TRIANZ℠

Security Incident Management & Response Procedure

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

1. Introduction

The Security Incident Management and Response Procedure is designed to provide a systematic and consistent approach for detecting, assessing, responding to, and restoring normal operations following security incidents that could compromise the confidentiality, integrity, or availability of the organization's information systems, data, or operations."

2. Objectives

The main objective of an Incident management & Response procedure is to restore normal service operations as quickly as possible and minimize the negative impact on business activities. A standardized process ensures an efficient and coordinated response to unplanned service disruptions, such as a server crash or a network outage etc.

Key Objectives of Incident Management and Response procedure are as follows.

- Incident Identification and Reporting
- Incident Response
  - ✓ Detection and Reporting
  - ✓ Assessment and Classification
  - ✓ Containment
  - ✓ Investigation and Analysis
  - ✓ Root Cause Analysis
  - ✓ Correction
  - ✓ Eradication and Corrective Actions
  - ✓ Recovery
  - ✓ Lessons Leaned
  - ✓ Continuous Improvement
- Compliance and Governance
- Incident Management Records Maintenance

3. Scope:

- This document applies to all Trianz associates including contractual employees, third party vendors, cloud service providers and all other individuals and groups who have been granted access to Trianz
- All users must understand and adopt this procedure and are responsible for ensuring the safety and security of the Trianz infrastructure working remotely or in the office/client premises for the information that they use or process. This includes both data stored electronically and in any other form.
- The procedure applies to all Trianz products and services.

4. Procedure Steps

4.1 Incident Identification and Reporting

Information Security Incidents shall be reported promptly to IT Service Desk and Infosec team by the associates keeping the reporting manager informed.

Associates need to fill the **Incident Reporting Template**

Details of the incident Reporting format shall comprise the following:

1. Date & Time of Detection, Systems Affected, Reported by, Department, Contact Information
2. Type of Security Incident:(e.g., Unauthorized Access, Malware Attack, Phishing, Data Breach, Physical Intrusion, Loss of Assets etc), Detailed Description:(Include what happened, how it was discovered/identified, and any immediate impact observed.)(can be elaborated), Initial Severity Assessment: *(Low / Medium / High / Critical),* Impact of the Incident(from the reportee on initial impact) with the details of the time reported

4.2 Incident Response

4.2.1 Detection and Reporting

Incident shall be reported using the Incident report template as soon as an incident is identified, and the details are to be provided to IT Service Desk and Infosec Team

CIO will report cyber incidents within 6 hours to CERT-In. based on the severity and applicability.

4.2.2 Assessment and Classification

Incident shall be analyzed for its impact w.r.t Data Loss/exposure, Financial Impact, Operational Disruption, Legal/ Regulatory Implications, Reputational Damage etc.

Also Assessment is carried out for validating on whether any assets are affected – Systems/Applications Involved, Data Compromised, User/ Accounts affected, Others if any.

4.2.3 Containment

IS team shall isolate affected systems, Networks or User accounts, Disable Compromised Services or Access Points and Apply temporary firewall or access Controls as applicable.

4.2.4 Investigation and Analysis

Logs and System Data shall be collected for forensic analysis as applicable.
Interviews and Investigation shall be carried out by IS Team as applicable
Work with Infosec to identify the attack vector and scope
Forensics: Collect and preserve evidence for internal and legal use.

4.2.5 Root Cause Analysis

Root Cause shall be determined based on Investigations and Contributing factors for the incident as applicable
Also identify the Security Controls that were failed or were missing that was causing the incident
All evidence shall be preserved for Legal Usage/purpose and for future reference. Can also be useful for the Lessons to be learnt from the incident.

4.2.6 Correction

As part of Immediate Correction, Actions shall be initiated to ensure the incident is Contained (as applicable)/ Temporary fixes shall be applied and notification shall be sent to Applicable Internal and External Stakeholders.
Remediation and actions required shall be carried out by the respective Project Teams and Function Teams

All findings, timelines and remediations/ Actions by each department shall be documented.

