TECHMED SOLUTIONS

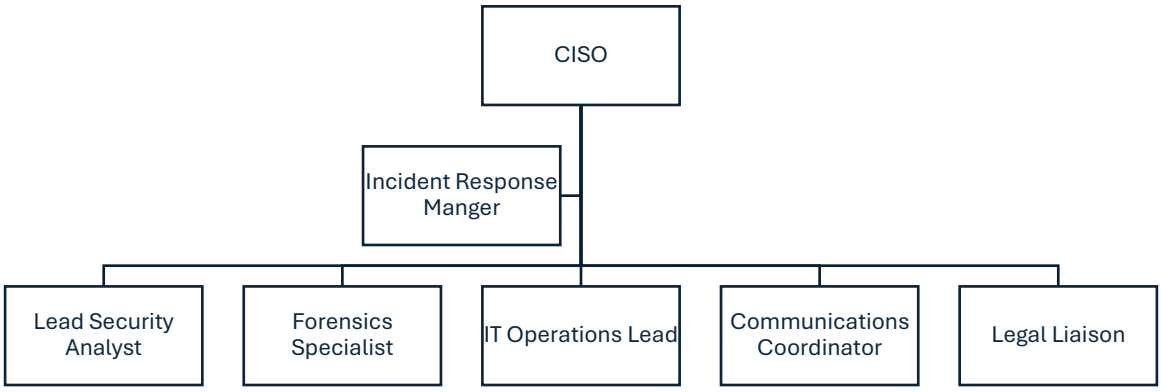
CSIRT STRUCTURE AND RACI MATRIX

DECEMBER 12, 2025

Table of Contents

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

CSIRT Organizational Chart



Role Definitions

Role	Responsibilities
Incident Response Manager	Leads and coordinates all incident response activities. Makes critical decisions during an incident. Provides regular status updates to executive leadership.
Lead Security Analyst	Performs initial triage and validation of suspected incidents. Leads the technical investigation Analyzes logs, network traffic, and system images.
Forensics Specialist	Collects and preserves evidence in a forensically sound manner.

	Performs deep technical analysis of compromised systems. Recovers deleted or encrypted data.
IT Operations Lead	Provides access to affected systems. Implements containment and eradication actions (e.g., network changes, system rebuilds). Monitors media and social media for related activity.
Communications Coordinator	Manages all internal and external communications during an incident. Drafts and distributes notifications to stakeholders. Monitors media and social media for related activity.
Legal Liaison	Guides on legal and regulatory obligations. Reviews all external communications. Manages any interactions with law enforcement.

RACI Matrix

RACI Key:

- R = Responsible (Does the work)
- A = Accountable (Owns the work)
- C = Consulted (Provides input)
- I = Informed (Kept up-to-date)

Activity	Incident Response Manager	Lead Security Analyst	Forensics Specialist	IT Operations Lead	Communications Coordinator	Legal Liaison	Executive Leadership
Incident detection and initial reporting	A	R	I	I	I	I	I
Incident validation and triage	A	R	C	I	I	I	I
Incident classification and prioritization	A	R	C	I	I	I	I

Evidence collection and preservation	A	C	R	C	I	C	I
Containment decision-making	A	C	C	C	C	C	C
Containment Execution	A	C	I	R	I	I	I
Eradication execution	A	C	I	R	I	I	I
System recovery and validation	A	C	I	R	I	I	I
Stakeholder communication (internal)	A	I	I	I	R	C	I
Stakeholder communication (external)	A	I	I	I	R	C	C
Regulatory notification and reporting	A	I	I	I	C	R	C
Post-incident review facilitation	R	C	C	C	C	C	A
Lessons learned documentation	R	C	C	C	C	C	A
IR plan updates and maintenance	R	C	C	C	C	C	A

Escalation Procedures

Escalation Criteria:

- Critical Incidents: Escalate to executive leadership and legal counsel immediately.
- High Incidents: Escalate to the CISO immediately
- Incidents involving PHI/PCI data: Escalate to the Data Privacy Officer and Legal Counsel immediately.
- Incidents with potential media attention: Escalate to the Communications team immediately.

Escalation Path:

1. Security Analyst detects a potential incident and escalates to the Lead Security Analyst
2. Lead Security Analyst validates the incident and escalates to the Incident Response Manager
3. Incident Response Manager assesses the severity and escalates to the CISO and other relevant stakeholders as per the criteria above.