

Information Security 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 and 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 Information Security in Business Technology and IT Operations.

Document Title	Information Security 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
2				
3				

Contents

1. POLICY SUMMARY	6
2. POLICY PURPOSE	6
3. INFORMATION SECURITY POLICY OBJECTIVE	6
4. SCOPE AND APPLICABILITY	7
General	7
Entities Applicable	8
5. LOGICAL SCOPE	8
6. PROCEDURES AND GUIDELINES	8
7. IMPLEMENTATION OF POLICY	8
8. POLICY OWNERSHIP	9
9. COMPLIANCE	9
10. INFORMATION GOVERNANCE	10
11. INFORMATION SECURITY STRATEGIES & PLANS	13
SECURITY OPERATIONS CENTRE (SOC)	13
CYBER RESILIENCE	14
RISK MANAGEMENT	15
12. POLICY STATEMENTS	15
12.1. Identification, Classification and Labelling of Information Assets	15
12.2. Data Classification	16
12.3. Segregation of functions	16
12.4. Risk Management	16
12.5. Cloud Security	16
12.6. Threat Intelligence	17
12.7. Technical Vulnerability Management	17
12.8. Mobile Devices and Remote working	17
12.9. Human Resource Security Policy	17

12.10.	Asset Management	18
12.11.	Cryptography	18
12.12.	Data Masking	18
12.13.	Operations Security	19
12.14.	Access Control	19
12.15.	Logging and Monitoring	20
12.16.	Physical Security	21
12.17.	Communications Security	21
12.18.	System Acquisition, Development and Maintenance	21
12.19.	Information Deletion	22
12.20.	Data Leakage Prevention	23
12.21.	Web filtering	24
12.22.	Supplier Relationships	24
12.23.	Intellectual property rights	24
12.24.	Secure Software Development Life Cycle Policy	25
12.25.	Configuration Management	25
12.26.	ICT Readiness for Business Continuity	27
12.27.	Maker-checker	27
12.28.	Incident Management	27
12.29.	Data Governance and Data Life Cycle Management Policy including Privacy Policy	28
12.30.	Responsible use of Artificial Intelligence and Machine Learning (AI/ML)	28
12.31.	Legal, statutory, regulatory and contractual requirements	28
12.32.	Audit Trails	28
12.33.	Protection of records	29
12.34.	Protection of information systems during audit testing	29
12.35.	Awareness Training	29

12.36. Exception Policy30

12.37. Compliance measurement30

12.38. Internal Audit30

13. CONTINUAL IMPROVEMENT31

14. POLICY VIOLATION31

15. Policy Exception31

16. Policy Compliance31

17. Review and Update32

18. Standards Reference32

1. POLICY SUMMARY

- 1.1 Information Security Policy provides a common language and systematic methodology for managing Information Security risk & highlights POLYCAB's commitment to Information security.
- 1.2 POLYCAB is committed to creating a culture of security that safeguards our customer and employee safety and privacy, reliability of service, shareholder value, and complies with all applicable laws and regulations.
- 1.3 Security policies and procedures will be updated as needed to maintain a proactive security stance at POLYCAB, address security-related requirements required by federal, state, and local laws and align with controls within industry frameworks.
- 1.4 All Information or Information security-related supporting policies and procedures must align to this Policy. Supporting policies and procedures may not expand or broaden the authorities permitted by this Policy. Business unit security policies and procedures may not supersede, counter, or reduce the controls required by the security system and specialized policies.

2. POLICY PURPOSE

- 2.1 All information and its assets are critical to POLYCAB operations and provides ability to achieve the strategic objectives of the organization. As a result, protecting the confidentiality, integrity, and availability of this information is imperative to our business.
- 2.2 The goal of this information security policy is to provide a framework to protect these assets from a wide range of threats and effectively lower the business risk. This framework will be applied when establishing, implementing, maintaining, and continually improving the information security as per the industry best standards.

3. INFORMATION SECURITY POLICY OBJECTIVE

The objective of the Information Security Policy is to set the guiding principles for establishing Information security of the implemented IT infrastructure and timely response to potential Cyber-attacks/threats. The policies define the baseline security that is appropriate for securing the IT infrastructure, underlying applications, processes, employee and customer data/information of POLYCAB in line with industry good practices.

The general security objectives comprise the following:

- Confidentiality – Information assets are accessible only to those authorized to have access (i.e., protected from unauthorized disclosure or (un)intended leakage of sensitive data)

- Integrity – Information assets are accurate, complete, and processed correctly (i.e., protected from unauthorized modification, which may include authenticity and non-repudiation)
- Availability – Information assets are resilient and accessible when required (i.e., protected from unauthorized disruption)

Additionally, the objectives of the Information Security policy are:

- Prevent occurrence and recurrence of Information incidents by implementing
 - security proactive/ protective measures.
- Create infrastructure for conformity assessment and certification of
 - compliance to Information security best practices, standards and guidelines
- Protection of client information and reduce the risks of loss to company.
 - Company stresses on securing the confidentiality, integrity and availability for all information
- Create mechanisms for security threat early warning, vulnerability
 - management and response to security threats
- Create processes, structures and mechanisms to generate necessary
 - situational scenario of existing and potential Information security threats and
 - enable timely information sharing for proactive, preventive and
 - protective actions.
- Promote and launch a comprehensive awareness program on
 - information and Information security. Ensuring that all users are aware of their responsibilities for appropriate use, protection and privacy of
 - information (including client)
- Enable effective prevention, investigation, and prosecution of
 - cybercrime and enhancement of law enforcement capabilities through
 - appropriate legislative intervention

4. SCOPE AND APPLICABILITY

General

This policy applies to all employees of POLYCAB subsidiaries and affiliates, unless otherwise expressly excluded, as well as agents and contractors of any firm system company.