4.2.7 Eradication/ Corrective Action

As part of the eradication and Corrective Action, the root cause of the incident shall be eliminated, Apply patches, change credentials, disable compromised accounts.
Remediation and actions required shall be carried out by the respective Projects and Functions to ensure the incident is not recurred for e.g. Awareness and Training Sessions shall be conducted.

4.2.8 Recovery

Systems and Services shall be restored to normal operation and Monitored for any signs of recurrence.

4.2.9 Lessons Learned

Post-incident review shall be conducted and lessons learned shall be documented
Policies Shall be updated controls applied, and training conducted based on findings.

4.2.10 Continuous Improvement

Conduct post-incident reviews (lessons learned) to identify weaknesses and improve future incident response.
Update security controls, policies, and procedures based on findings.

4.3 Compliance and Governance

Align the incident response procedure with organizational policies, industry standards (e.g., ISO/IEC 27001, NIST), and regulatory frameworks.
Demonstrate due diligence and accountability to auditors and regulators.

4.4 Incident Management Records Maintenance

Incident Records shall be maintained and reviewed periodically – once in three months

5. Roles and Responsibilities

Types of Incidents	Internal/External	Stakeholders involved	Incident Reporting	Assessment and Classification	Containment	Investigation and Analysis	RCA	HR	Lessons Learnt
Security Incidents	Internal/External	IT, Infosec, Delivery/or corporate functions, Legal	Can be from all associates	IS Team, Infosec, CIO, other stakeholders as applicable	IS Team and Infosec Team , CIO	IS Team, Infosec, CIO and Legal	IT, Infosec, Legal	As applicable	IT, Infosec
Service Incidents	Internal/External	IT, Infosec, Delivery/or corporate functions, Legal	Can be from all associates	IS Team, Infosec, CIO, other stakeholders as applicable	NA	IS Team	IT, Infosec	As applicable	IT, Infosec
Policy Violations- Employees violating Acceptable usage Policy, Laptop usage, Internet Usage Policy	Internal	IT, Infosec, Delivery/or corporate functions, Legal	Can be from all associates	IS Team, Infosec, CIO, other stakeholders as applicable	NA	,Infosec,CISO and other stakeholders as applicable	IT, Infosec, Legal	As applicable	IT, Infosec
Natural Calamilities -Floods, Theft, Fire etc	Internal/External	IT, Infosec, Delivery/or corporate functions, Legal, Admin	BCP Team	Admin & ERT Team, Infosec, CIO, other stakeholders as applicable	NA	Admin and Infosec , CIO	IT, Infosec, Legal, Admin	As applicable	IT, Infosec
Physical Incidents - related to Theft, Damage of Equipment	Internal/External	IT, Infosec, Delivery/or corporate functions, Legal, Admin	Admin Team	Admin & ERT Team, Infosec, IS Team, CIO, other stakeholders as applicable	NA	Admin, IS Team (As applicable) & Infosec , CIO	IT, Infosec, Legal, Admin	As applicable	IT, Infosec
Privacy Breaches	Internal/External	IT, Infosec, Delivery/or corporate functions, Legal	Can be from all associates	IS Team, Infosec, CISO and other stakeholders as applicable	IS Team and Infosesec Team , CISO	IS Team, Infosec Team, CIO, and Legal	IT, Infosec, Legal, Admin	As applicable	IT, Infosec
Pandemic Incidents	External	IT, Infosec, Delivery/or corporate functions, Legal, Admin	Can be from all associates	Admin & ERT Team, Infosec, CIO, HR Team and other stakeholders as applicable	NA	Admin &ERT Team and other Stakeholders as applicable	IT, Infosec, Legal, Admin	As applicable	IT, Infosec

6. Exit Criteria

- Completed Incident Reporting Analysis along and management of Incident Records

7. Prerequisites

7.1 Resources & Training

Incident Management

7.2 References

Document Name
ISO 27001:2022 Standard

8. Related Guidelines, Templates and Checklists

Document Name
Incident Reporting Template
Consolidated Incident Tracker & Analysis

