TECHMED SOLUTIONS

INCIDENT RESPONSE PLAN

DECEMBER 12, 2025

VERSION	1.0
EFFECTIVE DATE	30-12-2025
OWNER	GRC MANAGER
APPROVED BY	BOARD OF DIRECTORS / CEO

Table of Contents

Introduction

Purpose

This Incident Response Plan (IRP) aims to provide the Computer Security Incident Response Team (CSIRT) and associated stakeholders with useful, tactical guidance to enable the successful and efficient detection, containment, eradication, and recovery from cybersecurity incidents affecting TechMed Solutions' information assets and services. The IRP ensures compliance with the incident response policy and regulatory standards, especially PCI DSS and HIPAA.

Scope

This plan covers all TechMed Solutions-related systems, networks, facilities, applications (including the SaaS platform), data (PHI, PCI), and employees in all geographical and cloud (AWS) locations. In particular, it operationalizes the NIST Incident Response Lifecycle's four steps.

Phase 1: Preparation

The preparation phase involves establishing and training a CSIRT team, developing applicable procedures, and acquiring the necessary tools and resources. During this phase, TechMed Solutions will attempt to limit the number of incidents that will occur by selecting and implementing a set of controls based on the risk assessments.

CSIRT Structure and Composition

The CSIRT structure is a tiered model including the core team, extended team, and external resources.

a. The Core Team, which signifies the tier 1 / first point of contact, includes the technical responders who will be on call 24/7. The core team includes:

- Incident Responder Manager representing the chair leader
- Lead Security Analyst
- Forensic Specialist
- IT Operation Lead.

This team is responsible for direct handling and escalation of all confirmed security incidents in TechMed Solutions.

b. The Extended Team: these are the tier 2 layer of the CSIRT team, they are the business unit head/stakeholders as needed. They include:

  - Legal Counsel
  - Data Privacy Officer
  - Human Resources
  - Communications

- Application Owners

c. External Resources: these are the tier 3 layer of the CSIRT team, they are the third-party / contract partners of TechMed Solutions. They include:
    - Managed Security Service Provider (MSSP)
    - External Forensics Firm
    - Cyber Insurance Provider

Tools and Resources

Tool / Resource	Purpose
SIEM (Security Information and Event Management)	SIEM will be used to detect malicious activity in TechMed Solutions Network. It will help monitor and manage security events through the use of data analysis and automation. Splunk is a typical example of a SIEM tool that can be used.
IDS / IPS (Intrusion Detection System / Intrusion Prevention System)	IDS will be deployed to monitor the network traffic of TechMed Solution, and search for known threats and suspected malicious activity, while IPS will be deployed to intercept and analyze the malicious activities. An example is Snort
EDR (Endpoint Detection and Response)	EDR will be deployed to monitor, detect, and respond to cyber threats across all TechMed Solutions Endpoints (Laptops, Servers, Mobile Phones, Cloud Workloads). This will enhance real-time threat detection, automated incident response. Examples include: BitDefender, CloudStrike, SentinelOne.
Forensic Software	An Investigative tool used to collect, analyze, and report information on security incidents, it also examines evidence. Example include; FTK, EnCase.
Secure Communication Platform	Communication platform primarily for CSIRT, in case of security incidents. Platforms that can be used include; Slack, Signal.
Incident Response Ticketing System	A centralized hub where incidents are logged as tickets assigned to appropriate team of the CSIRT. The ticketing system will be designed to manage, track, and resolve incidents systematically. Example include; Jira, ServiceNow.

Training and Awareness

- CSIRT Team: annual incident response tabletop exercises should be conducted for the CSIRT Team, and role-specific training should be administered with tests and exercises. Specialized training in forensics, malware analysis should be administered. The team must comply with the training requirements.

- Employee Awareness: annually conduct security awareness training for all employees of TechMed Solutions. The awareness training should consist of phishing simulations, which will keep employees abreast of the tactics of attackers via email. Employees should also be trained on how to report a suspected security incident; they must also be taught the acceptable use of data, such as PHI and PCI data.

Communication Infrastructure

- Primary Communication: a dedicated chat channel, such as Slack or Microsoft Teams, should be put in place for day-to-day coordination among team members.
- Out-of-Band Communication: in case of the primary communication channel being compromised, an Out-of-Band channel should be established separately with a secure conference bridge (voice call) and encrypted messaging channel.

Phase 2: Detection and Analysis

The Detection and Analysis phase for TechMed Solutions will start with detection sources and methods used in detecting the incidents, it also includes the triage procedures, i.e., steps taken in case of a suspected potential security alert, incident analysis framework, and end with documentation requirements. The CSIRT will be made aware of security incidents through automated alerts using tools like SIEM, EDRs, IPS/IDS, users, and partners.

Detection Sources and Methods

Detection is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and initial classification of the incident, as well as any initial notifications required by law or contract. All TechMed Employees will be trained to broadcast awareness, and they will report to the appropriate quarters in real-time in case of suspicious activities. The TechMed IT department will be trained on how to report potential issues to the CSIRT for investigation as they troubleshoot and maintain the TechMed System. The detection sources and methods are not limited to:

- SIEM alerts
- IDS/IPS alerts
- EDR alerts
- Antivirus alerts
- User reports via Help Desk

- Third-party notifications

TechMed Solutions will rely on automated alerts prioritized by SIEM, driven by logs from critical assets such as the SaaS application logs, AWS access logs, and Cardholder Data Environment (CDE).