Nothing contained in this policy should be construed to suggest that employees of a particular subsidiary or affiliate of one entity are also employees of another entity or any other affiliate or subsidiary of POLYCAB. Moreover, this policy does not create any employment relationship between any person and any firm system company, nor does this policy confer any contractual right to any person to become or remain an employee of any firm system company.

Entities Applicable

This Policy is applicable to all POLYCAB subsidiaries and affiliates, and all POLYCAB employees, agents, and contractors including but not limited to the following entities:

- Polycab India Limited
- Polycab Support Force Private Limited
- Dowells Cable Accessories Private Limited
- Silvan Innovations Lab Private Limited

5. LOGICAL SCOPE

Following logical assets (Information Assets) are covered under the policy:

- Electronic information (softcopy)
- Physical information (hardcopy)
- Cloud infrastructure
- Security solutions
- Applications, API, software and databases.
- Equipment and communication networks (technical infrastructure).and Information storage devices (e.g., hard disk, USB stick).
- Staff, third parties
- Online service providers
- B2B service providers
- Use of Agentic AI and Machine Learning

6. PROCEDURES AND GUIDELINES

A separate document for “Procedures and Guidelines” shall be created. It documents the detailed guidelines of how to implement the policies and standards. The key objectives of developing Procedures and Guidelines are:

- To ensure that Information Security Policy and Standards are interpreted correctly and uniformly across POLYCAB.
- To provide guidelines for implementation of the policy & standards.
- To create awareness about policy & standards and assist in their compliance.

7. IMPLEMENTATION OF POLICY

7.1. Senior Management at POLYCAB has the overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for overseeing its implementation. All

employees have a specific responsibility to operate within the boundaries of this policy, take effective steps so that all employees understand the standards of behaviour expected of them, and to take action when behaviour falls below its requirements. Employees will be given training in order that they may do so.

7.2. The effectiveness of the implementation shall be subjected to periodic audit by internal and external auditors, the audit plan for the same shall be drawn periodically in consultation with Legal and Internal Audit Leads.

7.3. In formulating and implementing this Policy, we have:

- 7.3.1. Identified reasonably foreseeable internal and external risks to POLYCAB's security, confidentiality and/or integrity of electronic, paper or other records containing Private Information
- 7.3.2. Assessed the likelihood and potential danger of these threats, taking into consideration the sensitivity of the Non-public Information
- 7.3.3. Evaluated the sufficiency of existing POLYCAB policies, procedures, and other safeguards in place to minimize those risks
- 7.3.4. Designed and implemented an approach that puts safeguards in place to minimize those risks, consistent with the requirements of applicable laws/regulations
- 7.3.5. Included regular monitoring of the effectiveness of those safeguards
- 7.3.6. All security measures contained in this Policy shall be reviewed and re-evaluated annually or when there is a change in applicable laws or regulations or in the business activities of POLYCAB. POLYCAB reserves the right to modify this Policy at any time, with or without prior notice.

8. POLICY OWNERSHIP

POLYCAB has designated CDIO and CISO to be the owner of this document.

They will be responsible for:

- Initial implementation and maintaining responsibility for implementation of this Policy;
- Appropriate testing and evaluation of this Policy's safeguards;
- Reviewing the security measures in this Policy annually or when there is a change in applicable laws or regulations or in business activities of POLYCAB and conducting training as necessary for all POLYCAB employees with access to Non-public Information.
- Implementing policies and procedures to ensure the security of Information Systems and Non-public Information that are accessible to, or held by, Third Party Service Providers.

9. COMPLIANCE

The organization expects all employees and authorized external personnel including suppliers to comply with these policies and standards. Failure by any employees of POLYCAB to conform to applicable policies and standards may result in disciplinary action. Supplier users shall be dealt with according to the contracted covenant.

10. INFORMATION GOVERNANCE**10.1. INFORMATION SECURITY GOVERNANCE STRUCTURE**

Information Governance Committee comprises of senior management as under:

- Chief Information and Digital Officer (CDIO – Chairperson)
- Chief Information Security Officer
- Head – IT Infra and Applications
- Head – Digital
- Head – ERP
- Head – Legal
- Chief Financial Office
- Head – Risk

10.2. ROLES AND RESPONSIBILITIES

Well-defined roles and responsibilities of Senior Management are imperative, while implementing Information Security Governance, Stakeholders include:

Information Governance Committee:

- Set the tone for security risk management by clearly communicating to senior management the need to address security issues and create a culture that views security as “a corporate social responsibility” with adequate staffing and budget.
- The Senior Management at POLYCAB has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for overseeing its implementation to IT Department. Review and approve Risk Treatment Plans that align with the overall business strategy.
- Responsible for advising and making POLYCAB employees understand about the Information security risks to the company to ensure that they are adequately addressed from a governance perspective.
- Should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the Board meeting agenda.

CISO

- Provide security governance by informing and driving consensus on the proper risk tolerance level through establishing vision; rules, principles, system and specialized policies (control objectives) and procedures, and practices; and setting the standard of performance for POLYCAB.
- Provide oversight by evaluating, monitoring, and reporting on the design, operation, and maintenance of Information security control activities performed by the business units (first line of defence) per the expected standard of performance established under governance.

- Provide advisory services to business units for business planning, risk treatment, and common operating picture as well as strategic intelligence management, investigation, and incident management.
- Receive frequent and routine updates on the security posture and strategy, to include discussions on which security risk should be avoided, accepted, mitigated, or transferred through insurance, as well as the specific plans associated with each approach
- Understand legal implications of security risk.

