TRIANZ℠

Forensic Investigation 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 provide a systematic, standardized, and legal basis for the admissibility of legal evidence that may be required from a formal dispute or legal process.
- To help protect the information assets of Trianz through the application of best practice in IT forensics, there by minimize the impact of information security incidents and safeguarding the interests of Trianz and its clients.
- To maximize the use of digital evidence while minimizing the cost of an investigation

2. Scope

- This policy applies to all Trianz's full time associates, contract employees, vendors processing information assets of Trianz, all Process and Technology in use, whether working from Trianz office or Work from home or client location. However, the responsibility of Forensic Investigation mainly would be with Information Security Incident Managers, Legal Team, IS team, HR Head and the team involved in the security incident.
- This policy also applies to all Trianz products and services.

3. Policy Statement

- IT forensics is the application of techniques to detect and react to types of security incidents that require the collection, storage, analysis and preparation of digital evidence that may be required in legal or disciplinary proceedings.

- The use of IT forensics as a course of action is linked to decisions made during an IT security incident. As such, this policy is linked to, and should be read in

conjunction with, the IT Security – Information Security Incident Management Policy.

- This policy outlines the requirements to collect, preserve and analyse data in a systematic, standardized and legally compliant fashion to ensure the admissibility of evidence in a legal case, dispute or disciplinary hearing relating to an incident.

- TRIANZ is committed to detect and respond to all types of security incidents that require the collection, storage, analysis and preparation of digital evidences in a systematic, standardized and legally compliant fashion to ensure the admissibility of evidence in a legal case, dispute or disciplinary hearing relating to an incident.

- It covers both the proactive forensic monitoring of targeted systems and the reactive investigation of an unforeseen incident.

Such incidents will include but are not limited to:

- ✓ In-appropriate use of equipment
- ✓ Use of another user's logon credentials.
- ✓ Any attempt to circumnavigate existing or proposed security controls.
- ✓ Any attempt to defraud Trianz or its client or Trianz associate.

- Any tasks in a forensic investigation shall be conducted by a suitably trained team including Infosec Team, Legal Team, IS team, HR Head and any other applicable teams basis the incident within Trianz or with the support of an external agency who can assist with the forensic investigation.

- Proactive forensic monitoring comprises of those systems and practices in place at Trianz for monitoring computers, users, groups or systems. Examples include, but are not limited to computer security

logs, email logs, internet traffic monitoring etc.

- Reactive forensic investigations will be on request / approval from Chief Information security officer, Delivery Head, HR Head, Chief Information Officer, President or CEO of Trianz. The report will be shared with CISO, CIO and HR Head for review and further actions.

- All evidence provided as part of a forensic investigation must be recorded and securely stored in such a way as to maintain its integrity and establish the chain of custody until such time, as the case may be, all the hearings and appeals have concluded.

- This evidence may be in the form of log files, emails, back up data, mobile computing, network, removable media and others that may be collected in advance of an event or dispute occurring. All evidence must be version controlled to ensure they are not tampered.

- Any forensic investigation which presents a suspicion of fraud should be notified to the HR Head, CIO and CISO to further include other investigation agencies as required.

4. Roles and Responsibilities

Sl No	Roles	Responsibilities
1.	CISO/InfoSec Assurance Team	• Development and maintenance of the forensic policy • Forensic readiness planning • Periodic reports and briefing to SLT on forensic readiness at Trianz. • Reporting of suspicion of criminal activity to relevant stake holders and further investigations/notification to the Police • Oversight of all investigations • Ensure all incidents and investigations are reported at SLT meetings
2	Information Asset Owners	• Ensure that forensic readiness planning is adequately considered and documented for all information assets where they have been assigned ownership. • Forensic planning shall include: • Ability to gather digital evidence without interfering with business process. • Prioritizing digital evidence gathering to those processes that may significantly impact Trianz, its clients and its associates. • Allow investigation to proceed at a cost in proportion to the incident or event • Minimize disruptions to Trianz. • Ensure digital evidence makes a positive impact on the outcome of any investigation, dispute or legal action
3	Project Managers/Delivery Managers/ Delivery Head	• Responsible for ensuring that the team and area of responsibility operates within the information governance framework of Trianz. Shall ensure that:

		• There are effective methods for communicating information governance related issues within the respective team • Associates receiving relevant training, induction and mandatory updates in relation to information security. • Associates are aware of information security policies and ensure adherence. • Information security risk assessment done at project level/ area of responsibility. • Information security issues and risks are discussed at any team meetings.
4	Information Security Manager / Forensic investigation authority	• Responsible for the management of forensic investigations • Maintain and establish secure chain of custody for the evidence.
5	Trianz legal head / Legal counsel	• Ensure appropriate external relationships are maintained for facilitating forensic investigations by an independent investigator / investigation agency such as police, as the case may be.
6	Trianz's Associates	• All associates must maintain an up-to-date awareness of, and comply with, all Trianz policies, procedures etc. and co-operate with the investigating officer.

5. Definitions

- Forensic readiness
    - Ability of an organization to make use of digital evidence when required. Its aim is to maximize the Trianz's ability to gather and use digital evidence.
- Forensic readiness planning
    - Proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence related monitoring and collection processes and capabilities, storage requirements and costs.
- Chain of custody
    - Chain of custody (CoC), in legal contexts, refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.

6. ISO Control Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Organizational Controls	5.26 Response to Information Security Incidents	Forensic Investigation Policy
Organizational Controls	5.33 Protection of records Control records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Forensic Investigation Policy

Document Control

Owner	CISO	Release ID	FOIN-POL-053

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	30-Apr-19	Joshy VM	Balu Nair		Initial Version	Initial Draft
0.2	02-May-19	Joshy VM	Phani Krishna		Review by Phani Krishna	Policy purpose, scope, statements, roles & definitions modified
0.3	20-May-19	Joshy VM	Ganesh A		Reviewed by Ganesh	
1.0	20-May-19	Joshy VM	Phani Krishna	Ganesh A	Reviewed by Ganesh	Scope and roles
1.1	11-May-20	Karthik N	Balu Nair		Review	Roles modified with CISO/CEO
2.0	14-May-20	Karthik N	Balu Nair	Phani Krishna	For Approval	Approved and Baselined
2.1	28-Jan-21	Vijaya Rajeswari	Phani Krishna		For Review	Information Classification updated

3.0	28-Jan-21	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
3.1	23-Dec-21	Vijaya Rajeswari	Karthik N		For Review	Updated the information classification and formatting changes.
4.0	13-Jan-22	Vijaya Rajeswari	Sivaramakrishnan N	Sivaramakrishnan N	For Approval	Approved and Baselined
4.1	23-Feb-22	Sanjana	Karthik N	Sivaramakrishnan N	For Review	The scope has been extended to products and services
5.0	23-Feb-22	Sanjana	Karthik N	Sivaramakrishnan N	For Approval	Approved and Baselined
5.1	5-Apr-2023	Vijaya, Rama Madhavan	Anjaneyulu		For review	Updated Policy Statement and Roles & Responsibilities Migrated to new template
6.0	3-May-2023	Vijaya	Anjaneyulu	Srikanth M	For Approval	Approved and Baselined
6.1	15-Feb-2024	Vijaya	Balu	Srikanth M	For Review	Updated the section ISO Control Mapping aligning to ISO 27001:2022
7.0	23-Feb-2024	Vijaya	Balu	Srikanth M	For Approval	Approved and Baselined

7.1	17-Apr-2025	Vijaya	Balu		Yearly Review	Migrated to a new template and Yearly Review
8.0	14-May-25	Vijaya	Balu	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com