

Incident Management & Cyber Crisis Management Policy

6.- Incident Management and Cyber Crisis Management Policy and Procedure

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 to address incident management and cyber crisis management requirements in Business Technology and IT Operations.

Document Title	Incident Management and Cyber Crisis Management Policy and Procedure
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

6.- Incident Management and Cyber Crisis Management Policy and Procedure

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

Contents

1. Introduction	4
2. Scope and Applicability	4
3. Purpose	4
4. Roles and Responsibilities	4
5. Policy Statement	5
6. Incident Management Procedure	5
7. Cyber Security Incident Response Phases	6
8. Communication During an Incident	7
9. Incident Categorization and Severity Levels	8
10. Forensic Investigations	8
11. Post-Incident Review and Continuous Improvement	8
12. Incident Workflow	14
13. Policy Exception	14
14. Policy Compliance	14
15. Review and Update	15
Annexure 1: RCA Components Mandated	16
Annexure 2: Responsibility matrix	19

6.- Incident Management and Cyber Crisis Management Policy and Procedure

1. Introduction

The purpose of this document is to efficiently manage and resolve IT incidents to minimize evidence. It ensures quick identification, diagnosis, and resolution while maintaining service quality. The policy also emphasizes effective communication, accountability, and continuous improvement. Ultimately, it supports business continuity and compliance.

2. Scope and Applicability

This procedure applies to all information Technology incidents within Polycab, including security breaches, cyber-attacks, data leaks, or any event that affects the confidentiality, integrity, or availability of information. This includes incidents involving both IT infrastructure and human resources.

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

3. Purpose

The purpose of this procedure is to establish a formal framework for managing information security incidents to ensure the confidentiality, integrity, and availability of data and systems. This will help the organization:

- Detect and respond to incidents promptly
- Minimize impact and restore normal operations swiftly

4. Roles and Responsibilities

User Responsibilities

- Report security incidents immediately using the prescribed methods (Ticketing system, email, phone, etc.)
- Cooperate in incident investigation, providing any required information for analysis
- Incident Resolution Team
- Assess and determine severity of the incident
- Conduct investigation and identify the root cause of the incident
- Take corrective actions to resolve the incident and prevent future occurrences
- Escalate incidents to higher authorities if necessary (CISO, CDIO)

Incident Decision-Making Team

- Led by the CISO and includes IT Operations, HR, Legal, and Business representatives

6.- Incident Management and Cyber Crisis Management Policy and Procedure

- Make decisions regarding the containment, eradication, and recovery actions during and after the incident
- Maintain communication with external regulatory and legal authorities if necessary

Security/Forensic Experts (Internal/External)

- Investigate complex incidents, performing forensic analysis to determine the impact and collect evidence for further legal or operational actions

5. Policy Statement

Incident Management Policy

- Information security incidents shall be reported to CISO.
- All security incidents shall be responded, investigated and mitigated/resolved in a timely manner.
- Security incidents shall be reported by CISO in prescribed formats and as per prevailing guidelines to the Regulators and CERT-In.
- Root Cause Analysis (RCA) report of major incidents shall be prepared and submitted to by CISO to the Senior Management including lessons learnt and preventive steps to avoid recurrences.

Information security during disruption

Polycab shall ensure that information security is preserved during any disruption to business operations. Security controls, data protection measures, and incident response capabilities must remain effective and aligned with business continuity objectives. All employees, contractors, and third parties are required to follow established continuity and security procedures during disruptions."

Cyber security incident management policy

Polycab shall

- Identify assets to be protected from cyber-attacks and threats to those assets
- Prevent attempts of intrusion in the IT environment
- Protect information assets
- Detect intrusions and or compromises
- Respond to and recover from cyber incidents if the occur

6. Incident Management Procedure

1. Incident Logging

- Step 1: End users or analysts log the incident from one of the following sources:
 - Web Interface (<https://helpdesk.polycab.com/>)
 - Mobile App- Download the "Symphony AI Summit" app from the Google Play Store or Apple App Store.
 - Phone Call ++91 02268661799 Extensions 4930/4931/4932
 - Email helpdesk@polycab.com
 - In-person: Report directly to the IT Help Desk or IT Team

