TRIANZ℠

INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

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. Purpose

The purpose of this policy is to ensure a consistent and effective approach to the management of Information Security Incidents, including communication on security events and weaknesses. It enables the efficient and effective management of Information Security Incidents by providing a definition of an Information Security Incident and establishing a structure for the reporting and management of such incidents.

2. Objective

The objective of this policy is to restore normal service operation as quickly as possible in the event of any information security incidents and minimize the adverse impact on business operations, ensuring that agreed levels of service quality are maintained.

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 policy 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 policy applies to all Trianz products and services.

4. Policy

4.1 Incident Identification and Reporting

- Information Security Incidents shall be reported promptly to IT Service Desk and Infosec team by adhering to the SLA’s set as per the Incident Management Procedure and Security Incident Response Plan

4.2 Incident Classification

Incidents shall be categorized based on severity:

- **Low:** Minor policy violations with no sensitive data exposure.

- **Medium:** Potential risk to operations or moderate data compromise.
- **High:** Confirmed compromise of sensitive data or system availability.
- **Critical:** Wide-scale breach or threat to business continuity.

4.3 Incident Response

The following steps must be followed:

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

   - All associates shall be responsible for reporting the information security incidents.
   - Upon receiving/ noticing of the Security Incident from any source(associates/vendors) ,CISO shall mandatorily report cyber incidents within 6 hours to CERT-In. Process is detailed in Security Incident Response Procedure, subject to applicable law.

2. **Assessment and Classification**
   - Key information about Information Security incidents, including the impact of the incident (financial or otherwise), shall be formally recorded.
   - the records shall be analyzed in order to assess the effectiveness of information security controls.

3. **Containment**

   Incidents shall be contained as follows

   - Short-term: Prevent spread or further damage.
   - Long-term: Apply system fixes or configuration changes.

4. **Eradication**

   Incidents shall be eradicated by following the steps below.

   - Remove the root cause of the incident.
   - Apply patches, change credentials, disable compromised accounts.

5. **Recovery**

   Systems and Services shall be Restored to normal operation.

   And Monitored for any signs of recurrence.

6. **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.

4.4 Roles and Responsibilities

- **Employees:** Report incidents and cooperate during investigations.
- **IT Department:** Monitor systems, assist in containment and recovery.
- **Information Security Team:** Lead incident response, investigation, documentation, and communication.
- **Management:** Support policy enforcement and allocate resources.

4.5 Communication and Escalation

- Incidents must be escalated according to classification.
- Communication to external parties (customers, regulators, media) must be coordinated by authorized personnel only.

4.6 Documentation and Record Keeping

- Maintain an incident log detailing each event.
- Retain incident records for a minimum of [X] years, or as required by law.

4.7 Training and Awareness

- Conduct regular training and awareness programs.
- Periodically test incident response through simulations or tabletop exercises.

5. Compliance

- Failure to report an Information Security Incident and any other breach of this policy shall be considered to be a disciplinary matter. Incidents shall be reported to the IS@trianz.com and InfoSec@Trianz.com.
- In specified timeframe, CISO shall adhere to the compliance as per CERT-In guidelines, else it would be treated as non-compliance subject to applicable law.
- Incidents shall be reviewed on periodic basis by the Information security and data privacy assurance to audit policy compliance.
  This is to ensure that the procedures, guidelines, and standards set forth in the Incident Management Process are adhered to

6. Review and Updates

This policy must be reviewed at least annually or after any significant incident to ensure its continued relevance and effectiveness.

- Reference Policies & Procedures

Document Name
Information Security Incident Management Procedure
Security Incident Response Procedure

7. 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 incident management processes, roles and responsibilities.	Information Security Incident Management Policy
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 Policy
Organizational Controls	5.26 Response to information security incidents Control Information security incidents shall be responded to in	Information Security Incident Management Policy

	accordance with the documented procedures.	
Organizational Controls	5.27 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 Policy
People controls	6.8 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 Policy
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 Policy
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 Policy

8. Exceptions(s)

Any requests for exceptions to this policy must be submitted in writing and will be reviewed on a case-by case basis. Exceptions shall be permitted only after documented approval from the CISO/CIO.

Document Control

Owner:	CISO	**Release ID:**	ISIM-POL-0041

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Introduction/Reason for Change	Approver	Change Description
0.1	08 Aug 17	Kamadev Pradhan	Balakrishnan Nair	Creation of Policy		Initial Draft
1.0	23-Jun-18	Kamadev Pradhan		Approved by Ganesh	Ganesh Arunachala	Baselined
1.1	29-Apr-19	Balu Nair	Joshy VM	Review		Information classification modified
2.0	14-May-19	Balu Nair	Ganesh Arunachala		Approved for Release	Baselined
2.1	25 -Oct-19	Karthik N	Phani Krishna	Review		Added cloud aspects to the policy
2.2	30 -Oct-19	Karthik N	Balu	Final review		
3.0	22-Nov-19	Karthik N		Approved for Release to Blue Book	Vivek Sambasivm	Baselined

3.1	12-May-20	Karthik N	Balu Nair	Review		• Roles modified with CISO/CIO. • Updated section 1,2 and 3
4.0	14-May-20	Karthik N	Phani Krishna	For Approval	Phani Krishna	Approved and Baselined
4.1	14-Jan-21	Balu Nair	Phani Krishna	Review		Updated the information classification Formatted and minor changes
4.2	24-Mar-21	Balu Nair	Karthik N	Review	Phani Krishna	Updated the policy statement
5.0	25-Mar-21	Balu Nair	Karthik N	Approval	Phani Krishna	Approved and Baselined
5.1	30-July-21	Karthik N	Karthik N	Review	Phani Krishna	• Added Section 2,5,8 and 9 • Format and minor changes.
6.0	30-July-21	Karthik N	Karthik N	Approval	Phani Krishna	Approved and Baselined
6.0	23-Dec-2021	Karthik N	Sivaramakrishn an N	Annual Review		No Changes

6.1	13-Mar-2022	Kruti	Karthik	For review	For review	The scope has been extended to products and services
7.0	18-Mar-2022	Kruti	Siva N	For approval	Siva N	Approved and baselined
7.1	13-Jul-2022	Beniyel S Divya G	Vijaya R	For review	Siva N	Incorporated CERT-In regulations
8.0	15-Jul-2022	Beniyel S Divya G	Vijaya R	For approval	Siva N	Approved and baselined
8.1	22-Feb-2023	Beniyel S, Shalini Kumari	Karthik N	For Review		Modified section 7. New template change.
9.0	12-May-2023	Beniyel S	Karthik N	For Approval	Srikanth M	Approved and baselined
9.1	15-Feb-2024	Krutideepta	Vijaya R	For Review		1. Policy Statement has been modified as per the new standard ISO 27001:2022.

						2. Non-IT Related Incidents has been added. 3. ISO Mappings has been updated.
10.0	23-Feb-2024	Krutideepta	Vijaya R	For Approval	Srikanth M	Approved and Baselined
10.1	30-Apr-25	Krutideepta	Vijaya R	For Review		Migrated to New template.
11.0	14-May-25	Krutideepta	Vijaya R	For Approval	Srikanth M	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com