TECHMED SOLUTIONS

INCIDENT RESPONSE POLICY

DECEMBER 12, 2025

Table of Contents

POLICY NUMBER	1R-01
VERSION	1.0
EFFECTIVE DATE	30-12-2025
OWNER	GRC MANAGER
APPROVED BY	BOARD OF DIRECTORS / CEO

Purpose and Scope

Purpose

This policy outlines TechMed Solutions' approach to predicting, detecting, responding to, and recovering from security incidents. The goals are to protect sensitive data (including PHI and PCI data), minimize the impact of incidents, maintain business continuity, and comply with all legal and regulatory requirements. One major objective is to ensure the confidentiality, integrity, and availability of TechMed Solution’s assets, particularly Protected Health Information (PHI) and Payment Card Data (PCI), while recovering from security incidents.

Scope

This policy applies to all TechMed Solutions employees, contractors, outside service providers, and any other individuals who have access to TechMed Solutions' data and information systems. It encompasses all information assets, including hardware, software, data, and network infrastructure, whether they are located on-site or in the cloud.

Definitions

Term	Definition
Security Event	Any observable occurrence in a system or network, such as a failed login attempt or a high volume of data transfer.
Security Incident	A violation or imminent threat of a breach of computer security policies, acceptable use policies, or standard security practices, such as unauthorized access into a system or malware infection.
Incident Response	This process involves taking necessary actions to identify, contain, and recover from a security incident. Also, the systematic approach to addressing and managing the aftermath of a security breach or cyberattack.

Computer Security Incident Response Team (CSIRT)	A dedicated team of individuals responsible for coordinating and executing the incident response plan.
Protected Health Information (PHI)	Individually Identifiable health information that is transmitted or maintained in any form or medium.
Payment Card Industry (PCI) Data	Cardholder data and sensitive authentication data.
Incident Severity Levels	This categorization of security incidents is based on their impact on business, regulations, and service disruption, classified as Critical, High, Medium, and Low.

Roles and Responsibilities

Role	Responsibilities
Executive Leadership (CEO, Board)	Provide overall strategic direction, approve the incident response policy, and allocate necessary resources. Approval of HIPAA/PCI breach notification decision and ensuring business continuity for the TechMed SaaS platform.
Chief Information Security Officer (CISO)	Oversee the incident response program, chair the CSIRT, and make critical decisions during an incident.
GRC Manager	Develop and maintain the incident response policy and plan, ensure compliance with regulatory requirements, and coordinate post-incident reviews.
IT Operations	Provide technical support during an incident, including system access, network changes, and data restoration. Management of the Hybrid Cloud Environment of TechMed will be handled by IT Operations during containment and recovery phases of any security incident.
Legal Counsel	Guide on legal and regulatory obligations, including breach notification requirements. TechMed Legal Counsel is responsible for reviewing all documents regarding breach notifications and timelines.
Human Resources	Manage any employee-related aspects of an incident, including insider threats and disciplinary actions. In case of a security incident, HR will conduct and coordinate interviews relating to the incident and ensure they are handled well.
Communications	Manage all internal and external communications during an incident.

	Protects the organization's reputation, showcasing TechMed as a trusted Healthcare technology provider.
All Employees	Report any suspected security incidents immediately and cooperate with the CSIRT during an investigation. Adheres to rules and regulations, especially regarding the way data is handled, and attends trainings as required.

Incident Classification Framework

Incident Types

Type	Description
Malware	Ransomware, viruses, worms, trojans, spyware. Malware impacts the availability and integrity of systems.
Unauthorized Access	Access to systems or data by an unauthorized individual. Unauthorized access impacts confidentiality, especially that of PHI/PCI data.
Data Breach	Confirmed exfiltration of sensitive data.
Denial of Service (DoS)	An attack that prevents legitimate users from accessing the service. This impacts the availability of data, as when needed, causing service uptime.
Insider Threat	A malicious or unintentional act by an employee, contractor, former employee, or other insider resulting in system damage or data exposure.
Physical Security	Theft or loss of equipment, unauthorized access to facilities.

Incident Severity Levels

Severity	Criteria
Critical	Widespread impact, critical systems affected, significant data loss or exfiltration of PHI/PCI data, major business disruption, high likelihood of regulatory action.
High	Significant impact, multiple systems or departments affected, potential for data loss of sensitive data, moderate business disruption.
Medium	Localized impact, single system or small group of users affected, minimal data loss, minor business disruption.

Low	Minor impact, no critical systems affected, no data loss, no business disruption.

Reporting Requirements

All employees and contractors of TechMed Solutions who discover or suspect any action that may lead to a security incident must report it immediately, at the least within 1 hour of discovery or suspicion, through dedicated channels. The CSIRT Manager is expected to be in charge of all escalation paths.

- **Reporting Channel**: IT Help Desk, Dedicated Security Email Address, and Phone Number
- **Timeframe**: Immediately upon discovery
- **Escalation Path**: the IT Help Desk will escalate all suspected security incidents to the CSIRT for triage and validation.

Regulatory and Legal Compliance

TechMed Solutions is committed to complying with all applicable laws and regulations, including:

- **HIPAA**: The Health Insurance Portability and Accountability Act.
- **PCI DSS**: The Payment Card Industry Data Security Standard.
- **GDPR**: The General Data Protection Regulation.
- **SOC 2 Type II**: The Service Organization Control.
- **State Breach Notification Laws**: PIPEDA (Canada), CCPA (California).

All incident response activities will be conducted in a manner that preserves evidence for potential legal action and complies with all breach notification requirements.

Policy Review and Updates

This policy will be reviewed and updated at least annually, or more frequently if there are significant changes to the threat landscape, regulatory requirements, or business operations. The GRC Manager is responsible for coordinating the review and update process while ensuring Executive Approval.