TRIANZ℠

ASSET MANAGEMENT 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 purpose of Asset Management procedure is to establish a formal, structured and precise process for classifying and managing Assets in accordance with Information Security Policy and Asset Management Policy.

2. Objectives

The Asset Management procedure describes the mechanism, Trianz will use to develop and maintain best practice in asset management. The key objectives in this area that are to:

- Establish a structured framework for managing information assets effectively.
- Define roles and responsibilities for asset management.
- Ensure accountability for asset identification, classification, and protection.
- Ensure accountability for information assets across all business functions.
- Ensure adequate resources to ensure effective implementation and continuous improvement of asset management practices.
- Maintain a comprehensive asset inventory, including hardware, infrastructure, equipment, and licenses.
- Improve visibility into the actual cost of assets for better financial planning.
- Ensure detailed asset insights to assess the Total Cost of Ownership (TCO) of IT services.

3. Scope

All employees, contractors, part-time and temporary workers, and those who are employed by others to perform work regardless of geographical location, are covered by this procedure and must comply with associated policies and procedures.

This procedure applies to all the assets available in all forms but not limited to physical and electronic form.

This procedure applies to all the assets available on premises, either with vendor, suppliers, partners etc. or on cloud.

4. Assets

Assets are used to deliver services within Trianz. Assets will also include the computer systems, Cloud, network hardware, software etc. that are used to process the data. Some assets in a service are also configuration items (CIs) subject to configuration management. For example, a service monitoring application or a server are assets that are likely to be CIs, because they are critical to delivering the service and need to be controlled.
Non-computerized systems holding information must be asset registered with relevant file identifications and storage locations.

These are main categories of assets:

- Information– this includes databases, system documentation and procedures, archive media and data.
- Software – this includes application programs, 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. Asset Risk assessment

Risk assessment has to be carried out all the assets of Trianz.
Please refer to Risk and Opportunity Management Procedure.

6. Asset Management Procedure

6.1 Asset Identification:

- Identify all the assets pertaining to the project along with the source (Client/Trianz).Identify all the assets pertaining to the corporate function.

6.2 Asset Register/Asset inventory

- All Assets shall be documented in an asset register/asset inventory.
- Assets should also include the assets in the cloud-computing environment as a cloud service customer and inventory of assets should identify cloud service customer data and cloud service derived data.
- The Asset Register will be held and maintained by respective project managers/leads.
- The data/Information owner based on data type, value, sensitivity, and criticality to the organization must classify data and objects containing data.

.

6.3 Asset Tracking

- All assets shall be tracked using the asset management control doc tool as per the categories mentioned below.
- Asset categories – For e.g. desktop, laptop, HDD, network assets, printers, cloud assets, servers, storage, TV, projectors, RSA tokens and information assets critical documents and data.
- Procurement mode – For e.g. rental, purchase direct lease etc.

- Asset status – For e.g. active, damaged, e-waste, not working, End of life, theft etc.
- Asset location - any location
- Vendor/agency
- Asset id
- Serial number
- Assigned to
- Warranty/ insurance
- Project code
- Asset allocation date
- Organization's Assets which was assigned to individuals or projects/functions for Business purposes should be returned in case of termination or transfer of respective individual or a group.

.

6.4 Asset Tagging

- Physical Assets shall be tagged as per the Guidelines for Information Labelling & Handling. All other information assets will be tagged based on the respective license / subscription details.

6.5 Asset Review

- All the assets will be reviewed on a quarterly basis and email communication shall be sent to each individual asset owner.
- The purpose of this activity is to maintain asset records: change, update, or delete asset data as required.
- Incident Management, Problem Management and Configuration Management can trigger modifications to asset data. This activity also administers the asset database and performs asset reconciliation.
- The asset database includes all assets with a status designation such as ordered, in storage, assigned, retired, or disposed of, etc.

- Asset owner should acknowledge and confirm the status of the assets they own.

6.6 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.
- Disposal of Assets may determine that an asset is:
  - Obsolete
  - Unserviceable
  - To be traded in
  - To be sold
  - Missing (stolen)
  - To be disposed of by other means.

Please refer to Data Retention And Secure Disposal Policy

6.7 Acceptable usage of Assets.

- All Trianz assets shall be used only official purposes and project manager should ensure accordingly.
- Personal assets shall not be allowed in the Trianz premises and secure areas and depends on the project needs and requirements with necessary approvals.

Refer Acceptable usage policy.

6.8 Monitoring, Auditing, Compliance and Reconciliation of Asset Records

- In this activity, compliance status for licensing and information security requirements is also monitored.
- Formal inventory audits of all physical assets occur in this activity. Additionally, audits of the Asset Management System and audit reconciliation are performed.
- Audits of logical assets include installed software on workstations and IT configurations or as required by the organization.
- Compliance with this procedure is mandatory and all project managers must ensure continuous compliance monitoring within their projects.
- Compliance with the statements of this procedure is a matter of periodic review by Internal Audit and any violation of the procedure will result in corrective action by the management.
- An earlier review may be warranted if one or more of the following occurs:
    - As a result of regulatory/statutory changes or developments
    - Due to the results/effects of critical incidents
    - Or any other relevant or compelling reason

7. Roles and Responsibilities

Each role involved in this procedure should have main responsibilities as follows:

Role	Responsibilities
CISO	• Ensures organization's asset management strategy aligned with security policies and regulatory requirements. • Approve acquisition or disposal of assets.