Business Unit leadership:

- Identify and manage risk directly by designing and executing control activities necessary to respond to Information security risk
- Ensure business units comply with Information security system and specialized policies
- Design, implement, and operate control activities required by Information security system and specialized policies and procedures
- Classify processes and assets based on prioritization level for the area of responsibility; provide support necessary to ensure that assets are appropriately protected within their area of responsibility
- Inform the CDIO/ CISO of actual or potential Information security policy and standard, procedures and control violations impacting their assets
- Ensure timely completion of Information security assessments
- Are responsible for information security controls implementation and management of Information security risk within their business unit
- Assign representative to liaise with IT Team

All Polycab employees shall:

- Comply with this Policy and all policies that specify Information security actions.
- Immediately report known, suspected or potential violations of this Policy by contacting the IT Department
- Cooperate with efforts undertaken by the IT Department

10.3.COMMUNICATION

POLYCAB has established and implemented a communication process for internal and external interested parties in support of its information security.

The following table describe various activities of Information Security are communicated within organization and external interested parties:

Activities to be communicated	When to communicate	Who shall communicate	Whom to communicate	Channel to communicate	Reference
Information Security Policy and other relevant security-based policies	As & when/Yearly	Senior Management	All employees, Third party contractors and vendors	Via Email, Internal team meeting	Information security policies and other supporting documents
Organization roles, responsibilities & authorities	As & when/Yearly	Senior Management	Identified resources for information security management	Email Internal team meeting	Information security Roles and responsibilities
Risk Assessment & Risk treatment	As & when/Yearly	Senior Management	To all service leads and functions	Internal meetings Email	Risk management methodology
Communication on security breach or incident at the organizational level	As & when	Senior Management	External and internal interested parties including customers, regulatory authorities and Suppliers	Email Phone	Incident response procedure
Crisis or contingency	As & when	Senior Management	External and internal interested parties including all employees, regulatory authorities and contractors	Email Phone	Incident response procedure
Performance evaluation	Half yearly	CISO	Senior Management/CISO of POLYCAB	Email Management review meetings	Measurement of Effectiveness of Security Controls
Internal Audit of Information Security	Half yearly	CISO	To all Departments and offices	Email Newsflash	Process for internal audit
Management Review	Half yearly	CISO	Senior Management	Senior Management review meetings	Information Security Policy

10.4. LEADERSHIP AND COMMITMENT TOWARDS INFORMATION SECURITY

Management of POLYCAB shall provide evidence of their commitment to the establishment, implementation, operation, monitoring, review, maintenance, and improvement of the information security controls and by:

- Reviewing and modifying the Information Security policy and objectives that are compatible with the strategic direction of POLYCAB management.
- Establishing roles and responsibilities for information security within the Organization
- Communicating to the organization the importance of meeting the Information security objectives, conforming to the information security policy, POLYCAB's responsibilities under the applicable laws & regulations and the need for continual improvement
- Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the information security practices
- Directing and supporting the personnel who contribute to the effectiveness of the information security
- Supporting other relevant management roles within POLYCAB to demonstrate information security managements' leadership as applicable to their area of responsibility
- Determining the criteria for accepting risk and acceptable levels of risk
- Confirming that internal audits are conducted for information security
- Conducting management reviews of the information security
- Confirming that corrective actions are taken based on the outcome of internal audits, management reviews, security incidents and external audits etc. and thus promoting continual improvement and confirming that the information security practices achieve its intended outcomes.

11. INFORMATION SECURITY STRATEGIES & PLANS**SECURITY OPERATIONS CENTRE (SOC)**

- The responsibilities of the SOC shall include –
- Detecting security incidents related to attacks or anomalies through continuous monitoring of IT infrastructure.
- Analyse the logs of critical infrastructure during normal working conditions and in the event of crisis.
- The SOC shall be responsible for reporting, tracking, monitoring, and closure of incidents.
- Determine the scope of an internal investigation once an attack has occurred
- Identify and classify incidents.
- Assess threat intelligence and the proactively identify/visualize impact of threats on the organization.
- Identify threat vectors and develop use cases for security monitoring.

- Develop and maintain the technical architecture of the Security Incident and Event Management (SIEM) tool enabling all the components to perform as expected.
- Inform incidents to the CDIO and take appropriate action for cyber-attacks.
- Conduct follow-up reviews on the effectiveness of the organization's response to an actual attack.
- Review the SLAs for reporting and response against incidents that have been identified. Share periodic SLA reports to Information Security COE.
- Conduct any investigations within the determined scope.
- Promote Information security awareness within departments.
- POLYCAB shall establish a SOC to combat Information threats that will form a governance layer on top of the existing SOC.
- The responsibilities of the SOC shall be-
 - Providing threat intelligence
 - Information threat analysis across security domains
 - Information security incident management
 - Information security training
 - Information Crisis Management

CYBER RESILIENCE

Information resilience is defined as the ability of the organization to anticipate, withstand cyber-attacks and the capability to contain, recover rapidly and evolve to improved capabilities from any disruptive impact caused due to cyber-attacks. Below practices are to be exercised & tested to withstand Cyber-attacks:

CISO shall develop various exercises such as crisis simulation exercises, mock drills etc. which assess the adequacy and consistency of Information crisis management plan.

Red team testing exercise shall also be performed to measure the POLYCAB's defensive and responsive capabilities. These exercises & tests shall be conducted at planned intervals or whenever significant changes occur.

Resiliency tests are based on appropriate scenarios that are well planned and clearly defined aims and objectives. Resiliency tests outcomes shall minimize the risk of disruption of operations. Produce post exercise reports that contain outcomes, recommendations, and actions to implement improvement.

Information will be gathered through monitoring of the security testing mentioned below to be conducted at least once in a year with a specific schedule decided by the Internal Audit Team. This will help to drive continuous improvement of POLYCAB's Information security practices.