6.- Incident Management and Cyber Crisis Management Policy and Procedure

2. System Processing and Routing Logic
 - Step 2: Once the incident is logged, the service portal processes the configured routing logic.
 - Step 3: The incident is routed to the respective workgroup based on predefined rules.
3. Incident Assignment to Workgroup
 - Step 4: The incident is assigned to the appropriate workgroup, such as the Location Service Desk Workgroup.
 - Step 5: For some tickets, routing is based on the category, assigning it to the correct workgroup.
4. Service Request Validation
 - Step 6: IT Support Team validates the incident to check if it requires converting into a Service Request.
 - Step 7: If a service request is needed, the analyst converts the incident to a service request.
 - Step 8: The incident is auto cancelled once the service request is created.
5. Major Incident Validation
 - Step 9: Analyst conducts a first-level analysis, reviewing parameters like the number of users impacted, priority, etc.
 - Step 10: Based on the analysis, the analyst marks the incident as a P1/P2.
 - Step 11: The Major Incident process flow is initiated.
6. Support from Other Teams
 - Step 12: If additional support is required from another team, the analyst creates a Work Order.
 - Step 13: Follow the Work Order Process for resolution.
7. Vendor Dependency
 - Step 14: If vendor support is needed for incident resolution, the analyst changes the status to "Vendor Dependency".
 - Step 15: Respective Analyst shall follow the Vendor to get it resolved.
8. Incident Resolution
 - Step 16: If no dependencies exist, the analyst proceeds with the resolution of the incident.
 - Step 17: If L2 team support is required, the incident is transferred to the L2 team, and the L2 Incident resolution process is followed.
9. Execute Resolution Steps
 - Step 18: Analyst works on resolving the incident by executing the necessary resolution steps.
10. Incident Resolution Confirmation
 - Step 19: The analyst confirms the incident is resolved.
11. Incident Closure
 - Step 20: The incident is auto closed after 2 working days.

7. Cyber Security Incident Response Phases

The response to a security incident follows a structured, multi-phase approach:

i) Incident Discovery and Confirmation

6.- Incident Management and Cyber Crisis Management Policy and Procedure

- Identify and verify the occurrence of a security incident.
- Log and document all findings, including any suspicious activities or indicators of compromise (IOCs).
- Conduct initial risk assessment to determine the severity and scope of the incident.

ii) Containment and Continuity

- Take immediate action to contain the incident and prevent further damage.
- Protect evidence and back up compromised systems before performing any remedial actions.
- Inform relevant stakeholders and provide updates on containment efforts.

iii) Eradication

- Identify and remove the root cause of the incident (e.g., malware, unauthorized access points).
- Test systems and applications to ensure malicious code is fully eradicated.
- Ensure that no further vulnerabilities remain.

iv) Recovery

- Restore affected systems and services to their normal operational state.
- Apply patches, conduct vulnerability assessments, and reset passwords.
- Perform monitoring to ensure that systems remain secure post-recovery.

v) Lessons Learned

- Conduct a post-incident review to assess the effectiveness of the response.
- Document the incident's impact, root cause, and recovery timeline.
- Update policies, procedures, and training materials to improve future responses.

8. Communication During an Incident

Clear, accurate, and timely communication is essential during a security incident. Polycab's communication protocol includes:

- **Internal Communication:** Regular updates to staff and stakeholders regarding the incident's status, containment actions, and recovery efforts.
- **External Communication:** Timely and transparent communication with customers, partners, regulatory authorities, and the public as necessary. Communication templates are prepared in advance to ensure consistency and accuracy.
- **Sample Communication - Denial of Service (DoS) Attack:**
 - *Message:* "We are currently investigating a Denial-of-Service attack affecting our website, causing degraded performance. We assure you that no customer data has been impacted, and we are working with our ISP to restore services. Further updates will be provided."

6.- Incident Management and Cyber Crisis Management Policy and Procedure

• Sample Communication – Data Breach:

- *Message:* "At approximately 11:00 PM IST, we became aware of a potential compromise of our network and systems. We are working with internal and external experts to determine the extent of the incident. At this time, we cannot confirm whether sensitive data has been impacted. We will provide updates as soon as more information becomes available."