9. Measurement

Number of reported incidents reviewed and analyzed vs number of actual incidents

10. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Organizational Controls	5.24 Information security incident management planning and preparation Control The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security	Information Security Incident Management Procedure

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
	incident management processes, roles and responsibilities.	
Organizational Controls	5.25 Assessment and decision on information security events Control The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Information Security Incident Management Procedure
Organizational Controls	5.26 Response to information security incidents Control Information security incidents shall be responded to in accordance with the documented procedures.	Information Security Incident Management Procedure
Organizational Controls	Learning from information security incidents Control Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Information Security Incident Management Procedure
People control	Information security event reporting Control The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Information Security Incident Management Procedure
Organizational Controls	5.28 Collection of evidence Control The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Information Security Incident Management Procedure
Organizational Controls	5.29 Information security during disruption Control The organization shall plan how to maintain information security at an appropriate level during disruption	Information Security Incident Management Procedure

11. Appendix Incident Severity

An incident will be categorized as one of four severity levels. These severity levels are based on the impact to the organization and can be expressed in terms of financial impact, impact on the company's reputation, brand value, customer's trust etc. Following table provides a listing of the severity levels and a definition/description of each severity level.

Severity Level	Description	Examples
Critical	Incident where the impact is severe.	Examples are a disruption of business operations, companies' proprietary of confidential and sensitive information has been compromised, and a virus or worm has become widespread.
High	Incident where the impact is significant.	Examples are a delayed ability to order, delayed delivery of critical electronic mail or EDI transfers, etc.
Medium	Incident where the impact is minimal.	Examples are harmless email SPAM, isolated Virus infections, etc.
Low	Incident where the impact is very less	Examples are False positives - when investigation of suspicious activity finds no evidence of a security incident.

Document Control

Owner:	CISO	**Release ID:**	ISIM-PROC-0043

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.00	26-Feb-07	Jyotessh G Nair			Initial draft	
1.00	26-Feb-07	Jyotessh G Nair			Baseline approved by Zulfikar Deen.	Approved Baseline.
1.01	12-Jun 08	Bharatees ha B R			Revised the process incorporating reviews of GT	• Revised the Process by including Sections on • Preventive Controls • Detective controls Reactive Controls
2.00	29-Apr-09	Balu Nair			Approval for Baseline	Baselined
2.01	30-Dec-10	Chakravarthi			QMG review	Formatted entire document
3.00	31-Dec-10	Chakravarthi			Request for baseline	Baselined
3.01	24-May-11	Srilakshmi			QMG Review	Modified release id in header and cover page to make consistency

4.00	24-May-11	Srilakshmi			Approval for Baseline	Baselined
4.01	3-Aug-11	Sudharsana			QMG review	Replace Owner with Management Representative in place of CIO In Document Classification Scheme, "Retention period is 3 Years" row is removed
5.00	3-Aug-11	Sudharsana			Request for baseline	Approved and Baselined
6.00	02-May-12	Srilakshmi			QMG Review	• Modified Template as per documentation standards • Removed Causal Analysis Report and Escalation Matrix • Modified diagram to Visio for contacting specialists in the event of an information security incident. • Removed ISMC roles and responsibilities

						• Provide clarity on all sections Removed diagrams for learning from Information Security Incidents
7.00	08-Nov-12	Balu Nair			Standardization of Blue Book Process Assets	Modified the template format Changed the Logo
8.00	03-Jun-13	Srilakshmi			Re-Certification Audit of ISO 27001:2005 on 07th, 08th, 09th and 10th, May 2013	Modified section 5.3 and 5.4 – clarity is provided for incident resolution, incident follow-up and analysis to prevent recurrence of incidents
9.00	16-May-15	Sudharsana			Upgrading to ISO 27001:2013	Assessment of and decision on

						information security events - Response to information security incidents Collection of Evidence
9.1	15-Feb-2024	Krutideepta	Vijaya R		For Review	1. Non-IT Related Incidents has been added. 2. ISO Mappings has been updated.
10.0	16-Feb-2024	Krutideepta	Vijaya R	Srikanth M	For Review	Approved and Baselined