As a part of annual activity, following security audits and assessments need to be conducted:

- Vulnerability Scans/Penetration test (Internal & External)
- Application Scans and configuration review
- Internal Audits
- External Audits
- Risk Assessment
- IT DR plan review
- Information Security Operation Centre Review
- Information crisis management plan
- Investigation of Incidents
- Approval for publishing Applications.
- Change Management Process and Flow Review
- Security Certifications
- Source Code review
- Defining the scope of the security audit or assessment
- Assessing risk by reviewing compliance with security controls
- Identifying noncompliance and Documenting findings
- Risk remediation or risk acknowledgment
- Validation of risk treatment by the Risk Owners
- Vendor risk management review
- Review of Risk Appetite

RISK MANAGEMENT

- Failure to adhere to this policy and the procedures may put the organization at Information risk from Information security incidents.
- Information security incidents can result in a broad range of negative consequences, including reputational loss, financial loss, non-compliance with standards and legislation and liability to third parties. An Information security Incident could occur at any point of the life cycle of the affected information (i.e., at its creation, collection, use, processing, storage, disclosure, deletion, or destruction).
- POLYCAB will therefore regularly undertake risk assessments to identify, quantify, and prioritize risks associated with its Information security and subsequently develop controls to mitigate such risks. POLYCAB will undertake risk assessments using a consistent and systematic approach.

12. POLICY STATEMENTS

12.1. Identification, Classification and Labelling of Information Assets

The Company assets shall be identified and defined with appropriate protection responsibilities, ensure that information receives an appropriate level of protection in accordance with its

importance to the Company, and prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

The information asset team shall maintain and update an inventory of all information assets (in Service Management Portal). This inventory shall be categorized into five main types: hardware, software, services, Licenses and information. The assets inventory shall contain asset identification, description, location, classification, Owner, Custodian etc.

Refer: IT Asset Life cycle Management Policy

12.2. Data Classification

- 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

Refer: Data Governance and Data Life Cycle Management Policy

12.3. Segregation of functions

The IT and Cyber Security functions shall be segregated to reduce the risk of unauthorized activity or access to operational systems or data. Responsibilities must be assigned to individuals in such a way as to mandate checks and balances within the system and minimize the opportunity for unauthorized access and fraud.

Refer: IT Roles & Responsibilities in various policies

12.4. Risk Management

A risk management process must be used to balance the benefits of using technology including cloud computing with the security risks including but not limited to, vendor lock-in, associated with handing over control to a vendor.

Refer: IT Risk Management Policy

12.5. Cloud Security

Polycab is committed to ensuring the security of its data stored in cloud environment by maintaining confidentiality, integrity, and availability (CIA) of information. The Company will implement adequate controls to mitigate risks, comply with business, legal, regulatory, statutory, and contractual requirements, and ensure seamless and secure operations in the cloud.

Refer to Cloud Security Policy

12.6. Threat Intelligence

Polycab shall identify all the threats posed to the company. It shall identify means of collecting intelligence for such threats on an ongoing basis. It shall use the threat intelligence as inputs to downstream processes/to establish controls so that the corresponding risks can be mitigated.

Refer: Threat Intelligence Policy

12.7. Technical Vulnerability Management

Defines a systematic process for identifying, assessing, prioritizing, and remediating technical vulnerabilities across all IT assets. Vulnerability scans, penetration tests, and threat intelligence feeds will be used to proactively detect weaknesses, and remediation will be prioritized based on severity, exploitability, and business impact. Antivirus solutions shall be implemented on every endpoint.

Refer: Antivirus and Malware protection policy, Technical Vulnerability Management Policy, Secure system architecture and engineering principles

12.8. Mobile Devices and Remote working

Defines the guidelines for employees working outside the company's premises, whether from home or other locations. It specifies that mobile devices used for work are personal devices, with only certain company-approved applications provided and managed by the organization. The policy outlines acceptable usage, security measures, and responsibilities to ensure data protection and productivity while working remotely.

The policy ensures that employees have clear instructions on how to securely use personal mobile devices for work-related tasks while maintaining the security of company data. It helps mitigate risks related to unauthorized access and data breaches. By defining the scope of company-provided applications, the policy ensures that sensitive company information remains secure, even when accessed remotely.

Refer: Mobile & Remote Policy, Acceptable Usage Policy, Social Media Policy

12.9. Human Resource Security Policy

The Human Resource Security Policy specifies the information security requirements that need to be integrated with the HR processes such as recruitment, separation and throughout the employment life cycle or change of employment. This policy covers controls that need to be implemented for all employees for adherence to information security practices.

The objective of this policy is to:

- Ensure that the employees understand their responsibilities and roles regarding information security
- Have an adequate organization-wide training and awareness program for information security

- Safeguard information throughout the employee lifecycle
- Reduce the risks due to human error, theft, fraud or misuse of information assets and facilities
- Minimize the damage from the security incidents and malfunctions and learn from such incidents

Refer: Human Resource IT Security Policy, Security Awareness & Training Policy

12.10. Asset Management

The Asset Management Policy specifies the importance of physical and information assets including identification of the asset owner, asset classification and determining confidentiality, integrity and availability ratings of the assets. The policy establishes the requirement of controls that need to be implemented for protecting information assets. The scope of this policy covers the following:

- Asset requisition and maintenance
- Asset allocation
- Asset return and replacement
- Asset disposal
- Asset Movement

In addition to physical assets, information assets of Polycab shall receive comprehensive protection and shall have an identified owner. The objectives of the policy are to ensure that:

- An information asset register documenting the types of information assets of each business function is maintained
- The information assets of each business function have designated owners and custodians
- The CIA (Confidentiality, Integrity and Availability) ratings of information assets are defined
- IT assets are procured, maintained and disposed of as per the defined process

Refer: IT Asset Life Cycle Management Policy, IT Physical Security Policy, BYOD Policy

12.11. Cryptography

The policy on cryptography ensures that all the cryptographic services meet the requirements that are needed to protect the confidentiality, integrity and authenticity of the information assets.

