POLYCAB

Information Security Policy

Document Details

Title: 013- Information Security policy	Document Owner: Cyber Security Team
Document Author(s): Sanket Mhatre	Version: V3.0
Classification: Polycab - Internal	Release Date: 10-04-2026

Version Details

Sr No.	Version	Date	Modified By	Reviewed By	Approved By	Comments
1	V1.1	26-Apr-23	Niranjan Reddy	Niranjan Reddy	Gandharv Tongia	Initial Version
2	V2.0	04-Apr-25	Sanket Mhatre -IT Cyber Security (GRC)	Vijit Patil – CISO Ashish Anekar – IT Infra Head	Gandharv Tongia - CFO/CIO	Alignment to ISO & NIST standard
3	V3.0	15-Apr-26	Sanket Mhatre -IT Cyber Security (GRC)	Pradipta Patro - CISO	Gyan Pandey - CDIO	Reviewed with No changes

Contents

1. Introduction

This information security policy outlines Polycab's approach to Information Security Management. It provides the guiding principles and responsibilities necessary to safeguard the Company's information system to ensure a secured operating environment for its business operations.

This Information Security Policy addresses the information security requirements of:

1.1 Confidentiality: Ensures that Polycab data or information shall be accessed only by authorized users.

1.2 Integrity: Protecting information from unauthorized modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate, complete and consistent.

1.3 Availability: Ensuring information is available when it is required.

To meet this commitment Polycab shall:

- Maintain an effective ISMS
- Deploy appropriate technology and infrastructure to ensure the security of information
- Create and maintain a security-conscious culture
- Continually monitor and improve the effectiveness of the ISMS

2. Purpose:

The purpose of the Information Security Policy is to establish a framework for protecting the organization's information, systems, and assets from unauthorized access, disclosure, alteration, and destruction. It aims to ensure the confidentiality, integrity, and availability of data, while also ensuring compliance with legal, regulatory, and industry standards. The policy helps mitigate risks, maintain business continuity, and promote a culture of security within the organization. Additionally, it provides guidelines for managing security incidents, implementing controls, and safeguarding against cyber threats.

3. Scope

This policy applies to all employees, contractors, partners, and Interns/Trainees working in the Company. Third-party service providers offering services to Polycab or managing data outside the premises must also comply with this policy. The scope of this Information Security Policy includes all information, assets, and data stored, communicated, and processed within the Company, as well as the Company’s data across outsourced locations.

4. Consequences for policy violations

Violations of the following policies leads to corrective actions by company management. Disciplinary measures is determined through an investigation.

Refer : IT Disciplinary Procedure

5. Ownership

The Board of Directors is ultimately responsible for information security and is the owner of this policy.

- **Information Security Governance Committee / Management Team (IT)**

Information Security Governance Committee / Management Team (IT) The Information Security Governance Committee/Management Team (IT) is made up of leadership, organizational structures, and processes responsible for monitoring information security threats. The organizational structure of Information Security shall include the following elements

Critical outcomes of information security governance committee/Management Team (IT) include

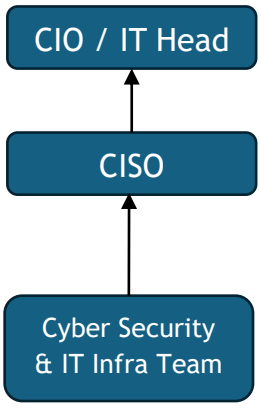
- Alignment of information security with business strategy to support organizational objectives
- Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level
- Management of the performance of information security by measuring, monitoring and reporting information security metrics(KPI) to ensure that organizational objectives are achieved
- Optimization of information security investments in support of organizational Objectives

CISO Shall approve policies, procedures and standards to ensure the security, confidentiality and privacy of information that is consistent with organizational Information Security policy

It is important to consider the organizational necessity and benefits of information security governance. They include increased predictability and the reduction of uncertainty in business operations, a level of assurance that critical decisions are not based on faulty information, enabling efficient and effective risk management, protection from the increasing potential for legal liability, process improvement, reduced losses from security-related events and prevention of catastrophic consequences and improved Polycab's reputation in the market.

The policies & procedures shall be reviewed by the owner of the document every year or at the time of any major changes in the existing Polycab IT environment, which would affect the areas, covered in the document.