9. Incident Categorization and Severity Levels

Incident Factors	Severity	P4	P3	P2	P1
Systems Affected	Internal only	Internal systems/apps	Internal systems/apps	Internal & external systems	Widespread impact (internal/external)
Impact to Infrastructure		None	Minor	Partial (section affected)	Organization-wide
User/System Impact		Few users	Few users	Department-wide	Organization-wide
SLA		5 days	2 days	<= 4 hours	<= 2 hours
Resolution Availability		Readily available	Readily available	Workaround available	No available resolution

10. Forensic Investigations

For incidents involving potential criminal activity, forensic investigation may be initiated by the **Decision-Making Team**. Key steps include:

- Preserving evidence (e.g., keeping systems powered on)
- Engaging forensic experts (internal or third-party)
- Ensuring compliance with legal and regulatory requirements
- Following strict evidence handling protocols

11. Post-Incident Review and Continuous Improvement

- A **Post-Incident Review** is conducted after each major incident to identify areas for improvement.
- **Lessons learned** are incorporated into future incident management strategies and security controls.

Response Checklist

6.- Incident Management and Cyber Crisis Management Policy and Procedure

To demonstrate and improve the effectiveness of Polycab incident response team and security tools, Polycab requires a record of all actions taken during each phase of an incident. Supporting documentation is required, including all forensic evidence collected such as activity logs, memory dumps, audits, network traffic, and disk images.

PHASE OF CYBER INCIDENT	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
Incident Discovery and Confirmation	Describe how the team first learned of the attack (security researcher, partner, employee, customer, auditor, internal security alert, etc.).		
	Analyze audit logs and security applications to identify unusual or suspicious account behavior or activities that indicate a likely attack and confirm attack has occurred.		
	Describe potential attackers, including known or expected capabilities, behaviours, and motivations.		
	Identify access point and source of attack (endpoint, application, malware downloaded, etc.) and responsible party.		
	Prepare an incident timeline to keep an ongoing record of when the attack occurred and subsequent milestones in analysis and response.		
	Check applications for signatures, IP address ranges, files hashes, processes, executables names, URLs, and domain names of known malicious websites.		
	Evaluate extent of damage upon discovery and risk to systems and privileged accounts. Audit which privileged accounts have been used recently, whether any passwords have been changed, and what applications have been executed.		

6.- Incident Management and Cyber Crisis Management Policy and Procedure

PHASE OF CYBER INCIDENT	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
	Review your information assets list to identify which assets have been potentially compromised. Note integrity of assets and evidence gathered.		
	Diagram the path of the incident/attack to provide an "at-a-glance" view from the initial breach to escalation and movement tracked across the network.		
	Collect meeting notes in a central repository to use in preparing communications with stakeholders.		
	Inform employees regarding discovery.		
	Analyze incident Indicators of Compromise (IOCs) with threat intelligence tools.		
	Potentially share information externally about breach discovery. You may choose to hold communications during this phase until you have contained the breach to increase your chances of catching the attacker. If so, make sure this aligns with your compliance requirements.		
Containment and Continuity	Enable temporary privileged accounts to be used by the technical and security team to quickly access and monitor systems.		
	Protect evidence. Back up any compromised systems as soon as possible, prior to performing any actions that could affect data integrity on the original media.		
	Force multi-factor authentication or peer review to ensure privileges are being used appropriately.		
	Change passwords for all users, service, application, and network accounts.		
	Increase the sensitivity of application security controls (allowing, denying, and restricting) to		

6.- Incident Management and Cyber Crisis Management Policy and Procedure

PHASE OF CYBER INCIDENT	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
	prevent malicious malware from being distributed by the attacker.		
	Remove systems from production or take systems offline if needed.		
	Inform employees regarding breach containment.		
	Analyze, record, and confirm any instances of potential data exfiltration occurrences across the network.		
	Potentially share information externally regarding breach containment (website updates, emails, social media posts, tech support bulletins, etc.).		
Eradication	Close firewall ports and network connections.		
	Test devices and applications to be sure any malicious code is removed.		
	Compare data before and after the incident to ensure systems are reset properly.		
	Inform employees regarding eradication.		
	Potentially share information externally regarding eradication (website updates, emails, social media posts, tech support bulletins, etc.).		
Recovery	Download and apply security patches.		
	Close network access and reset passwords.		
	Conduct vulnerability analysis.		
	Return any systems that were taken offline to production.		
	Inform employees regarding recovery.		