IT team shall be responsible for the implementation, maintenance and authorization of cryptographic controls. It is their responsibility to see the development, usage and protection of keys during their lifecycle.

Refer: Cryptography Policy

12.12. Data Masking

Data Masking is a vital security measure employed to safeguard sensitive information by altering original data with realistic yet concealed content. This practice shields personally identifiable or

sensitive data from exposure in non-production settings or when shared with individuals who do not require complete access to the authentic data.

Our policy outlines the specific data categories subject to masking, details the methodologies and tools utilized for this purpose, establishes stringent access controls, and defines monitoring and auditing guidelines for data masking practices. These protocols ensure the confidentiality and privacy of sensitive data, ensuring compliance with regulatory requirements and organizational security standards.

12.13. Operations Security

This policy addresses safeguarding of information and computing resources from various business and environmental threats, by ensuring documentation of operating procedures, defining a process for change and capacity management, Logging & Monitoring, backup procedures, vulnerability, installation of software, malware and patch management.

It establishes appropriate controls that need to be implemented to prevent unauthorized access, misuse or failure of the information systems and equipment and to ensure confidentiality, integrity and availability of information that is processed by or stored in the information systems/equipment.

Polycab shall ensure the effective and secure operation of its information systems and computing devices. Appropriate controls shall be implemented to protect the information contained in and/or processed by these information systems and computing devices.

The objectives of this policy are to: -

- Identify, and document operating procedures and responsibilities for information systems
- Protect information assets from the adverse impact of malicious code and ineffective capacity management
- Develop an appropriate backup procedure for ensuring the availability of information and communication services
- To ensure management of technical vulnerabilities of information systems.
- Conducting at least annual audits to minimize disruptions to business processes by highlighting security gaps and taking appropriate actions to mitigate it.

Refer: Change Management Policy, Patch Management Policy, Backup Management Policy, Capacity Management Policy

12.14. Access Control

Polycab shall establish, document, and enforce an access control policy to ensure that access to information, systems, and resources is authorized, appropriate, and regularly reviewed. Access rights must be granted on the principle of least privilege, aligned with business and security requirements, and revoked promptly when no longer required.

Refer: Access Control Policy, Password Management Policy, Mobile and Remote Access Policy

12.15. Logging and Monitoring

IT team shall ensure the event logs have recording of critical user-activities, exceptions and security events to assist in future investigations and access control monitoring:

- The activities of privileged users such as system administrators shall be logged and independently reviewed on a regular basis.
- All access to critical applications and Polycab network shall be monitored for suspicious activities or security breaches. Adequate response mechanisms shall be in place for containing security breaches.

The audit logs shall be retained based on the record retention requirements.

Logging facilities and log information shall be protected against tampering and unauthorized access.

The clocks of all relevant information processing systems within Polycab shall be synchronized with an agreed accurate time source.

It shall be ensured that the system administrators do not have permission to erase or de-activate logs of their own activities.

Activity logs shall be generated, monitored, and retained for the following:

- Authorized access
- Privileged operations
- Unauthorized access attempts
- Audit Logs

Changes to, or attempts to change, system security settings and controls.

The results of monitoring activities shall be reviewed at specified intervals. The intervals shall be decided as per the criticality of the information systems.

The fault logs, security logs, access logs and activity logs shall always be enabled and protected from unauthorized access, modification, or destruction.

Refer:

Backup policy and procedure

CERT-In requirement

Hardening documents for specification of logs to be enabled

Operational Security Policy

12.16. Physical Security

Security of information must be taken into account in all forms of its existence, including physical access to information systems, computers, and information in written, spoken, or otherwise stored form. Physical security includes:

- Securing your workstation, your working place, office area, or working with information remotely with secure-aware manners are all relevant elements in building a secure working culture.
- Outside of the home, unattended portable devices like laptops, portable storage, and media must be physically secured (e.g. with a cable) or securely stored out of sight (e.g. locked drawer). A screen lock must be activated on unattended computers, laptops, smartphones, and tablets.
- Devices are not to be left unattended when in public.
- The office location shall have cameras, burglar and smoke alarms, secure printing, badges, and locked storing room/cabinets, and a locked cupboard for storing sensitive information.

Refer: Physical Security Policy, Clear Screen Clear Desk Policy

12.17. Communications Security

IT Communications security shall be implemented by IT functions to protect organization's network. The policy shall ensure that network-related documentation (e.g. – SOPs, Network Diagram, Network Device hardening documents) is maintained and updated regularly. Suitable information security controls shall be implemented for safeguarding the Organization's infrastructure and systems.

- The primary objectives of a network security policy shall ensure that access to Company's network is only provided to authorized users and that adequate controls are in place to manage remote users
- All hardware equipment such as servers and switches must be configured for allowing required services only
- Networks shall be segregated, and appropriate network routing protocols are enabled.

Refer: Network Security Policy, Mobile and Remote Access Policy, email usage procedure

12.18. System Acquisition, Development and Maintenance

The Information systems acquisition, development and maintenance policy defines the security requirements that need to be identified and integrated during the development and maintenance of applications, software, products and/or services. This policy includes the requirements for system development and testing, information systems services over public network, protection of application service transactions, system change control, review of applications after operating platform changes, restriction on changes to software packages, system security testing, system acceptance testing and protection of test data.