Organizational Structure



- For financial approval
- Escalation of operational risk issues
- Escalations of issues
- Updates on Information Security related happenings

Roles and Responsibilities

Refer: IT Roles & Responsibilities

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.

Ref: IT Asset Life cycle Management Policy

Data Classification

Polycab – Internal confidential	This a internal label with only view permission with reply all, content cannot be copied, printed, saved or forwarded.
Polycab - Internal	This is a internal label can be used only within organization and has full permission
Polycab – Internal & External	This is confidential label with view and reply back permission and can be used with both internal and external communication
General – No Restriction	This is a common label can be used for both internal and external communication.

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

6. Risk Management

A risk management process must be used to balance the benefits of 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

7. 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

8. 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

9. 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

10. 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

11. 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. 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: Operational Security Policy

13. Access Control

The Company information assets must meet the required security controls for providing authorized access and preventing unauthorized access to IT resources and information asset based on business and security requirements. The Company users authenticate their claimed identities appropriately for the risk level of the system and/or transaction. The policy statements in this document address the controls that helps to ensure that the IT resources and information assets are properly protected against unauthorized access while meeting the access requirements for all authorized users. Critical to achieving this objective is the implementation of controls that address each of the requirements stated in the user access management policy.

Polycab's information must be safeguarded against unauthorized or illegal access through robust access control systems and procedures that maintain the accuracy, confidentiality, and availability of data. By implementing access controls across Polycab's information systems and network resources, the risk of data destruction—whether accidental or intentional—shall be minimized, and the information shall be protected from unauthorized distribution.

Ref: Access Control Policy

14. 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.

Log information shall be protected against unauthorized access, alterations and operational problems. Access to logs shall be provided on a 'need-to-know' and 'need-to-have' basis.

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

Appropriate controls shall be implemented to prevent:

- Alterations of the message types that are recorded.
- Alterations or deletions of the log files
- Exceeding the storage capacity of the logging media

15. Personnel Security

Personnel security controls are to ensure that the Company's information assets are protected from the adverse actions of personnel. It is also to mitigate the risk of legitimate access to the Company assets being exploited for unauthorized purposes. In particular, this policy serves to mitigate the "insider threat" and associated risks, the causes of which are inherent vulnerabilities arising from accidental, negligent, or deliberate(malicious) actions by a user within the Company.

The personnel security process shall include pre-employment process (e.g: employee background check and screening), training, new joiners' induction, security awareness, and termination processes.

Ref: Employees Code Of Conduct for the details

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.

Ref: Physical Security policy

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 (eg - 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

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: SDLC Policy

19. 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-Supplier Relationship Policy

20. Information Security Aspects Of Business Continuity Management

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

21. Maker-checker

he 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.

22. Incident Management

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.

Ref: Incident management procedures for the details

23. Audit Trials

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 auditing them on a periodic buasis would bring down the risk to the acceptable level.

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.

24. 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 defense 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.

Ref: Security Awareness & Training Policy

25. 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.

26. 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

27. 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 covers all IT-related assets, services, and relevant departments, with the scope defined for each specific audit. It supports the implementation of an Information Security Management System (ISMS) aligned with industry standards, focusing on risk management and IT governance.

To identify potential risks, strengthen internal controls, and promote continuous improvement in IT operations. Audits help minimize disruptions to business processes, ensure compliance with statutory and internal requirements, and verify the effectiveness of the ISMS. Regular follow-up audits ensure that previous non-conformities are addressed, fostering an ongoing commitment to security and operational excellence within the organization

Ref: IT Internal Audit Policy

28. Non-compliance to the policy

Any failure to adhere to the established rules, procedures, or standards designed to protect an organization's information and IT systems. This can include neglecting security protocols, mismanagement of sensitive data, unauthorized access, or failure to implement necessary controls and safeguards.

Non-compliance can lead to severe risks such as data breaches, financial loss, legal penalties, and reputational damage. It undermines the integrity and confidentiality of the organization's information, making it vulnerable to cyberattacks or misuse. Ensuring compliance with the Information Security Policy is crucial for protecting sensitive data, maintaining trust with stakeholders, and ensuring regulatory and industry standard adherence

Refer: Compliance Policy

29. 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