6.- Incident Management and Cyber Crisis Management Policy and Procedure

PHASE OF CYBER INCIDENT	ACTION	TEAM MEMBER/ SYSTEM	DAY/TIME ACTION TAKEN
	Share information externally regarding recovery (website updates, emails, social media posts, tech support bulletins, etc.).		
Lessons Learned	Review forensic evidence collected.		
	Assess incident cost.		
	Write an Executive Summary of the incident.		
	Report to the executive team and auditors if necessary.		
	Implement additional training for everyone involved in incident response and all employees.		
	Update incident response plan.		
	Inform employees regarding lessons learned, additional training, etc.		
	Potentially share information externally (website updates, emails, social media posts, tech support bulletins, etc.).		

Sample Threat classification

Incident	Scope	Severity	Action
Denial of service attack/ Application attack	Limited to no impact on business apps	Low	Monitor Traffic and fine tune DDOS appliances to eliminate noise Inform ISP
	Critical business application performance impacted	Medium	Initiate incident response protocol Engage ISP Perform RCA Provide updates to affected parties

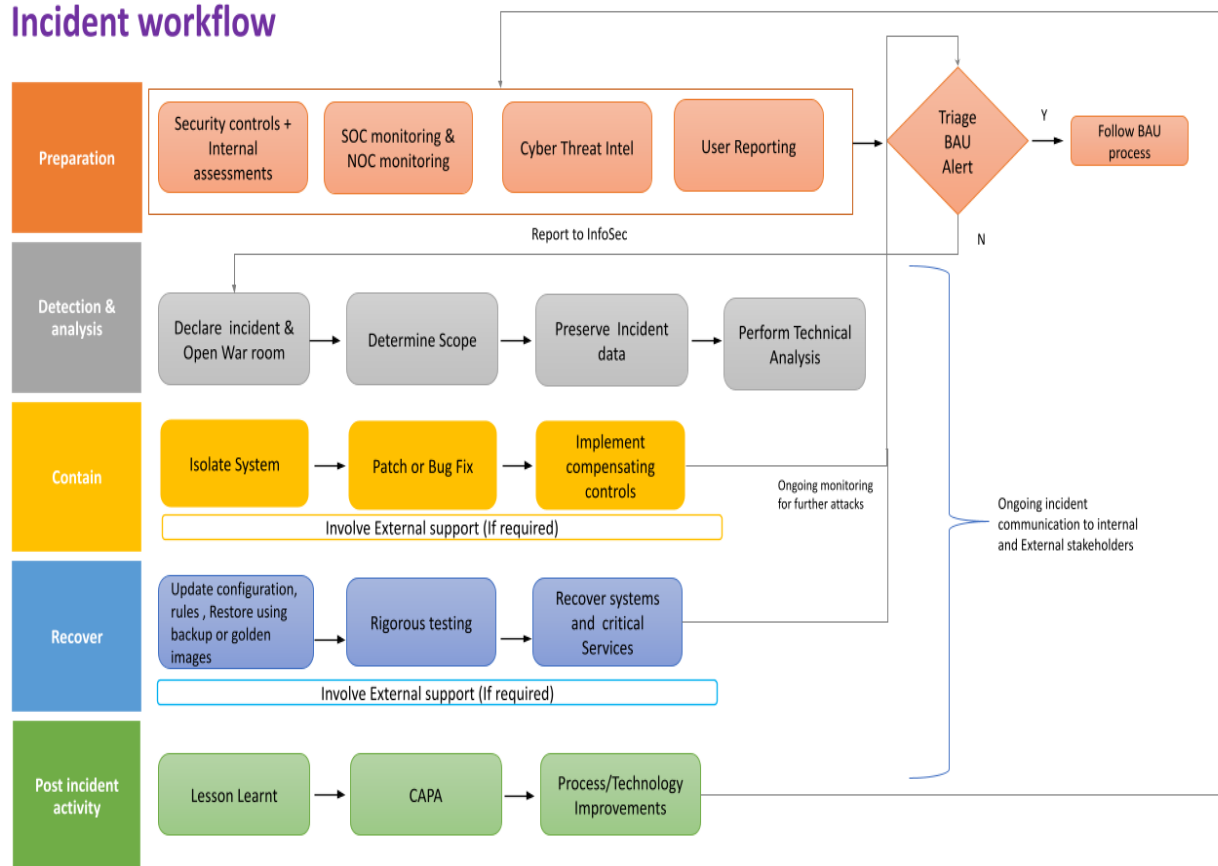
6.- Incident Management and Cyber Crisis Management Policy and Procedure

