TECHMED SOLUTIONS

INCIDENT RESPONSE METRICS AND CONTINUOUS IMPROVEMENT

DECEMBER 12, 2025

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

Incident Response Metrics and Continuous Improvement

Key Performance Indicators

- Mean Time to Detect (MTTD): This metric measures the effectiveness of monitoring and alerting systems of TechMed Solutions. MTTD represents the average time from the occurrence of an event to its detection, which represents initial alert generation.
- Mean Time to Respond (MTTR): This metric measures the team's ability to engage quickly in an occurrence of a security breach. MTTR represents the average time from detection to the initial response, i.e., initial triage.
- Mean Time to Contain (MTTC): measures the effectiveness of short-term containment strategies. MTTC represents the average time from detection to the point of isolation till containment.
- Mean Time to Recover (MTTR): measures the efficiency of recovery and restoration procedures. MTTR represents the average time from containment to post-incident activity / post-validation.
- Incident Volume Trends: represents the number and distribution of incidents by type over a period of time. This metric will identify common attack vectors and resource allocation needs.
- False Positive: represents the percentage of alerts categorized as security events that are ultimately classified as false alarms. This metric measures the accuracy and tuning of detection tools.

Metrics Collection and Reporting

A concise executive dashboard should be created quarterly for review by executive leadership (CEO/COO/CIO/CISO) of TechMed Solutions. Data will be collected and calculated monthly, measuring the KPIs of the data. The Incident Response Manager will be responsible for analysing the data and comparing performance with defined targets. The executive dashboard will highlight trends, systemic risks identified, and adherence/compliance status.

Continuous Improvement Process

- Post-Incident Review and Root Cause Analysis should be done continuously to identify gaps, especially in a case of a critical/high-severity incident.
- Incident Response Manager should conduct a formal review of performance metrics (KPIs) quarterly with the findings of PIR and RCA alongside the CSIRT team.
- Tabletop Exercises should be performed to test the plans developed (Incident Response Plan, Communication Plan). Scenario play should be considered to keep employees abreast in case of a security incident.
- Incident Response Plan, Incident Response Policy, Communication Plan, and other supporting documents should be regularly revised and updated following any security incident or significant regulatory change.
- Security Awareness Training should be conducted regularly for staff alongside role-specific training, especially for the CSIRT team

Program Maturity Assessment

The Capability Maturity Model approach will be deployed to regularly assess the maturity of the Incident Response Program of TechMed Solutions.

Maturity Levels:

- Initial (Level 1): At this stage, the Incident Response Program is ad-hoc, relying on individual efforts. During this stage, documentation is minimal; this is the initial stage of TechMed before the Incident Response Program was developed.
- Repeatable (Level 2): at this stage basic formal policy and plan (IRP) exists, KPIs are tracked, but the processes are not optimized.
- Defined (Level 3): at this stage, the IRP is fully documented, tested annually with repeatable response. The RACI matrix is enforced with well-integrated legal and communication liaisons.
- Managed (Level 4): at this stage, continuous improvement is formalized, and KPIs are consistently met.
- Optimizing (Level 5): at this stage, advanced threat intelligence is integrated into detection methods. Automated response is utilized; at this stage, the IRP program is capable of handling complex incidents with high efficiency.