ASSET MANAGEMENT POLICY

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

Asset Management is the process of identifying, classifying, managing, recording, and coordinating the Trianz assets to ensure their security and the continued protection of confidentiality, integrity and availability of data. For the purposes of this policy and associated asset management processes, Trianz defines an 'Asset' as any item, system, application or entity that has potential or actual value to our organization.

2. Purpose

The purpose of this policy is to manage organizational assets (tangible and intangible) and to document those assets to ensure knowledge and understanding of their value, purpose, risk, and location.

Trianz ensures that all assets are assigned an Information Asset Owner (IAO) who has overall responsibility for managing, updating, recording, and destroying the asset. The nature and value of every asset is documented and understood for better enabling the Trianz to restrict access where applicable, develop effective recovery and continuity programs, optimize spending, support lifecycle management, strategic decision-making within Trianz and protect the interests and assets belonging to customers and clients.

Understanding these assets enables us to manage our organization's information and systems and the risks associated with them. For this purpose, we utilize an Information Asset Register (IAR)enabled by a tool to identify, document and map all information assets, and assign them an owner. In addition cloud assets are managed and controlled by Cloud Administrators.

3. Scope

- Applicable to all Assets at Trianz located on premises, offshore, client premises and cloud infrastructure.
- Client specific information classification policy (if any) shall supersede this policy into specific engagement for client's information asset as per client's contractual requirements.

4. Objectives

Asset classification is to ensure that individuals who have a legitimate right to access a piece of information can do so, whilst also ensuring that assets are protected from those who have no right to access them.

This policy helps all Trianz employees to ensure that correct classification and handling methods are applied to their day-to-day activities and managed accordingly.

This policy is to ensure,

All assets must be handled and managed in accordance with their classification.

- Trianz assets should be made available to all who have a legitimate need to access them.
- The integrity of information must be maintained; information must also be accurate, complete, timely and consistent with other related information and events.
- All Trianz employees who have access to assets, have a responsibility to handle them in accordance with asset classification.
- Asset owners are responsible for ensuring that the Trianz classification scheme (which is described in the Information Security Policy) is used appropriately.

- All the unauthorized addition, removal, update, and management of organization assets shall be restricted.

5. Policy

5.1 Asset Identification:

• All information assets and assets associated with information and information processing facilities shall be identified.

5.1.1 Asset classification

Information assets classified at Trianz in four categories as listed below:

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

These are main categories of assets:

- Information– this includes databases, system documentation and procedures, archive media and data.
- Software – this includes application programs, cloud service applications, systems, development tools and utilities.
- Physical – this includes infrastructure, equipment, furniture and accommodation used for data processing.
- Services – including computing and communications used for data processing.
- People – including qualifications, skills and experience in the use of information systems Other – for example contracts and agreements etc.

5.1.2 Asset Register/Asset inventory

- An inventory of such identified assets shall be established and maintained.

- Asset inventory should account for information stored in the cloud-computing environment as a cloud service customer.

- Inventory of assets should identify cloud service customer data and cloud service derived data as a cloud service provider.

- Asset inventory shall be regularly updated and periodically audited.

5.2 Asset Tracking

- All Assets must be tracked to make sure that all assets are intact and available for use.

5.3 Asset Tagging

- All assets must be tagged for easy identification and to ensure proper traceability.

5.4 Asset Review

- All the assets will be reviewed on a quarterly basis and email communication shall be sent to each individual asset owner.
- Scheduled regular maintenance must be carried out based on the asset's usage and manufacturer's guidelines as preventive maintenance and measures

5.5 Secure Disposal:

- Organization Assets need to be securely disposed when no longer needed. This includes removal of Physical devices, Hard copies or Digital assets, cloud service customer assets that has information.

6. Acceptable Use of Assets

- The purpose of this policy is to outline the acceptable use of computer equipment's at Trianz. These rules are in place to protect the employee and other information's assets.
- Inappropriate use of these assets exposes to risks including virus attacks, compromise of network systems and services, and legal issues.

- Refer Acceptable usage policy.

7. Information Labelling, Handling and Disposal

- Trianz employs a labelling system that categorizes the content of systems, files, applications and documents, without the necessity of disclosing the actual contents. This enables our employees to understand what content or information resides on a system or in a location, without accessing or seeing the personal content.
- Labelling allows us to document and control information, whilst still respecting access restrictions.