Infosec Team	• Accountable for ensuring that the “Asset Management policy and “Asset Management Procedure” (to classify asset, identify asset’s value and manage appropriately) is properly communicated and understood within its respective organizational units with the approval of CISO.
Project Manager	• Accountable for ensuring that the “Information Asset • Classification policy and “Information Asset Management Policy & Procedure” are properly communicated and understood within their project teams. • Responsible for ensuring all project assets are classified, approved and adequate user access controls are implemented • Responsible for the design of the information system and ensuring classification of the information processed by the systems. • Responsible for maintaining and updating the assets inventory.
Asset Owner	Accountable for ensuring information assets are classified as per organization Information Asset Management Policy.
User	Responsible for complying with the “Information Asset Management policy and Information Asset Management Procedure”. Responsible for protecting the assets entrusted to the user.
IS Senior Manager	• Ensure capacity planning, acquisition, deployment, maintenance, and disposal of IT assets. • Manage IT asset procurement, track financials, and optimize cost efficiency. • Ensure IT assets are protected against security incidents and properly managed during changes. • Maintain an up-to-date asset inventory, generate reports, and ensure visibility of IT assets.

IS Asset Coordinator	Responsible for Tracking assets through their acquisition, distribution, use, and disposal and for ensuring that all Information Technology asset management policies conform to Trianz standards.
Purchase Coordinator	Responsible for procurement of assets

8. Acronyms/Abbreviations

Acronym/Abbreviation	Expansion
ITAM	IT Asset Management
HAM	Hardware Asset Management
SAM	Software Asset Management
AMC	Annual Maintenance Contract

8.1 Related Guidelines, Templates and Checklists

Document Name
Media Handling
Data Retention and Disposal Procedure
Acceptable usage policy

9. Measurement

Key Performance Indicator (KPI)	Definition
New Asset purchases	☒ Number of new purchases made of asset types
Assets in Stock	☒ Number of assets updated as "in stock", "reserved" or "deployed" from status "in-transit" or "received"
Assets Lost	☒ Number of Change requests for 'lost/stolen' over period
Assets Deployed	☒ Number of requests to deploy assets over period
Assets Disposed	☒ Number of requests for asset disposal

10. ISO Control Mapping(s)

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 associated	Asset Management Procedure

	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:	AMP-PROC-0129

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	24th Oct 2019	Karthik N	Phani Krishna		Initial Draft	None
0.2	5th Nov 2019	Karthik N	Phani Krishna		Review post changes suggested by Phani	Review changes incorporated
1.0	20-Nov-19	Balu Nair		Vivek Sambasivam	Approved for release to bluebook	Baselined
1.1	11-May-2020	Karthik N	Balu Nair		Review	Roles modified with CISO/CIO Integrated with the new template
2.0	15-May-20	Karthik N	Phani Krishna		For Approval	Approved and Baselined
2.1	18th Jan 2021	Ankur Rastogi	Rakesh Vijendra		Initial Version	Asset Management Procedure updated in alignment with ISO 20000-1 : 2018 standard
3.0	18th Jan 2021	Ankur Rastogi	Rakesh Vijendra	Vivek S.	Baseline and Approval	Baselined version
3.1	22-Dec-2021	Balu Nair	Karthik N		Yearly Review	Corrected few areas & formatted to

						increase the readability
4.0	13-Jan - 2022	Balu Nair	Siva N	Siva N	Baseline and Approval	Baselined version
5.1	14-Mar-2022	Kruti	Karthik N		For Review	The scope has been extended to products and services
6.0	20-Mar-2022	Kruti	Siva N	Siva N	For Approval	Approved and baselined
6.1	07-Apr-2023	Shivateja, Rama Madhavan	Karthik N	Srikanth M	For Review	Reviewed with no changes Migrated to new template
7.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
7.1	10-Jan-2024	Beniyel	Balu Nair, Vijaya R		For Review	Updated with ISO/IEC 27001:2022 standard requirement on “return of Assets during termination/transfer” in section 6.3 ISO Controls Mappings has been updated.
8.0	23-Feb-24	Beniyel	Balu Nair, Vijaya R	Srikanth M	For Approval	Approved & Baselined.
8.1	04-March-25	Krutideepta Barik	Vijaya R, Balu Nair & Beniyel S		For Yearly Review	Objective, Scope, Asset Risk assessment, Asset Identification, Asset

						Resister/Inventory, Asset Tagging section has been Updated & Modified. CISO, Infosec Team, IS Senior Manager, Purchase Coordinator Roles and Responsibilities have been modified. Migrated to a new Template.
9.0	14-May-2025	Kruti	Balu Nair, Vijaya R	Srikanth M	For Approval	Approved & Baselined.

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com

The content in this document is copyrighted; any unauthorized use – in part or full – may violate the copyright, trademark, and other laws. This document may not be modified, reproduced, or publicly displayed, performed, or distributed, or used for any public or commercial purposes. The Trianz name and its products are subject to trademark and copyright protections, regardless of how and where referenced.