Initial Triage Procedures

The steps to take upon reception of a suspected potential alert are highlighted below:

- Receive suspected incident report
- Create a new incident ticket immediately, even if the status is “Suspected”, and log it into the incident ticket management system.
- Validate the report to check if it’s a true positive, correlate the alert with external intelligence and internal systems log, and check the EDR for file execution or SIEM for lateral movement.
- Assign an initial severity level, classify the incident with the Incident classification framework to determine if it’s a data breach, malware infection, or ransomware, and Severity Level, if it's Critical, High, Medium, or Low based on the report's findings.
- Escalate to the Incident Response Manager, especially if the severity level is Critical or High.

Incident Analysis Framework

After confirmation of a security incident:

- Scope the incident: identify all affected systems and data. Forensic tools will be used to answer questions like: “Which systems are affected?” “Which accounts are compromised?” “Which data (PHI/PCI) were involved?”
- Identify the attack vector: identify the method of entry that caused the attack, which could be through phishing mail, misconfiguration, or an exploited vulnerability.
- Collect and preserve evidence: snapshots of compromised resources, archive logs from compromised systems; the integrity of the chain of custody must be preserved for all evidence relating to PHI/PCI data.
- Analyze logs, network traffic, and system images.
- Document all findings in case of an external audit; there will be evidence to back up all actions.

Documentation Requirements

A detailed documentation must be recorded in the Incident Management System:

- Incident ticket with all actions taken, such as the precise time logs were taken, the action performed on the logs, and the outcome.
- Initial assessment report, detailed findings, hypotheses, and supporting data, such as IOCs, file hashes, must be included in the assessment report.
- Evidence Logs (chain of custody): a formal record of all collected data, including hash values and storage locations.
- Forensic analysis report

Phase 3: Containment, Eradication, and Recovery

The primary objectives in executing containment, eradication, and recovery activities are aligned with the incident priority levels.

Containment Strategies

Containment Strategies will prioritize the safety of PHI/PCI data and the availability of the SaaS platform:

Short-Term Containment (0-4 hours)

- Network Isolation: isolate all affected systems from the network, use firewall rules to isolate the compromised system/network segment from the entire internal network, and maintain monitoring access for the CSIRT.
- Disable compromised accounts/ revoke credentials by disabling or forceful password resets of compromised accounts.
- Block malicious IP addresses/blacklist the known malicious IP addresses.

Long-Term Containment (Till Eradication)

- Move affected systems to a quarantine VLAN
- Temporary technical controls will be deployed to mitigate the root cause of the attack, for example, implementing MFA for all administrative access and implementing temporary firewall rules.
- Apply Hardening / Patching to the affected system.

Eradication Procedures

- Ensure all attack vectors/vulnerability is understood and patched.
- Removal of all malicious files, backdoors, and configuration changes from affected systems.
- Reset all compromised credentials.
- Rebuild systems from a known good image, if necessary, and deploy enhanced monitoring, such as file integrity monitoring.

Recovery Processes

Recovery must be performed periodically to ensure the incident does not recur:

- Restore data from validated and tested back-ups, and check for data integrity of the back-ups.
- Validate that recovered systems have passed a security check; they must be clean and fully functional.
- Return systems to production.
- Implement enhanced and continuous monitoring.

Business Continuity Integration

If a critical incident occurs, the Business Continuity Plan (BCP) will be activated, while the CSIRT team will work with the BCP team to prioritize recovery efforts based on business impact.

The Incident Response Plan focuses on eradicating threats, while the Business Continuity / Disaster Recovery (BC/DR) plan focuses on maintaining essential operations via failover or manual procedures.

Phase 4: Post-Incident Activity

This phase ensures TechMed Solutions learns from the incident to improve its security posture.

Lessons Learned Process

A mandatory Post-Incident Review (PIR) meeting will be held within two weeks of incident closure. If there’s a large number of critical and high incidents, the post-incident review should be conducted within 7 business days. The Post-Incident Review will focus more on the effectiveness of processes carried out, the flow of communications between the team, and the shortcomings encountered during each phase. Participants of the PIR will include the CSIRT, relevant business stakeholders, and executive leadership. The goal of the meeting will center around what went well, what could be improved on, and the root cause of the incident.

Root Cause Analysis (RCA)

The 5 Whys technique must be used to identify the underlying cause of the incident. Root cause analysis must be documented for every critical and high incident to identify the systemic underlying failure that allowed the incident to occur.

Improvement Recommendations

- All lessons learned will be translated into actionable recommendations;

- Each recommendation will be assigned an owner and a due date.
- Progress will be tracked in the GRC tool.

Metrics and Reporting

Key Performance Indicators (KPIs) must be calculated and reported monthly to measure program effectiveness:

- The GRC Manager will produce a quarterly incident response for executive leadership.
- The report will include key metrics such as:
  - Mean Time to Detect (MTTD): measures the effectiveness of monitoring.
  - Mean Time to Contain (MTTC): measures the speed of the response team.
  - Mean Time to Recover (MTTR): measures efficiency of recovery procedures.
  - Incident Volume Trends.