TRIANZ℠

Media Handling 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

Improper handling of removable media will cause data loss and data leakage. Removable media can contain sensitive information which can pose serious security threats if it gets corrupted or accessible to an unauthorized person. This policy states the media handling requirements to ensure confidentiality, integrity, availability, and privacy of the information.

2. Objective

To ensure the secure management of media to protect sensitive or personal information from intentional or accidental exposure or misuse.

3. Scope

This policy applies to all Management, Employees, Contractors, and Third-Party Employees, who use the media of Trianz. Also, this policy applies to all products and services, organizational IT assets of Trianz.

4. Privacy

The media handling policy document shall be considered as “confidential” and shall be made available to the concerned person with proper access control. Subsequent changes and versions of the document shall be controlled.

5. Policy Statements

5.1 Media Handling

- All Trianz associates are responsible for ensuring physical security of the media.
- Use of USB flash drives shall be blocked for all the associates. Use of the same by associate shall be permitted only after the approval from CIO/CISO.
- Personal CDs/DVDs/data tapes/hard disk drives/flask drives/external memory cards and other devices shall not be allowed.

- Use of CD/DVD writers shall be restricted to all the associates. The use of the printer facility will be restricted to official use for all employees.
- All media should be handled with care, and it must be ensured that it is not kept near magnetic material and not exposed to extreme heat or pollution.
- Compliance with this policy is the responsibility of the overall delivery and corporate functions.

5.2 Media Shipping for Work-from-home Associates

- All devices containing information must be shipped securely and special procedures to be followed over and above this policy when Associates are working from home.
- This is required as shipping shall be done from Trianz office or to or between Non office locations.
- In case of media in transit Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification.
- A record must be maintained for incoming and outgoing physical media containing Personally Identifiable Information or Personal Data or Personal Sensitive Data.
- In case of media in transit, packaging should be adequate to protect the contents from any physical damage in accordance with manufacturers' specifications.

5.3 Disposal of Media and equipment

- Media shall be disposed off securely and safely when no longer required. Sensitive information may be leaked to outside persons through careless disposal of media.
- If no longer required, the previous content of any re-usable media that is to be removed from the company should be deleted by low-level formatting by obtaining prior approval from CISO/CIO.
- Disposal of sensitive items must be logged to maintain an audit trail and for other regulatory requirements.

- All items of equipment containing storage media will be checked for confidential information and the same will be backed up or removed prior to disposal.
- Storage devices containing sensitive information are physically destroyed or securely overwritten. For example, low level formatting is done rather than using the standard "Delete" function.
- All licensed software installed on the equipment will be removed before disposing of the same.
- Damaged storage devices containing sensitive data are checked for data access and then the decision is taken whether to repair, discard or destroy it.

5.4 Removal of Equipment

- Equipment (like desktops, Laptops, Servers, VOIP phones etc.), information or software will not be taken off-site without prior authorization from IS Operations and CISO/CIO.
- Verification Report shall be prepared by authorized IT representative and sent either physically signed (or) email to admin for preparing gate pass.

5.5 Reuse of Equipment

- Equipment shall be re-used where feasible. Data and software will be removed securely, and the equipment re-provisioned for use.
- Dismantling and re-use of parts if there is any potential for recovering valuable components from the item.
- Equipment will be recycled on a unit or component level using the external disposal contract and company co-ordinated by IT Services.

6. Roles & Responsibilities

Roles	Responsibilities	Internal/External
All Associates, Including,	Any exception to this policy, raise a request with proper business justification	Internal

Contract Employees	and obtain the approval from the reporting Manager and CISO/CIO	
Admin Team	Ensure all the logistics in line with this policy and related procedures	Internal
IS Operation Team	Ensure all the IS operations in line with this policy and related procedures	Internal
Infosec Team (CISO/CIO)	Approval of exception based on the business justifications & Risk of information loss	Internal

7. Applicable standards

ISO 27001:2013

ISO 27701:2019

8. Reference Policies & Procedures

Media Handling Procedure of Work from Home Associates

Data Retention and Secure Disposal Policy

Information Removal Verification Report Template

9. Implementation Procedures

TDCPL Administration Procedure
ISO Operations Process
Physical Access Control and Environmental Security Policy and Procedure

10. Exceptions(s)

This policy applies to all Trianz Associates. Any project specific needs & CISO/CIO approved systems will be excluded from this policy, with prior approval from the project managers and IS Operations.

