose for which it is held
- Data should be accurate and, where necessary, kept up to date
- Data should be kept only for as long as necessary
- Data should be processed in accordance with the rights of data subjects
- Data should be securely maintained to avoid loss or destruction
- Data should not be shared / transferred to place where there is no / inadequate level of protection.

All Personal Information that is not Open Source or Public and classified as equal to **"SENSITIVE"** or **"RESTRICTED"** by clients or as per applicable law, will be treated as **SENSITIVE** when it is received by ECLAT. Access to this information is restricted to a limited number of personnel in a group on a "**NEED TO KNOW**" basis.

ECLAT is committed to ensure that Personal Information is **not** disclosed to unauthorized third parties including family & friends of employees. All employees of ECLAT should always maintain the secrecy of the Personal Information they are handling or coming in contact with.

However, there will be certain circumstances where ECLAT will have to disclose or transfer the data, which the Data Subjects authorize ECLAT to do.

- Legitimate Disclosure (with prior consent taken by ECLAT)

✓ Disclosure of Information required in performance of contract

✓ Disclosure in the legitimate interest of the concerned / ECLAT

- Disclosure without consent

✓ When required by a Court of Law

✓ When required by a Regulatory Body

✓ To safeguard national security

- Unless otherwise directed by a specific non-disclosure agreement, Personal Information is treated as per this procedure.

4.2 Roles & Responsibilities

Roles	Responsibility
Department Head	Protection of data, Obligation to protect data, Determining Right to access
Project Manager /Department Head	Identifying and defining the confidentiality of data / assets; Protection of data, Determining Right to access, Disclosure of data
System Administrator	Protection of data, Implement the control
Individual Employees	Protection of data and complying with this procedure

4.3 Identification of Personal Information

Any Personal Information which is received from Data Subjects and already classified by the clients or business partners as ECLAT equivalent of **"RESTRICTED"** would be treated as Classified Data.

This Personal Information would be handled as per the protection & security procedure defined in this document.

4.4 Protection of Personal Information

- The Ops/Coding Manager should be responsible for protection of Personal Information in his/her project.
- The Ops/Coding Manager should identify the confidentiality levels of the Personal Information.
- Based on the level of confidentiality required, the Ops/Coding Manager should define the access for Personal Information and he / she should also define the protection level in coordination with Department Head-IT or Mgr Compliance or ISF Head.
- ECLAT reserves the right to use any technology or measures which it feels is required / adequate / feasible in protecting the Personal Information available in their custody, wherever necessary.
- If there are any Legal / Client specific requirements, ECLAT will implement the appropriate technology / measures.
- ECLAT has obtained ISO 27001:2013 certification for its information security management system.

4.5 Obligation to Protect Personal Information

- The Management of ECLAT is obliged to ensure the protection of Personal Information collected, taken, received during its normal course of business engagements with various data subjects to fulfill the above listed Principles of Data Protection. However, this is limited only to Classified Data which is equivalence of "**SENSITIVE**" OR "**RESTRICTED**" as per ECLAT's classification policies or as per applicable law.

- The necessary Technical, Procedure oriented, Organizational measures would be implemented across all the activities of ECLAT to ensure that the process of "**DUE CARE**" is followed to protect the Personal Information, always, which the Data Subjects acknowledge as secure and adequate for the protection of the Personal Information.

4.6 Implementation of the Controls

4.6.1 Storage of Personal Information

Personal Information is in the form of feedback, client information, used by TLs and Managers physically in folders of their respective machines or servers if required. Access to these folders / servers should be limited and given to only those users who are working for that specific customer and have a specific "Need to Use".

4.6.2 Backup of Personal Information

Backup of Personal Information wherever necessary, however, Eclat never saves any sensitive information.

4.6.3 Retention & Disposal of Personal Information

- All Personal Information collected / received from various sources as part of Business engagements should not be retained beyond the agreed / required period in the custody of ECLAT.

- On completion of the contract / term, the Personal Information should be removed from the work area. However, ECLAT should be entitled to take a backup of the Personal Information for its own references which should be preserved at onsite and offsite location with the highest classification possible such as "**SENSITIVE**" OR "**RESTRICTED**". The physical and logical access afforded for this copy of data should always be commensurate with the classification.

- All other copies either manual or electronic should be destroyed commensurate with their classification.

4.7 Right to Access

Data Subjects (within the scope of this policy) may access, update, or correct their Personal Information with due notice to the management of ECLAT.

If you find any discrepancies or have any grievances in relation to the processing of Personal Information under this Policy, please contact our Grievance Officer listed below.

5. References/Forms/Templates

- Information Asset Classification and Labeling Policy
- Backup Policy
- Log Analysis and Retention Policy
- Media Disposal Guideline

Grievance Officer appointed under the Information Technology Act, 2000	
Name	**Contact details**
Mr. Ramprasad Tandle	ramprasad.tandle@eclathealth.com;