

Data Governance & Data Lifecycle Management Policy

Intellectual Property / Confidentiality Statement

The information in this document has been made available to Polycab India Limited on the strict understanding that it, or the information herein, will not be shown, read, or passed to any person who is not a current employee of POLYCAB. This Policy has been developed by Polycab India Limited and its subsidiaries (POLYCAB) and is strictly confidential and applicable to all POLYCAB employees.

Document Approval:

This document has been approved by below-mentioned authorities.

Sr. No	Name	Designation	Date	Signature & Approval Status
1	Mr. Gyan Pandey	Chief Digital & Information Officer (CDIO)	30-Sep-26	Approved
2	Mr. Pradipta Patro	Chief Information Security Officer (CISO)	30-Sep-26	Approved

Document Abstract:

This document specifies guidelines and requirements to address Data governance & Data lifecycle in Business Technology and IT Operations.

Document Title	Data Governance & Data Lifecycle Management Policy
Document Classification	Internal Revision No. 1.0
Document Publish	30 th Sep 2026
Latest Review Date	30 th Sep 2026
Review Cycle	Yearly
Review Next Review Date	01 st Oct 2027
Document Ownership	CISO
Document Author	CISO
Document Change Reviewers	CDIO
Document Circulation List	All Approvers, All Employees

Revision History				
Sr. No	Version	Date of Change	Author Revision	Description
1	V1.0	30 th Sep 2026	Sanket Mhatre	New document

Contents

1. Introduction	5
2. Scope and Applicability	5
3. Purpose	5
4. Roles and Responsibilities	5
5. Policy Statement	6
6. Core Principles	6
7. Data Governance Effectiveness KPIs	6
8. Data Classification & Labelling	6
9. Operational Procedures (SOP-Level) Data Classification Procedure	6
10. Data Lifecycle Management	7
a. Data Creation & Collection	7
b. Data Storage (On-Prem, Cloud & SaaS)	7
c. Data Consumption & Usage	7
d. Data Sharing & Transfer	7
e. Data Retention	7
f. Data Retirement & Destruction	7
11. Data Security Controls	8
12. DPDP Act Compliance	8
13. Governance	8
14. Enforcement	8
15. Review and Update	9
16. Controls Reference	9

1. Introduction

This policy will govern the end-to-end lifecycle of data at Polycab, ensuring regulatory compliance (including DPDP Act), security, accountability, and responsible usage across all systems, platforms, and digital initiatives.

2. Scope and Applicability

This policy applies to all data created, collected, processed, stored, shared, or retired by Polycab across on-premises systems, cloud platforms, SaaS applications, analytics platforms, and AI-enabled solutions.

Entities Applicable

- Polycab India Limited
- Dowells Cable Accessories Pvt Ltd.
- Polycab Support force Pvt Ltd
- Silvan Innovations Lab Pvt Ltd

3. Purpose

The purpose of this policy is to define a structured, enterprise-wide framework for managing data across its lifecycle – from creation to retirement and destruction – while ensuring data security, privacy, regulatory compliance, and business accountability.

4. Roles and Responsibilities

- Data Owner (fiduciary):
 - Senior business owner accountable for data accuracy, usage, and classification
 - Approves data usage, sharing, and retention
 - Ensures lawful purpose and DPDP compliance
- Data Steward (Processor):
 - Maintains data definitions, quality, and lineage
 - Ensures metadata, classification, and documentation are maintained
 - Coordinates with IT and InfoSec on controls
- IT / digital:
 - Provides and manages data platforms and infrastructure
 - Implements access control, encryption, backup, and monitoring
 - Ensures secure integration and data movement
- Information security & Privacy:
 - Defines security controls, data protection standards, and privacy measures
 - Ensures DPDP Act alignment
 - Conducts periodic risk and compliance reviews

5. Policy Statement

Polycab is committed to establishing robust data governance and lifecycle management practices to ensure the confidentiality, integrity, availability, and lawful use of information assets. All data—whether personal, sensitive, financial, or operational—shall be classified, protected, and managed throughout its lifecycle: creation, usage, transfer, storage, archival, retention, backup, and secure deletion. Data governance processes will define ownership, accountability, and stewardship responsibilities, ensuring compliance with ISO 27001:2022, DPDP Act, and other applicable regulations. The organization shall continuously monitor, audit, and improve its data governance framework to safeguard trust, enable transparency, and support business resilience.