Refer to *Exception Handling Policy*

11. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action in line with the HR policy.

12.ISO Control mapping(s)-

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Physical Controls	7.10 Storage media Control Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Media handling Policy
	7.10 Storage media	

Document Control

Owner:	CISO	**Release ID:**	MH-POL-0007

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 is approved by Zulfikar Deen.	Approved
1.01	30-Jul-08	Bharateesha B R			Revised the policies in accordance with the revised ISMS Framework	Changed the Policy statements, Changed the template Added Document Classification Scheme
2.00	28-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	06-May-11	Srilakshmi			To maintain common release id allocation for bluebook documents	Modified Release ID in cover page and header

4.00	06-May-11	Srilakshmi			Request 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
5.01	14-Oct-11	Venkateswar Reddy GD			QMG Review	Used new template as per documentation guidelines ‘Shall’ word is replaced by ‘Will’ throughout policy Reviewed for continued suitability
6.00	14-Oct-11	Venkateswar Reddy GD			Approval for Baseline	Baselined
7.00	08-Nov-12	Balu Nair			Standardization of Blue Book Process Assets	Modified the template format Changed the Logo

7.1	25-Jan-16	Balu Nair			Client Audit and alignment with shared assessment checklist.	Added Removal of Equipment Added Reference section
8.0	08-Feb-16	Balu Nair			Approved by Mahesh (CISO)	Baselined
8.1	29-Apr-19	Balu Nair	Joshy VM			Changed the Trianz logo Information classification modified
9.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
9.1	13-Nov-19	Anitha Ravindran	Phani Krishna		Updated for meeting requirements of 27018	Updated requirements for Physical media in transit containing PII
10.0	22-Nov-19	Anitha Ravindran	Phani Krishna	Vivek Sambasivam		Baselined version
10.1	08-May-20	Balu Nair	Phani Krishna			• Added CISO as an approval New Template format

11.0	14-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
11.1	28-Jul-20	Balu Nair, Vijaya Rajeswari	Phani Krishna		For Review	Approval of CISO/CIO for Removal of Reusable Media is added as responsibility, Formatted the document for more legibility
12.0	30-Jul-20	Balu Nair, Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	• Approved and Baselined
12.1	15-Sep-20	Anitha Ravindran	Phani Krishna	Phani Krishna	Updated Policy for Covid-19 related circumstance of need for shipping devices from non-office locations	Added Policy for shipping devices from non-office locations
13.0	15-Sep-20	Anitha Ravindran	Phani Krishna	Phani Krishna	Baselined and approved Version	Baselined and approved Version
13.1	11-Feb-21	Balu Nair	Phani Krishna		Review	Updated the information classification
14.0	11-Feb-21	Balu Nair	Phani	Phani	For Approval	Approved and Baselined

			Krishna	Krishna		
14.1	30-Jul-21	Balu Nair	Phani Krishna		As part of Annual review and inputs from external audit	Changed the template and totally revamped the policy
15.0	30-Jul-21	Balu Nair	Phani Krishna	Phani Krishna	Approved for Baseline	Baselined
15.0	06-Jan-22	Krutideepta	Balu Nair		For Review	No Changes
15.1	17-Mar-22	Sanjana	Balu Nair		For Review	The scope has been extended to products
16.0	21-Mar-22	Sanjana	Siva N	Siva N	Approved for Baseline	Baselined
16.1	03-May-23	Shalini and Asha Veeramallu	Balu Nair	Srikanth	For Review	Field 4, Privacy, Changes in policy statement and enforcement is added New template change
17.0	08-May-23	Shalini	Balu Nair	Srikanth	For Approval	Approved and Baselined
17.1	04-May-23	Shalini	Vijaya	Srikanth	For Review	• Editorial changes
17.2	15-Feb-24	Shalini	Vijaya	Srikanth	For Review	• Mapped with New ISO control 7.10

18.0	23-Feb-24	Shalini	Vijaya	Srikanth	For Approval	• Approved and Baselined
18.1	5-May-25	Vijaya	Balu			• Migrated to new template
19.0	14-May-25	Vijaya	Balu	Srikanth	For Approval	• Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com