Incident	Scope	Severity	Action
	Business apps offline	High	Initiate crisis management protocol Inform executives and business leaders Send communications to customers and other parties
Data breach	Limited amount of data exposed	Low	Initiate Incident response protocol and take relevant action to block to leak
	Considerable amount of data exposed	Medium	Initiate Crisis management protocol. Consult with Corporate counsel, privacy and compliance officers Inform Board of Directors Update communication templates for media, customers, investors and authorities Engage forensics team
	Suspected data breach	High	Initiate Crisis management protocol. Consult with Corporate counsel, privacy and compliance officers Inform Board of Directors Update communication templates for media, customers, investors and authorities Engage forensics team

6.- Incident Management and Cyber Crisis Management Policy and Procedure

12. Incident Workflow

Incident workflow



13. Policy Exception

- Any exclusions to this policy shall be approved through the policy waiver.
- 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

14. Policy Compliance

- All the requirements specified in the Information Security Policy are to be followed by all employees of POLYCAB.
- Compliance to this policy will be measured by the internal or external audits.
- 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.

6.- Incident Management and Cyber Crisis Management Policy and Procedure

15. Review and Update

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

6.- Incident Management and Cyber Crisis Management Policy and Procedure

Annexure 1: RCA Components Mandated

1. RCA Component #1: Introduction

The introduction should provide the audience with background information about the event, the report's purpose, and the essential points covered throughout the document. Since RCA reports should be compiled per event, their scope should be narrow and their introduction brief. Some reports will have a problem statement or a one-sentence summary of the event.

2. RCA Component #2: Event Description

In-depth recap of the event—based on the information gathered.

The description should include:

- Date and time of the event
- What occurred
- How the event was discovered
- Who reported the event
- Response actions taken and by whom—before, during, and post-event
- Communications regarding event reporting—internal and external
- Impact of the event (e.g., financial, regulatory compliance)

3. RCA Component #3: Event Timeline

To record and/or view all activities that occurred or did not occur leading up to and after an event is chronologically. The timeline should not be overloaded with details, only factual data.

For example, activities may be logged in an RCA report's event timeline as follows:

§ February 21, 2025 @ 0200: SIEM event occurred on Server X

§ February 21, 2025 @ 0317: SIEM event Acknowledged by Operator Mills

This example shows a one-hour and 17-minute gap between the event occurring and the operator's acknowledgment. The significance of that gap (e.g., reasons for response delays, recommendations to reduce delays) will be covered elsewhere in the report when providing more thorough event descriptions and the RCA team's complete analysis. As a timeline entry, only need the basic facts.

4. RCA Component #4: Analytical Methodology

The methods used in the root cause analysis can vary based on the nature of the event. The RCA team's investigation may employ any of the following techniques:

- Barrier – Examine the pathways a threat can take toward a target or asset that can cause an undesired outcome
- Cause Factor Tree – Use a hierarchical or tree design to display the actions, conditions, and contributing factors that lead to an adverse event

6.- Incident Management and Cyber Crisis Management Policy and Procedure

- Change – Systematic approach to review impact and risk management strategies involving change within an organization, especially how expected and recent changes affect cybersecurity effectiveness
- Failure mode and effects – An review of product or process failures, strictly from an engineering perspective
- Fault tree analysis – Known as the “tree of logic,” this method examines an event using a logical tree of “AND,” “OR,” or “NOR” logic gates to show the contributing factors of an incident where the undesired event is the root.
- Fishbone – An analytic tool for examining effects and the contributing factors that create the effect. Often referred to as fishbone because the display of opposing lines for causes and effects resembles a fish skeleton.
- Pareto – A statistical cause analysis summary that looks at selected actions or tasks that produce a significant result (i.e., the incident being investigated). With this method, you can distill many factors down to those contributing the most towards an incident's occurrence.
- The Five “Why” Analysis – A problem statement is established (the incident), and a series of “Why” questions are asked until a root cause is found.

The root cause analysis report should include one of the above or similar methods to properly investigate all contributing factors.

5. RCA Component –Findings and Root Causes

The fifth component of the root cause report is the findings and presentation of the determined root cause. Here is where the RCA team delivers the root cause of an event after objectively conducting some of the below activities:

- Reviewing logs, reports, and other documents about the incident
- Identifying precursors or indicators as evidence leading to the incident
- Determining any impact to the organization before incident detection
- Stating whether the actual cause was identified
- Determining if the incident is the recurrence of a previous incident
- Estimating the damages attributed to the incident (e.g., noncompliance, financial, reputational)
- Comparing initial impact findings to final impact findings
- Presenting security program advisory and recommending preventive measures based on the incident

6. RCA Component Corrective Actions

The root cause analysis report should include a corrective and preventive section to guide any further remediation efforts and standard cybersecurity strategy. This section leverages the RCA findings to help prevent incident recurrence.