Appropriate security controls shall be integrated during the acquisition, development, deployment and maintenance of the application software, system software, products and/or services, ensuring

confidentiality (C), integrity (I) and availability (A) of the information. This policy intends to maintain the information security of application system software and information during its lifecycle.

Refer: Secure Software Development Life Cycle Policy

12.19. Information Deletion

It is Polycab's policy to delete information that is no longer required for operational, legislative or other, justifiable reasons.

Information deletion must be carried out in compliance with Polycab retention policies which define how long various types of records must be kept for.

Consideration must also be given as to whether information may be useful to the organization in anonymized form.

Methods of information deletion may vary according to the way in which the information is stored and may include:

- Automated deletion after a specified period of time (for example for email)
- Using secure deletion software to ensure that information may not be retrieved
- For information held on paper, shredding using a cross-cut shredder
- Physical destruction of storage devices such as hard drives
- Manual deletion of information once no longer required (for example, temporary files at the end of a project)
- Restoration of factory settings (for example in the case of a mobile device)

Care must be taken to ensure that the most appropriate method of information deletion is used according to the circumstances, including consideration of the sensitivity of the information involved.

Where possible, evidence of the deletion of information (for example audit logs) must be recorded and retained for a specified period of time.

In cases where deletion is carried out by a third party, a relevant certificate or similar attestation of completion must be obtained.

The use of information deletion techniques must at all times take account of Polycab's compliance obligations under relevant privacy legislation.

Where information is to be deleted as a result of a legal request by a PII principal under relevant privacy law, care must be taken to ensure that the information involved is deleted from all locations in which it is held, including those of processors and sub-processors.

For information held in third party cloud services, due diligence must be carried out prior to contract signing to confirm that information deletion methods meet Polycab requirements.

For information that is classified as very sensitive, periodic audits must be carried out to confirm that procedures have been followed correctly and that deleted information cannot be recovered. It may be appropriate to use a third-party supplier which has specific expertise in this field for this purpose.

Refer: Media Disposal Procedure details

12.20. Data Leakage Prevention

It is Polycab's policy to monitor systems, networks and endpoint devices to detect and prevent the unauthorised extraction of sensitive information by individuals or systems.

Monitoring will be carried out in accordance with applicable legislation and solely for the legitimate interest of Polycab in protecting its sensitive information.

The following major types of information will be classified as sensitive for the purpose of this policy:

- Customer personal data
- Employee records
- Product designs and other intellectual property
- Confidential financial records

Unauthorised extraction will be interpreted as the copying or moving or otherwise exporting of sensitive data without the asset owner's permission to a location or medium that falls outside the organization's boundaries, such as a cloud service, mailbox or removable storage device.

Where technically possible, steps must be taken to restrict user access to extract sensitive data by design, such as limiting the user's ability to copy and paste within an application or preventing the connection of removable storage devices.

Technical controls must be supplemented by regular user awareness training activities which inform users about the nature of data loss and how to avoid it.

Where possible, appropriate data leakage software tools will be used to detect the disclosure of information classified as sensitive and prevent the identified action (such as file copying or sending an email) from taking place.

Unauthorised physical actions such as photographing or taking screenshots of sensitive data are not permitted and all employees of Polycab have a responsibility to report such instances to management.

Personnel found to be responsible for unauthorised extraction of information falling under the remit of this policy may be subject to disciplinary action. In some circumstances a targeted programme of awareness training may also be appropriate for those found to have breached this policy.

Refer: Data Leakage Prevention Policy

12.21. Web filtering

Access to the Internet from devices provided by Polycab will be monitored in order to ensure that exposure to malicious content is minimised.

Where possible, this will include access via networks outside of the control of Polycab, such as broadband connections when working from home or when mobile working.

Monitoring will at all times comply with relevant legislation within the employee's country of employment.

Access to websites that are considered to be inappropriate will be blocked to the user. Specific, business-justified requests to access blocked websites may be allowed by management on an exception basis.

A list of categories of websites that will be blocked will be maintained by the [ICT Team]. In general, these will include websites which:

- Host malware or are involved in phishing activities
- Are concerned with illegal content, such as file sharing
- Provide inappropriate content, such as sexually explicit, illegal drugs, intolerance, violence and weapons
- Host downloads of specific file types, such as executables

Access to web-based email will be allowed but must be used with caution. File downloads of allowed file types will be permitted.

12.22. Supplier Relationships

The failure of a service provider in providing a specified service, a breach in security/ confidentiality, or non-compliance with legal and regulatory requirements by them may lead to financial losses or loss of reputation for the organization. It is therefore imperative for organizations to ensure effective management of the risks due to outsourcing.

The objective of this document is to ensure that access and usage by third parties to the organization's information systems, information processing facilities, physical facilities and Intellectual Property Rights are controlled and protected from all third parties.

Refer: IT Supplier Security Policy

12.23. Intellectual property rights

Polycab shall identify, respect, and protect intellectual property rights (IPR) in all its operations. Employees, contractors, and third parties must ensure that copyrighted materials, trademarks, patents, software licenses, and proprietary information are used only in accordance with applicable laws, contractual obligations, and organizational policies. Unauthorized use,

reproduction, or distribution of intellectual property is strictly prohibited, and compliance with licensing terms shall be monitored and enforced

12.24. Secure Software Development Life Cycle Policy

The purpose of this policy is to ensure that security is integrated into every phase of the software development life cycle, reducing risks and protecting organizational assets, customer data, and regulatory compliance.

