Data Privacy Policy

Document Details

Title: 028 – Data Privacy Policy	Document Owner: Cyber Security Team
Document Author(s): Sanket Mhatre	Version: V1.0
Classification: Polycab - Internal	Release Date: 10-04-2025

Version Details

Sr No.	Version	Date	Modified By	Reviewed By	Approved By	Comments
1	V1.0	04-Apr-25	Sanket Mhatre -IT Cyber Security (GRC)	Vijit Patil – CISO Ashish Anekar – IT Infra Head	Gandharv Tongia - CFO/CIO	Updated to align with industry standards (NIST and ISO 27001)

Contents

1. Introduction: 4
2. Scope 4
3. Purpose 4
4. Roles and Responsibilities 4
5. Collection of Customer Data 6
7. Procedure 7
7.1 Confidentiality 7
7.2 Data Privacy and Security Controls 7
7.3 Handling employee data at Polycab 8
7.4 Access Request 9
8. Enforcement 11
9. Training and Awareness 11
10. Review and Update 11
11. Control Reference 11

1. Introduction:

This Policy explains the types of personal information we collect, how we use, store, and safeguard it, and the measures we take to protect your privacy when interacting with our services. It aims to provide transparency about our data collection practices and your rights regarding your personal data.

2. Scope

This Policy applies to all individuals who access or use our website, mobile applications, services, or any other platforms associated with us. It covers the collection of personal information through these platforms, how we use and share such data, and how we comply with relevant privacy laws to ensure that your personal information is handled responsibly and securely.

3. Purpose

The purpose of this policy is to enable Polycab to:

- Comply with the law with respect of the data it holds about individuals.
- Follow good privacy practices.
- Protect Polycab employees, consultants, and customers
- Protect the organization from the consequences of a breach of its responsibilities.

4. Roles and Responsibilities

Data Subject (Individual) Rights

- **Right to Consent**: Ensure that data subjects provide clear, informed consent before their data is collected.
- **Right to Access**: Allow data subjects to access their personal data upon request.
- **Right to Rectification**: Enable data subjects to update or correct inaccuracies in their personal data.
- **Right to Erasure**: Grant the right to delete personal data, in certain cases, when it is no longer needed or upon request.
- **Right to Data Portability**: Provide data subjects with the ability to transfer their data to another service provider if required.
- **Right to Object**: Allow data subjects to object to the processing of their data in certain scenarios.

Data Controller

The **Data Controller** is the entity responsible for determining the purposes and means of processing personal data. Their responsibilities include:

- **Data Collection and Usage**: Ensure that personal data is collected fairly, transparently, and for legitimate purposes.
- **Consent Management**: Obtain and manage consent from data subjects, ensuring that it is informed, explicit, and revocable.
- **Data Processing Accountability**: Oversee and be accountable for all data processing activities within the organization, ensuring compliance with DPDP requirements.

- **Security Measures:** Implement appropriate technical and organizational security measures to protect personal data from unauthorized access, loss, or theft.
- **Data Retention:** Define data retention periods and ensure data is securely disposed of once no longer needed.
- **Data Privacy Impact Assessment:** Regularly conduct assessments to identify and mitigate risks to the privacy of data subjects.
- **Notification:** Notify authorities and affected individuals in case of a data breach.

Data Processor

A **Data Processor** handles personal data on behalf of the data controller but does not control how the data is processed. Their responsibilities include:

- **Data Processing Agreements:** Ensure that contracts or agreements with the data controller define their roles and responsibilities, as per the DPDP.
- **Security of Data**: Implement security measures to protect data as per the instructions of the data controller.
- **Assist with Data Subject Rights**: Assist the data controller in fulfilling obligations related to data subject rights (e.g., access, rectification, erasure).
- **Sub-processing**: If subcontractors or sub-processors are used, ensure that they adhere to similar data protection standards.