6.- Incident Management and Cyber Crisis Management Policy and Procedure

The RCA team will offer actionable tasks relevant to the root cause and its contributing factors, which includes daily or periodic responsibilities, baseline configurations, and the change management program. The improvement plans contain the following headings:

- Area of improvement
- Corrective action (from the root cause analysis summary)
- Responsible party (individual or department)
- Expected start date
- Anticipated completion date

6.- Incident Management and Cyber Crisis Management Policy and Procedure

Annexure 2: Responsibility matrix

Department /Role	RESPONSIBILITY CONTACT	CONTACT DETAILS/SPOC
CDIO / CISO	Declaration of incident Approve Security Incident Response Plan Provide strategic direction on overall incident response Coordinating the response and recovery efforts, Guidance on containment and restoring impacted systems Ongoing incident updates to executive team and Board of Director Onboarding of forensic investigators or external support as needed and oversee the activates	Mr. Gyan Pandey Mob: 9666797151 Gyan.Pandey@polycab.com Mr. Pradipta Patro Mob: 9930567770 <Pradipta.Patro@polycab.com>
IT Infra	Creating a virtual War room at the of incident Assist in isolation and containment of the affected system(s)/network(s) as needed Applying patches or fixes or preventive measures as required Providing additional resources (HW/SW) as required Providing the required logs for incident analysis Support in performing the RCA Working with Vendors/Partners for fix if required from their side (E.g. AWS,) Ensuring restoration of systems and Services Ongoing monitoring of the Systems during the incident	Mr. Ashish Anekar Mob: 9323010810 Ashish.Anekar@Polycab.com
SOC	Triage the incident Prepare Security Incident Response Plan Analyze the alerts & logs from various systems & Sources to identify the root cause Recommend immediate fix (incident containment) and Long term solution as required Maintaining chain of custody for incident evidences Assist the Forensic investigator with required	Mr. Amrendra Yadav Mob: 8076000103 Amrendra.Yadav@polycab.com

6.- Incident Management and Cyber Crisis Management Policy and Procedure

Department /Role	RESPONSIBILITY CONTACT	CONTACT DETAILS/SPOC
	data/Information Update runbooks and document lesson learnt from the incident	
Digital	Guiding developers on corrective actions if the incident is at application level Working with partners like (Cloudflare, AWS) for compensating controls until final fix is implemented for application specific attacks	Ritesh Arora Ritesh.Arora@Polycab.com Mob: 9880501639
InfoSec - GRC	Ensuring the respective Notification to relevant stakeholders (Internal and External) are sent out	Mr. Sanket Mhatre Sanket.Mhatre@polycab.com Mob: 9920940884
ERP	Provide immediate Bug fix if application level issue leading to incident DB restoration , Patching and Upgrades	ERP Hrishikesh Joglekar Hrishikesh.Joglekar@polycab.com Mob: 9833242682
Marketing & PR	Communicates externally with customers, partners, and the media. Coordinates all communications and requests for interviews with internal subject matter experts and security team. Involve PR team Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach.	Shwetal Basu Shwetal.Basu@polycab.com Mob: 9987267300
Legal & Compliance	Assist the organization to comply with the legal obligations and not to violate regulations and government mandates. Assist in vetting the communication to stakeholders Identify if there is need for external legal support	Legal Manita Gonsalves Manita.Gonsalves@Polycab.com Mob: 9833873070

6.- Incident Management and Cyber Crisis Management Policy and Procedure

Department /Role	RESPONSIBILITY CONTACT	CONTACT DETAILS/SPOC
	Notification of incident to the respective regulatory bodies as mandated	
HR	Inform internal employees on the incident and the Do's and Don'ts	Ashish Kakkar Ashish.Kakkar@polycab.com Mob: 9821051537
Finance	Assess the financial impact and assist in managing any budget required for crisis management initiatives	Niyant Maru Niyant.Maru@polycab.com Mob: 9811244770
Management	Provide strategic direction and Approvals as required	Board of Directors

Controls Reference

ISO 27001:2022

- Annex A5.24 Information Security Incident Management Planning and Preparation