This policy applies to all software development projects, including in-house, outsourced, and third-party integrations at all stages of development as under:

- Planning & Requirements
 - Security requirements must be defined alongside functional requirements.
 - Regulatory and compliance obligations (e.g., data protection laws) must be considered.
- Design
 - Threat modelling and risk assessments must be conducted.
 - Secure architecture principles (least privilege, defence-in-depth, secure defaults) must be applied.
- Development
 - Developers must follow secure coding standards (e.g., OWASP, CERT).
 - Code must be peer-reviewed with a focus on security vulnerabilities.
 - Use of approved libraries and frameworks only.
- Testing
 - Security testing (static analysis, dynamic analysis, penetration testing) must be performed.
 - Identified vulnerabilities must be remediated before release.
- Deployment
 - Secure configuration management must be enforced.
 - Secrets (keys, passwords) must be managed securely.
 - Continuous monitoring for vulnerabilities must be enabled.
- Maintenance
 - Regular patching and updates must be applied.
 - Incident response procedures must be in place for discovered vulnerabilities.
 - Periodic security audits must be conducted.

Refer: Secure Software Development Life Cycle Policy

12.25. Configuration Management

Polycab uses a wide variety of components in creating and running its ICT infrastructure and end-user devices. These consist of hardware, software, cloud services and networks and all are potentially vulnerable to attack from threats from different sources. In order to lessen the risk of

these components becoming compromised, it is important that we identify the most appropriate ways of configuring them and then ensure that these methods are used throughout our ICT landscape.

This policy describes the main principles on which such standard configurations must be based and sets out the rules for their use.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Polycab systems.

New components that make up Polycab's hardware, software, services and networks must have their required security settings defined and correctly configured prior to their implementation within our ICT environment.

Configurations of existing components must be reviewed periodically to ensure they meet the requirements of this policy.

Such components will include, but are not limited to:

- Endpoint devices, such as desktops, laptops, mobile phones and tablets
- Physical network devices, such as routers, switches and firewalls
- Physical servers, including system software such as operating systems, databases and web servers
- Cloud infrastructure, such as virtual servers, networks and storage

Where possible, standard templates will be used to document the required configuration of ICT components. These templates will be subject to change and version control.

The configurations defined will take appropriate account of available sources of information about securing the relevant components, such as vendor templates, guidance from cyber security authorities and best practice organizations, system hardening guides and our own information security policies.

Details of configuration standards will be protected as sensitive information which would be of use to an attacker.

Configuration standards must be reviewed on a regular basis and kept up to date with changes in the components themselves (such as new hardware or software versions) and the threats and vulnerabilities they face.

The correct configuration of components will be monitored and instances where existing settings deviate from the established standard will be investigated and, if necessary, corrected.

Automated audit tools may also be used to check configurations regularly and report on and correct those found to be noncompliant.

12.26. ICT Readiness for Business Continuity

The business continuity management policy defines the set of rules which help the critical business process of any organization to function during any disturbance such as failures of the system or disasters. The business continuity management policy defines the controls to establish a framework to counteract interruptions to business activities and to protect the critical business processes from the effects of business disruptions such as major failures, disasters, etc. and their timely resumption.

To have a planned response in the event of any contingency ensuring recovery of critical activities at agreed levels within the agreed timeframe thereby complying with various requirements and minimizing the potential business impact. Additionally, to create a system that fosters continuous improvement of business continuity management.

Business Continuity Planning Objectives shall ensure:

- Business continuity plan
- Crisis communication plan
- A proactive response to any contingency.
- Recovery of identified critical activities within an agreed timeframe.
- The details on the aspects of planning, implementing, verifying, reviewing and evaluating continuity shall be documented in the following documents:

Refer: BCP & DR Policy

12.27. Maker-checker

The Maker-Checker process involves two roles: the Maker who creates or initiates actions, and the Checker who reviews and approves them. It ensures accuracy, prevents fraud, and maintains accountability by separating responsibilities. This process minimizes risks and protects sensitive data. It is essential for improving security, compliance, and operational integrity.

12.28. Incident Management

The objective of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within SLA limits.

Refer: Incident Management and Cyber Crisis Management Policy & Procedure

12.29. Data Governance and Data Life Cycle Management Policy including Privacy Policy

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

Refer: Data Governance and Data Life Cycle Management Policy

12.30. Responsible use of Artificial Intelligence and Machine Learning (AI/ML)

This policy governs the safe, secure, and compliant use of AI (including Generative AI) across Polycab. It is mandatory for all AI initiatives, AI-enabled platforms, internal agents, and vendor-embedded AI capabilities. The core principles that govern the responsible use of AI/ML are

- Human accountability: AI assists; humans remain responsible for decisions and outcomes.
- Security & privacy by design: AI shall not weaken data security posture.
- Enterprise-grade controls: only approved tools, subscriptions, and governed pathways.
- Auditability & traceability: AI usage, prompts, outputs and approvals must be traceable for risk and audit.
- Value and adoption over experimentation: priorities measurable outcomes and governed scaling.

Refer: AI & Generative AI Governance Policy

12.31. Legal, statutory, regulatory and contractual requirements

Polycab shall identify, document, and comply with all applicable legal, statutory, regulatory, and contractual requirements relevant to its information security management system. These requirements shall be regularly reviewed, updated, and integrated into policies, procedures, and controls to ensure ongoing compliance. Any changes in applicable laws, regulations, or contractual obligations must be promptly assessed, communicated, and implemented to maintain conformity and protect organizational interests."

12.32. Audit Trails

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including where or on what system the activity was performed from (subject)?
- What was the activity performed on (object)?
- When was the activity performed?

- What tool(s) was the activity performed with?
- What was the status (such as success vs. failure), outcome, or result of the activity?

Logging from the Company's critical systems, applications and services can provide key information and potential indicators of compromise. Logging information and reviewing them on a periodic basis would bring down the risk to the acceptable level.