6. Core Principles

- Data is a business-owned enterprise asset
- Data shall be used only for lawful and approved purposes
- Privacy and security shall be built by design
- Access shall follow least-privilege and need-to-know principles
- Data shall remain accurate, reliable, and protected
- Data retention and disposal shall follow legal and business requirements
- Data sharing and usage shall be controlled and monitored
- All data activities shall comply with DPDP Act and applicable regulations

7. Data Governance Effectiveness KPIs

- Data Classification Coverage: $\geq 98\%$ of enterprise data assets classified
- Data Owner Assignment: 100% critical datasets have assigned owners
- Data Quality Score: $\geq 95\%$ accuracy, completeness, consistency
- Policy Compliance Rate: $\geq 97\%$ adherence across business units

8. Data Classification & Labelling

All data must be classified and labelled based on sensitivity and regulatory impact. Classification determines access, encryption, retention, and sharing controls.

- Public – Non-confidential information approved for public use
- Internal – Business information for internal use only
- Confidential – Sensitive business data requiring restricted access
- Sensitive / Personal Data (PII) – Data governed under DPDP Act

9. Operational Procedures (SOP-Level) Data Classification Procedure

- Identify dataset at creation or ingestion
- Apply classification using decision tree
- Tag in metadata/catalog
- Validate by Data Steward
- Auto-enforce controls (DLP/IAM)

10. Data Lifecycle Management

a. Data Creation & Collection

- Data must be collected for a defined, lawful business purpose
- Personal data collection must follow DPDP consent and notice requirements

b. Data Storage (On-Prem, Cloud & SaaS)

- Data may reside on on-prem systems, approved cloud platforms, or SaaS solutions
- All platforms must meet Polycab security and access standards
- Data location and residency must be documented

c. Data Consumption & Usage

- Data access is role-based and approved by the Data Owner
- Data must be used only for approved business purposes
- Downstream usage (analytics, AI, reporting) must respect classification

Access: Data Owner approval (mandatory for sensitive data) → Role-based provisioning by IT → Periodic access review (quarterly) → Auto-revocation upon role change/exit

d. Data Sharing & Transfer

- Internal and external data sharing requires Data Owner approval
- Third-party sharing must be contractually governed
- Personal data sharing must comply with DPDP obligations

Raise request with purpose justification → Data Owner approval → Legal approval (if external) → Security controls applied (encryption, masking) → Agreement executed (NDA/DPA) → Audit log maintained

e. Data Retention

- Data retention periods must be defined and documented
- Retention is driven by legal, regulatory, and business requirements
- Personal data shall not be retained beyond lawful purpose

Assign retention based on classification/legal basis → Configure in system (automated lifecycle tools) → Trigger alerts before expiry → Data Owner review (extend/archive/delete) → Secure deletion (certified) → Log and audit trail maintained

f. Data Retirement & Destruction

- Data must be securely retired at end of retention period
- Destruction must be irreversible and auditable

- Deletion certificates may be required for regulated data

Lifecycle Management KPIs: Retention Compliance: ≥ 99% adherence, **Data Disposal SLA:** 100% within defined timelines, **Orphan Data Reduction:** < 2% unowned data

11. Data Security Controls

- Encryption at rest and in transit
- Strong identity and access management
- Monitoring, logging, and audit trails
- Backup, recovery, and incident response mechanisms

Security & Risk KPIs: Unauthorized Access Incidents: 0 critical / < 5 minor per quarter, **MTTD (Detect):** < 12 hours, **MTTR (Respond):** < 24 hours, **Encryption Coverage:** 100% for confidential & PII data

12. DPDP Act Compliance

This policy ensures compliance with DPDP Act requirements including lawful processing, purpose limitation, data minimisation, storage limitation, *security safeguards*, and *data principal rights*.