Data Protection Officer (DPO)

- **Compliance Monitoring**: Oversee and ensure compliance with the DPDP and other data protection regulations.
- **Training and Awareness**: Conduct training and awareness programs within the organization on data protection principles.
- **Data Protection Strategy**: Develop and implement the organization’s data privacy policies and strategies.
- **Advisory Role**: Advise on Data Protection Impact Assessments (DPIAs) and ensure they are conducted when required.
- **Liaison with Authorities**: Act as the point of contact for data protection authorities and data subjects.

Third Parties and Sub-processors

- **Third-party Agreements**: Ensure contracts with third parties, such as service providers, align with the DPDP regulations regarding data handling and privacy.
- **Monitoring Compliance**: Ensure that third parties or sub-processors comply with the same data protection standards as the data controller.

Employees

Employees and staff who have access to personal data have the following responsibilities:

- **Confidentiality**: Maintain confidentiality of the personal data they handle and protect it from unauthorized access.
- **Compliance with Policies**: Follow the organization's data protection policies and procedures.
- **Reporting Violations**: Report any data protection breaches or concerns to the appropriate authorities within the organization.

Legal & Regulatory Compliance

- **Regulation Adherence**: Stay updated with local and international data protection regulations (such as the DPDP) and ensure organizational compliance.

- **Data Breach Notification**: Ensure that the organization complies with timely notification requirements in the event of a data breach.
- **Periodic Audits**: Conduct internal or external audits to ensure compliance with the DPDP Act and other applicable data protection laws.

Data Breach Management

- **Incident Response Plan**: Develop and maintain an incident response plan for data breaches, ensuring quick identification, containment, and resolution of breaches.
- **Notification of Breaches**: Notify regulatory authorities and affected individuals within stipulated timelines in case of a data breach.
- **Record Keeping**: Maintain a record of all data breaches, including their nature, effects, and remedial actions.

Data Security

- **Data Encryption**: Implement encryption techniques to secure personal data in storage and during transmission.
- **Access Control**: Ensure that only authorized personnel have access to personal data.
- **Security Audits**: Regularly audit data security systems and processes to identify vulnerabilities.

5. Collection of Customer Data

The course of the relationship with the Relevant Individual, Polycab needs to collect Customer Data. Depending on the applicable legal requirements, consent may be obtained from the relevant parties before collecting data. The type of Information that may be collected includes (but is not limited to), where relevant:

Name, gender, residential / correspondence address, telephone number, email address or other contact information; Signature and Photograph; payment instrument details; or any other detail for providing services.

6. Collection of Personal Data from Employees

- Recruitment, engagement, or training records including CVS's, applications, notes of interview, applicant references, qualifications, education records, test results.
- PAN, Aadhar, name, contact number, mail id, DoB, Driving license, photo, thumb impression, Face Scanning for Attendance, Bio metric, Eye Scan, criminal data
- Information about the Relevant Individual's medical condition – health and sickness records. Height, weight
- The terms and conditions of employment/engagement, employment contracts with Polycab and/or previous employer.
- Performance, conduct, and disciplinary records within Polycab and/or with previous employers; mobility records generated in the course of employment/work with Polycab.
- Leave records (including annual leave, sick leave and maternity leave).
- Financial Information relating to compensation, bonus, pension and benefits, salary, travel expenses, tax rates, taxation, bank account, Bank Name, IFSC Code, Personal Address PAN, provident fund account details.
- Information captured as result of monitoring of Polycab assets, equipment, network owned and/ or provided by Polycab.
- Any other information as required by Polycab.