12.33. Protection of records

Polycab shall establish and maintain procedures to protect records containing business, legal, regulatory, and operational information. Records must be accurate, complete, retrievable, and protected against unauthorized access, modification, loss, or destruction. Retention and disposal of records shall comply with applicable legal, statutory, regulatory, and contractual requirements, and records shall remain accessible for the duration of their retention period.

Refer: Record Retention and Protection Policy

12.34. Protection of information systems during audit testing

Protecting systems during audits is critical for integrity and data safety. Limiting auditor access using strict controls ensures only necessary data is viewed. Segregating duties prevents conflicts of interest. Secure testing environments mirror live systems, with robust logging to track auditor actions. Agreements on confidentiality enhance security. Anonymizing data shields sensitive information. Continuous monitoring identifies issues, and post-audit sanitization removes test data risks. These measures ensure confidentiality, integrity, and trust in audit assessments.

12.35. Awareness Training

Information Security awareness and training is an important aspect in protecting the Confidentiality, Integrity, and Availability (CIA) of sensitive information. Employees are the first line of defence and must be made aware of the security risks associated with the work performed at Polycab.

Polycab understands that people are often the biggest threat (intentionally or unintentionally) to the security of sensitive information. As such, all users of information systems must be made aware of the security risks associated with their activities. Those with significant security responsibilities must be adequately trained to carry out their assigned information security-related duties and responsibilities.

All employees, Contractors and anyone accessing the Company information systems must understand how to protect the CIA of information and information systems.

The Company shall ensure that all employees and contractors are given Information security awareness training during the new hire process and before accessing any Polycab systems. This training reflects common Information Security awareness specific to the Polycab environment

including, but not limited to, physical access, restricted areas, potential incidents, how to report incidents, laptop best practices, and how to spot phishing and social engineering scam.

Refer: Security Awareness & Training Policy

12.36. Exception Policy

An Exception Policy in an Information Security Management System (ISMS) defines the circumstances under which deviations from standard security policies or procedures may be allowed. It establishes the process for requesting, reviewing, and granting exceptions to established controls, ensuring that they are properly documented and justified.

The Exception Policy is important because it provides flexibility in managing unique situations where standard policies may not be practical or applicable. It ensures that any exceptions are assessed for risk and do not compromise the overall security and integrity of the organization's systems. The policy helps maintain control over deviations, ensuring that security is not compromised while allowing for necessary adjustments based on specific business needs or unforeseen challenges.

12.37. Compliance measurement

CISO shall provide security directives to achieve the security objectives at relevant functions and levels. The information security objectives shall demonstrate:

- Consistent with the information security policy
- Measurable (if practicable)
- Take into account applicable information security requirements, and results from risk assessment and risk treatment
- Communicated through management meetings
- Updated as appropriate

12.38. Internal Audit

The Internal Audit Policy establishes guidelines for independent assessments of the organization's IT systems, controls, and processes. It aims to ensure compliance with industry standards, enhance security, and evaluate operational effectiveness.

The audit shall covers all IT-related assets, services, and relevant departments, with the scope defined for each specific audit.

Such audits shall be carried out as per the audit plan

The auditor can be internal or external

Audit results shall be communicated to information Governance Committee

Refer: Internal Audit of IT policy and procedure

13. CONTINUAL IMPROVEMENT

- 13.1. Information Security office/CISO Office continually improves the suitability, adequacy, and effectiveness of the Information Security in POLYCAB through the use of the processes detailed in this policy, other supporting information security policies, information security objectives, audit results, information security incidents, performance evaluation, corrective actions and management reviews.
- 13.2. Reviewing the adequacy of the internal and external issues periodically during the management reviews; and Updating the Risk and Opportunities related to interested parties annually to ensure that it remains current and considers changes if applicable.

14. POLICY VIOLATION

- 14.1. All POLYCAB personnel (including employees, contractors, and applicable third parties) must maintain the security, confidentiality, availability, and integrity of information and their supporting assets. Violations of such professional practices and acknowledged policies may be considered serious breaches of trust, which can result in disciplinary action up to and including termination of employment or contract and prosecution in accordance with applicable federal, state, and local laws.

15. Policy Exception

- 15.1 Any exclusions to this policy shall be approved through the policy waiver.
- 15.2 Exceptions will not be universal but will be agreed on a case-by-case basis, upon official request made by the information owner. The waiver request must include, at a minimum, the following: Justification for the exception:
 - Risk due to the exception
 - The mitigation controls to manage the risk
 - The plan of action to manage the risk
 - The validity period of the exception and
 - Details of assets on which the exception is applicable

16. Policy Compliance

- 16.1 All the requirements specified in the Information Security Policy are to be followed by all employees of POLYCAB.
- 16.2 Compliance to this policy will be measured by the internal or external audits.
- 16.3 An individual or a committee found to be not complying with the requirements specified in the policy is bound to accept consequences specified in Compliance Management Policy.

17. Review and Update

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

18. Standards Reference

- A.4.3-Determining the scope of the information security management system
- A.4.4-Information security management system.
- A.5.1-Leadership & commitment
- A.5.2-Policy
- A.5.3-Organizational roles, responsibilities and authorities
- A.6.1-Actions to address risks and opportunities
- A.6.2-Information security objectives and planning to achieve them
- A.6.3 Planning of changes
- A.7.1-Resources
- A.7.3-Awareness
- A.7.4-Communication
- A.7.5-Documented Information
- A.8.1-Operational planning and control
- A.8.2-Information security risk assessment
- A.8.3-Information security risk treatment
- A.9.1-Monitoring, measurement, analysis and evaluation
- A.9.2-Internal Audit
- A.10.2-Nonconformity and corrective action