  Please refer to Media Handling, labelling and disposal policy.

8. Compliance and Monitoring

- All assets should be classified and managed as per this policy.
- IT and digital assets should use encryption, firewalls, and access controls to safeguard data.
- This policy is subjected to review at least annually or whenever there is a change in the requirements of Information Asset management policy.

9. Roles and Responsibilities.

SL. No.	Roles	Responsibilities
1	Information Owner	Classifying the documents as per the policy
2	Function Owner	Make sure that information is classified as per this policy
3	CISO/CIO	Approve the policy and ensure its implementation
4	IS Manager	Approve acquisition or disposal of Information Technology assets.
5	IS Asset Coordinator	Responsible for Tracking Information Technology assets through their acquisition, distribution, use, and disposal and for ensuring that all Information Technology asset management policies conform to Trianz standards.
6	Service desk Coordinator	Responsible for logging, testing, accepting, installing, maintaining, and preparing for disposal of Information Technology assets. Service desk is also responsible for updating the Information Technology Asset Inventory when any changes to Information Technology assets have been made.

7	Purchase Coordinator	Responsible for ordering physical Information Technology assets.
8	Asset Owner	Asset owner is accountable for ensuring assets are classified appropriately
9	Project Manager	Responsible for maintaining the Asset Risk Register/ Asset Inventory.

10. Exception(s)

There is no exception to this policy.

11. ISO Control Mappings

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Organizational Controls	5.9 Inventory of information and other associated assets Control An inventory of information and other associated assets, including owners, shall be developed, and maintained.	Asset Management Procedure
Organizational Controls	5.10 Acceptable use of information and other associated assets Control Rules for the acceptable use and procedures for handling in formation and other	Asset Management Procedure

	associated assets shall be identified, documented, and implemented.	
Organizational Controls	5.11 Return of assets Control Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Asset Management Procedure

Document Control

Owner:	CISO	Release ID:	ASMP-POL-056

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	23rd Oct 2019	Karthik N	Phani Krishna		Initial draft	None
0.2	30Oct-2019	Karthik	Balu		Changes made as per Balu's feedback	
0.3	4-Nov-19	Karthik	Phani Krishna		Review	
1.0	20Nov-19	Balu Nair		Vivek Sambasi vam	Approved for release to blue book	Baselin ed
1.1	11May-2020	Karthik N	Balu Nair		Review	Changed the template
2.0	14May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined

2.1	18Jan-2021	Ankur Rastogi	Rakesh Vijendra		Initial Version	Asset Management Policy updated in alignment with ISO 20k – 2018 standard
3.0	18Jan-2021	Ankur Rastogi	Rakesh Vijendra	Vivek S.	Baseline and Approval	Baselined version
3.1	22Dec-21	Balu Nair	Karthik N		Yearly Review	Corrected few areas & formatted to increase the readability
4.0	13Jan-2022	Balu Nair	Siva N	Siva N	Baseline and Approval	Baselined version
4.1	13Mar2022	Sanjana	Balu N		For review	The scope has been extended to products and services
5.0	20Mar2022	Sanjana	Siva N	Siva N	For Approval	Approved and baselined
5.1	07Apr2023	Shivateja, Rama Madhavan	Karthik N	SrikanthM	For Review	Added Asset Review and Secure Disposal New template change
6.0	03May2023	Shivateja	Karthik N	Srikanth M	For Approval	Approved and Baselined

6.1	15-Feb-2024	Beniyel S	Vijaya R		For Review	ISO Control Mappings has been updated.
7.0	23-Feb-24	Beniyel S	Vijaya R	Srikanth M	For Approval	Approved and Baselined.
7.1	04-March-2025	Krutideepta Barik	Vijaya R, Balu Nair & Beniyel S		For Yearly Review	1.Purpose & Objective Section has been updated and modified. 2. Included Compliance on IT and digital assets to safeguard data, preventive measures based on usage and guidelines Migrated to a new Template.
8.0	14-May-2025	Kruti	Vijaya R	Srikanth M	For Approval	Approved and Baselined.

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com