9.01	25-Jan-16	Paramita Ghosh and Balu Nair			Client Audit and alignment with shared assessment checklist.	• Progress of the incidents (with due consideration for confidentiality) shall be provided to those who reported the incident and all relevant stakeholders. • Data loss incidents • Damage or physical loss of assets • Unauthorized change to privacy information • A 24X7X365 incident response team consisting of Delivery head, CISO and IT Head of respective locations should be present. The Delivery Manager will be the primary contact with the client.
10.00	08-Feb-16	Balu Nair			Approved by Mahesh (CISO)	Baselined

10.01	14-Oct-16	Sriharsha			Addition of Cloud services as scope of Certification.	Modified the process by including the cloud related aspects.
11.00	07-Dec-16	Balu Nair			Approved by CISO	Baselined
11.00	23-Jun-18	Kamadev Pradhan			Reviewed the documents	No changes done in the Document
11.1	29-Apr-19	Balu Nair	Joshy VM			Information classification modified
12.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
12.1	11-May-20	Karthik N	Balu Nair		Review	Updated Incident reporting tools and incident categorization. Integrated with new template
13.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
13.1	9-Feb-21	Balu Nair	Phani Krishna		Review	Updated the information classification Formatted and few minor changes made
14.0	12-Feb-21	Balu Nair	Phani Krishna	Phani Krishna	Approved for Release	Approved and Baselined
14.1	24-Mar-21	Karthik N	Phani Krishna	Phani Krishna	Review	Updated the lessons learned, section 5.7
15.0	25-Mar-21	Karthik N	Phani Krishna	Phani Krishna	For approval	Approved and Baselined
15.1	30-July-21	Karthik N	Phani Krishna	Phani Krishna	Review	Updated the entire procedure as per the standard practice.
16.0	30-July-21	Karthik N	Phani Krishna	Phani Krishna	For approval	Approved and Baselined

16.0	23-Dec-2021	Karthik N	Sivaramakrishnan N		Annual Review	No changes
16.1	23-Feb-2023	Karthik N, Rama Madhavan	Karthik N		For Review	Updated the roles and responsibilities New template change
17.0	09-May-2023	Karthik N	Karthik N	Srikanth M	For Approval	Approved and Baselined
17.1	15-Feb-24	Shalini and Kruti	Vijaya and Bala		For Review	Mapped with new ISO 27k 2022 controls
18.0	23-Feb-24	Shalini and Kruti	Vijaya and Bala	Srikanth M	For Approval	Approved and Baselined
18.1	10-Jan-25	Nagarathinam V	Vijaya R	Srikanth M	For Review	Updated section7.1: Insider Threats, MITM, zero-day attacks and section 7.2, 7.2.5: Forensic analysis 7.26: Monitoring post recovery
19.0	07-Feb-25	Nagarathinam V	Balu Nair and Vijaya R	Srikanth M	For Approval	Approved and Baselined
19.1	18-Mar-25	Krutideepta Barik	Balu N, Vijaya R & Beniyel S		For Review	1. Purpose section changed to Introduction. 2. Roles & Responsibility section: Information Security and Data Privacy Assurance team & Crisis Management Team have been updated. AI.saac Tool has been replaced by MS Sentinel (SIEM) Tool. 3. Responding to an Incident

						section has been updated.
19.2	16-Apr-25	Vijaya	Pranesh & Chaitanya		For Review	1. Updated types of Incidents 2. impersonating CEOs, CFOs, and senior executive's incident management added
20.0	15-May-2025	Vijaya	Pranesh & Chaitanya	Srikanth Mantena	For Approval	Approved and Baselined
20.1	12-Sep-2025	Vijaya, Balu	Pranesh & Siva		For Review	Incident Management Procedure and Security Incident Reporting Procedure combined and RACI is defined Incident Management Reporting Template Revisited
21.0	12-Sep-2025	Vijaya, Balu	Pranesh & Siva	Srikanth	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com