DPDP-Specific KPIs: Consent Capture Rate: 100% for personal data, **DSAR Response Time:** < 7 days, **Breach Notification SLA:** < regulatory threshold

13. Governance

- A Data Governance Council shall oversee policy compliance and exceptions
- Periodic audits and reviews will be conducted
- Non-compliance may result in corrective actions

14. Enforcement

Preventive Controls: Classification tagging, RBAC enforcement, Encryption policies

Detective Controls: SIEM alerts, DLP monitoring, Access anomaly detection

Corrective Controls: Incident response, Access revocation, Data remediation

Detailed RACI Matrix						
Activity	Data Owner	Data Steward	IT	InfoSec	Legal	Business
Data Classification	A	R	C	C	C	I
Data Access Approval	A	R	C	C	I	I
Data Quality Mgmt	A	R	C	I	I	C
Data Retention Definition	A	C	C	C	R	I

Detailed RACI Matrix						
Activity	Data Owner	Data Steward	IT	InfoSec	Legal	Business
Data Disposal	A	R	R	C	C	I
Data Sharing	A	R	C	C	R	I
Incident Response	I	C	R	A	C	I
Audit & Compliance	C	C	C	A	R	I
Legend:						
R = Responsible A = Accountable C = Consulted I = Informed						

15. Review and Update

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

16. Controls Reference

ISO 27001:2022

Clause 4 – Context of the Organization

4.1 Understanding the organization and its context (data governance aligned with business and regulatory context).

4.2 Needs and expectations of interested parties (stakeholders' privacy requirements).

4.3 Scope of the ISMS (include data governance and privacy processes).

Clause 5 – Leadership

5.1 Leadership and commitment (executive accountability for data governance).

5.3 Organizational roles, responsibilities, and authorities (data owners, stewards, custodians).

Clause 6 – Planning

6.1 Actions to address risks and opportunities (privacy risks, data lifecycle risks).

6.2 Information security objectives (privacy and governance objectives).

Clause 7 – Support

7.2 Competence (training for handling personal and sensitive data).

7.3 Awareness (employees aware of privacy obligations).

7.5 Documented information (policies, registers, DPIAs, retention schedules).

Clause 8 – Operation

8.1 Operational planning and control (implementing governance and privacy processes).

8.2 Risk assessment (privacy risks, data misuse, retention).

8.3 Risk treatment (controls for lawful processing, deletion, masking).

Clause 9 – Performance Evaluation

9.1 Monitoring, measurement, analysis, and evaluation (privacy KPIs, governance metrics).

9.2 Internal audit (auditing privacy and governance compliance).

9.3 Management review (reviewing governance and privacy effectiveness).

Clause 10 – Improvement

10.1 Nonconformity and corrective action (addressing privacy breaches or governance failures).

10.2 Continual improvement (enhancing governance and privacy practices).

A.5.09 Inventory of Information and Assets (data classification and ownership).

A.5.10 Acceptable Use of Information and Assets (rules for lawful data use).

A.5.14 Information Transfer (secure sharing of data).

A.5.34 Privacy and Protection of PII (explicit privacy control).

A.8.10 Information Deletion (secure disposal of data).

A.8.11 Data Masking (protecting sensitive data in use).

A.8.12 Data Leakage Prevention (preventing unauthorized disclosure).

A.8.15 Access Control to Information (restricting access to personal data).

Other policy and procedure cross reference:

- Encryption Policy
- Access Control Policy
- Log Management mentioned in Information Security Policy and Operational Security Policy
- Backup Management Policy
- Incident Management and Cyber Security Management Policy