POLYCAB

Cyber Crisis Management

Document Details

Title: 008 – Cyber Crisis Management 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	Updated to align with industry standards (NIST and ISO 27001)
3	V3.0	04-Apr-26	Sanket Mhatre -IT Cyber Security (GRC)	Pradipta Patro - CISO	Gyan Pandey – CDIO	Compliance section revised

Contents

1. Purpose

The purpose of this Security Incident Response Policy is to establish a comprehensive framework for identifying, responding to, and managing security incidents that may affect Polycab's information systems, data, and business operations. This policy ensures a standardized, efficient, and effective response to security incidents to minimize damage, protect sensitive information, and comply with legal and regulatory requirements.

2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, suppliers, and third parties who interact with Polycab's IT systems, networks, or data. It covers all types of security incidents, including, but not limited to, data breaches, cyberattacks, denial of service attacks, malware infections, and unauthorized access to sensitive systems.

3. Definitions

- **Security Incident:** Any event that results in, or has the potential to result in, a security breach, loss of data, unauthorized access, or damage to information systems.
- **Incident Response:** The coordinated efforts to identify, investigate, contain, eradicate, and recover from a security incident.

4. Roles and Responsibilities

Incident Response Head (CISO)

- Oversee the Security Incident Response Plan (SIRP).
- Ensure the SIRP is documented, reviewed, tested, and updated annually.
- Lead investigations and ensure timely escalation of incidents.
- Coordinate with external stakeholders, such as law enforcement and legal teams.
- Approve and authorize external investigations and access to evidence.

Security Incident Response Team (SIRT)

- Educate and train all staff on identifying and reporting security incidents.
- Investigate incidents reported by staff and document findings.
- Take immediate action to contain and mitigate the impact of incidents.
- Analyze logs and security data to identify the cause of incidents.
- Assist with evidence collection and maintain chain of custody.

IT Department

- Ensure the availability and functionality of systems during incidents.
- Assist with system isolation, containment, and remediation actions.
- Provide necessary resources, including hardware, software, and logs.

- Support the recovery of impacted systems and services.

SOC (Security Operations Center)

- Triage incoming security alerts and validate potential incidents.
- Identify the root cause of the security incident.
- Recommend immediate and long-term containment actions.
- Ensure the protection and preservation of incident evidence.

Digital/Development Team

- Address application-level security issues and work with external partners for fixes (e.g., Cloudflare, AWS).
- Guide developers on implementing corrective actions and compensating controls.

Legal and Compliance

- Ensure that all legal and regulatory obligations are met during an incident.
- Communicate with relevant authorities and assist with breach notifications.
- Ensure communications are compliant with privacy regulations.

Marketing & PR

- Manage external communication during an incident, including media, customers, and partners.
- Maintain pre-prepared crisis communication templates for rapid deployment.

HR

- Communicate with internal employees regarding the incident and provide instructions on safety and security measures.

Finance

- Assess the financial impact of the incident and manage budgets for crisis management activities.

All Staff

- Report any suspected or actual security incidents to the designated Incident Response Lead or a member of the SIRT.
- Follow internal security policies and procedures.
- Cooperate with incident investigations and recovery efforts.

5. Incident Response Phases

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

1. Incident Discovery and Confirmation

- 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. Threat Classification and Severity Levels

Incidents are categorized based on their severity, as follows:

- **Low Severity:** Incidents with minimal or no impact on business operations or sensitive data. Examples include non-critical system alerts and minor security issues.
- **Medium Severity:** Incidents that may affect business operations or expose limited amounts of sensitive data. Examples include a moderate data breach or system vulnerabilities.
- **High Severity:** Critical incidents that disrupt business operations, compromise sensitive data, or threaten the integrity of systems. Examples include a major data breach, ransomware attack, or critical system downtime.

7. Communication Protocol

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.

Communication Templates:

- **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."
- **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."

8. Compliance and Legal Requirements

Polycab is committed to complying with all relevant data protection and cybersecurity laws and regulations, including but not limited to:

- **Digital Personal Data Protection Act (DPDPA)**
- **Cybersecurity and Infrastructure Security Agency (CISA) guidelines**
- **ISO 27001 2022 ISMS standards**

In the event of a security incident, Polycab will notify the appropriate regulatory authorities within the required timelines and provide necessary documentation and reports as required.

9. Training and Awareness

- **Staff Training:** All staff members must undergo security incident response training at least once per year to ensure they understand their roles and responsibilities.
- **Incident Response Drills:** Periodic mock incident response exercises will be conducted to test the readiness of the SIRT and other teams.

10. Policy Review and Updates

This policy will be reviewed and updated annually, or more frequently as needed, to ensure it remains relevant and effective in addressing emerging threats and compliance requirements.

11. Annexure

- Crisis Management Procedure

008 - Crisis Management Procedu

- Crisis Management Plan

008%20-%20Cyber%20Crisis%20Managen