7. Procedure

This policy covers how customers/employees/Contractors/Suppliers data are handled in Polycab

7.1 Confidentiality

It takes all the required steps to ensure that all data being held or processed will be protected and safeguarded. Some of the things that are likely to be confidential, but may well not be subject to Data Protection, include:

- Information about the organization (and its strategies, plans, or finances)
- Information about other organizations, since Data Protection only applies to information about individuals.
- The information, which is not recorded, either on paper or electronically
- Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a "relevant filing system" in the Data Protection Act

7.1.1 Understanding of Confidentiality

It is important to set out who has access, to which data, for which purposes. Access in this case means not just by staff, but also by people outside the organization. Normally access will be defined on a "need to know" basis; no one will have access to information unless it is relevant to their work. This may be relaxed in the case of information that poses a low risk: for example, a list of business contacts may be made generally available, even if this means people having access who don't strictly need it.

7.1.2 Communication with Data Principles

Polycab will have a privacy statement for Data Principles, setting out how their information will be used, and this will be available on request.

7.1.3 Communication with staff

Staff, consultants and contract workers are required to sign the terms and conditions statement & consent indicating that they have been made aware of their confidentiality responsibilities.

7.1.4 Authorization for Disclosures

Where anyone within Polycab feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with the authorization of the DPO. All such disclosures will be documented.

7.2 Data Privacy and Security Controls

This section of the policy only addresses security issues relating to personal data. It does not cover the security of the building, business continuity, or any other aspect of security. POLYCAB has identified the following risks:

- Information passing between the office and branches could go lost or be misdirected.
- Staff with access to personal information could misuse it.
- Contract workers could continue to be sent the information after they have stopped working for POLYCAB, if their records are not updated promptly.

- Poor web site security might give a means of access to information about individuals once individual details are made accessible online.
- Staff may be tricked into giving away information, either about customer information or internal employee information to colleagues, especially over the phone, through “social engineering”.

7.2.1 Security levels

Security is an integral part of POLYCAB from the day of operations. We have implemented tight controls in terms of securing the information systems; all our information systems are kept under continuous monitoring. Security violations found are reported to the incident management team and made sure they are followed until the closure.

7.2.2 Handling of customer data by Polycab Employees

- If employees are required to read customer data as part of their work, this data shall never be disclosed to any person not directly concerned with that work.
- If employees believe that someone is deliberately attempting to read or handle customer data, not within their official duties, the facts must be reported immediately to their manager, or the Cyber Security Team or a member of the senior management team.
- Employees working with personal data and on leaving the room they must either lock the data away or ask another authorized member to be responsible for the data until they return.
- Polycab – Confidential(paper) information left unlocked in an unattended room will be kept in secure locked cupboards or cabinets or in a secure filing room when not in use and will not be taken out of the POLYCAB premises except for specified purposes authorized by the concerned owner and or by Management of POLYCAB.

7.2.3 Monitoring & enforcement

The monitoring controls are enforced through set process as part of continual improvement. POLYCAB has implemented all physical and logical controls to ensure that the privacy of data is maintained.

7.3 Handling employee data at Polycab

A single database holding basic information about all employees by HR. A separate register shall be maintained for the supporting, visitors and temporary employees if any working at branches. POLYCAB regularly review its procedures to ensure that its records remain accurate and consistent and, in particular:

- The Systems are designed, where ever possible, to encourage and facilitate the entry of accurate data.
- Data on any individual are held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes.
- Staff or volunteers who keep more detailed information about individuals are given additional guidance on accuracy in record keeping.

- Permission is opted from the respective owner/individuals for their choice to create, process, store, retained, destroy the data that is residing at Polycab by privacy notice.

7.3.1 Monitoring (Customer and Employee Data)

- Periodically monitor the data confidentiality and integrity

7.3.2 Storage

The data collected, processed, and prepared are carefully stored in the storage and they are appropriately managed. The backups are defined and managed to ensure that activities are managed correctly. The data stored in the central servers are managed through a defined practice. Periodical testing of the backup data is done and ensured that they are appropriate and ensured that there is no loss of data.

7.3.3 Retention periods

The established retention periods as per the Data Retention Policy & Schedule.

The following are the categories of data that is retained:

- All forms of Customer data
- Employees, Consultants, Staff, Seasonal workers information
- Backup of scoped data, agreements

7.3.4 Archiving

Archiving of data happens during the defined period. The backup data are moved to the archival mode after the defined period of storage. Archiving of data is appropriately handled and only the important data is moved. The data related to customer data and transactional information is stored for eight years. The data storage can be also being based on the customer requirement defined in the contracts.

7.3.5 Data Disposal

Maintains all the data as per the applicable statutory, and regulatory requirements. Data is disposed of as per the disposal procedure, where it is ensured that the data cannot be retrieved once destroyed.

Refer Media Disposal Procedure (IT Asset Life cycle Management Policy)

7.4 Access Request

Any requests for access will be handled by the Privacy Steering Committee.

Processing of the request will be based on the approval from BU Head

7.4.1 Provision for verifying identity

Prior to disclosing any information, the identity of the individual making a subject access request and the purpose of the request will be carefully verified.

7.4.2 Access to Data

The required information will be provided in the permanent form either is Read-only or Read and Write unless the applicant makes a specific request, which is approved by BU Head. By default, every user shall be provided access to the data based upon their roles and on the business reasons for which they are supposed to have access.

7.4.3 Disclosure and Transparency

POLYCAB is committed to ensuring that in principle Data Subjects are aware that their data is being processed and

- For what purpose it is being processed.
- What types of disclosure are likely; and
- How to exercise their rights in relation to the data.
- How long the data will be held

Data Subjects will be informed in a formal way about their data which will be processed and will be clearly stated that their scoped data shall be securely stored. The people working on the data are being made aware of the sensitivity of the data they are handling and on a periodic basis have been re-evaluated and trained if required to handle such data.

7.4.5 Responsibility

The responsibility of handling data will be with every employee who has access and works on it and his reporting manager. POLYCAB will take all necessary steps to store data securely and handle it with a great amount of care.

7.5 Compliance with legislative and contractual obligations

POLYCAB has obligations to maintain confidentiality under the following legislation and guidance:

- All business functions shall be committed to adhere to these requirements and aim to bring a compliance culture in the organization.
- Customer data will not be held on personal computer; if the business needs to perform day-to-day activities, such requests must be reviewed and approved by concerned reporting authority and or BU Head.
- Will be checked regularly to ensure that all uses and especially disclosure or leakage of customer data are prevented.

7.6 Staff Training and Acceptance of Responsibilities

- Training is an integral part of POLYCAB, every employee who joins POLYCAB has to go through trainings. Every employee undergoes induction training on completion of joining formalities, which consists of HR induction and Information Security training.
- The training materials are prepared with at most care in addressing the requirements of data protection and security.
- All staff, whom they have access to any kind of personal data will have their responsibilities outlined during their induction procedures.
- Data Protection will be included in foundation training for all the employees. Exam is made compulsory to all the employees to understand the level of acceptance of the training, it has been mandated that every employee had to clear the exam failing which he needs to sit for the next session for successful completion.

7.7 Continuing training

Polycab will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervision. Information Security mailers are sent to all employees across

POLYCAB. The importance of security is also addressed through screen savers. Annual training is done to all employees to give updates on data protection.

Every employee is made to sign terms and conditions document that clearly addresses the Confidentiality clause, which is part of the NDA, the data being handled are never to be leaked during their employment and after separation from the employer. Compliance with the security policies will be a matter of random periodic review by the Cyber Security Department. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as deemed appropriate by the policies of management and Human Resources.

8. Enforcement

- Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.
- Polycab will take appropriate legal action against any individual or organization that causes harm to Polycab.

9. Training and Awareness

- The Cyber Security team shall conduct necessary awareness campaigns to sensitize the employees, contractors, vendors, and third-party partners about Polycab data security policies.

10. Review and Update

- This policy shall be reviewed annually and updated as necessary to reflect changes in process, technology, laws, or regulations

11. Control Reference

ISO Reference

- A.5.34 Privacy and protection of personal identifiable information (PII)