TRIANZ℠

Media Handling Procedure of Work From Home Associates

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

Purpose of this document is to describe the Media Handling procedure when requests are raised to ship devices containing Information across Non office locations especially when Associates are working from home.

2. Objective

To ensure that any Media or devices like Laptops having information (Personal, Sensitive, Confidential) are shipped securely and all corresponding actions are addressed proactively so as to minimize any information risks.

3. Scope

- All Associates (Permanent and contractor employees)
- All corporate functions & Delivery functions in Trianz
- All Trianz products and services

4. Roles and Responsibilities

- All Employees, contractors or temporary personnel are responsible for following Consent Procedure before collecting any personal data.

Role	Responsibility	Internal/ External
All Associates , Including, Contract Employees	Raise requests with admin team, IS team with necessary approvals as indicated in the procedure	Internal

Admin Team	To ensure shipping the devices across Non Office locations by working with the Vendors following steps mentioned in procedure	Internal
HR Operations team	Wherever appropriate esp for Associates serving resignation as indicated in procedure coordinate with Associate for a smooth implementation of this process ensuring the workflow	Internal
IS team	Ensure verification and / or required implementation for safeguarding data or information in the device	Internal
Purchase Team	Ensure required Insurance and or Vendor agreements are in place	Internal
Infosec Team	Any approvals for exception to this process or clarifications on this procedures	Internal

5.Media Shipping for Work-from-home Associates

For Trianz owned Information Assets (eg: Laptops)

• For new hire – same as onboarding process and no change in this

- For resigned Associates, HR to communicate to Associate to raise a request with IS @trianz.com with subject "**IS Verification and approval for shipping device(laptop) due to resignation"**

- For other active Associates where employment is active, in case of any required movement from one associate to another, Admin to communicate to Associate to raise a request with IS @trianz.com with subject "**IS Verification and approval for shipping device(laptop) for Project purpose**"

- IS team to Verify the following once request is received from Associate o Live video call for checking Health or condition of the Device(Laptop)

    o In case of Devices (laptop) of resigned Associates, remote wipe to be performed, if possible o If remote wipe is not possible technically or due to project need,

    - verify if encryption is enabled
    - enforce Associate to get an approval from PM that there is no critical client or Trianz data
    - relevant data is backed up from the device o IS team to give a go ahead after the above steps are completed to Admin team for going ahead with shipping

    o Admin team to go ahead with the shipping after receiving go ahead from IS team

    For Client owned Information Assets (Eg. Laptops)

    o   Admin team to ensure below:

- enforce an approval and confirmation from PM that there is no critical Client or Trianz Data in Device (Laptop)

  - adequate backups have been taken for the data on the Device (Laptop) o Admin to proceed ahead with Shipping if above steps are completed

    o The other generic points that Admin team needs to look into still holds good wherever required with Purchase team-

    o If we can have agreements with Shipping vendors (loss recovery or Damages cost, nondisclosure clause) (agreement for DTDC, Bluedart)

    o Feasibility of Insurance (Please check transit damage) o Update in the Asset movement register

For both assets irrespective of ownership,

Following must be ensured by Admin team: - o Packaging should be adequate to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications

    o Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification e.g. use of locked containers, Tamper-evident packaging (which reveals any attempt to gain access)

  Following must be ensured by Admin and Purchase team o Agreements with Shipping vendors to be ensured with adequate clauses giving protection to the asset during transit like loss recovery or damages cost, non disclosure clause)

o   Insurance to be ensured wherever possible   o   Update in the Asset

  movement register

- type of physical media

- the authorized sender/recipients

- the date and time

- number of physical media

- If any Personal or critical information is present

6. Resources

- Admin Team
- Information Systems Team
- Purchase Team
- HR Operations team
- Information Security Assurance Team

7. Training

- None

8. References

Media Handling Policy
Data Disposal Policy , procedure and template

9. ISO Control Mapping(s)-

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022

Technological 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 Procedure for Work from home associates

Document Control

Owner:	CISO	Release ID:	MEDHL_PROC_0133

For Trianz Process Improvement Group (TPIG) Purpose only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.01	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
1.0	21-Sep-20	Anitha Ravindran	Phani Krishna	Phani Krishna	Baselined and approved Version	Baselined and approved Version
1.1	28-Jan-2021	Vijaya Rajeswari	Phani Krishna		For Review	Information classification updated
2.0	28-Jan-2021	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
2.0	06-Jan-22	Divya	Balu Nair		For Review	No Changes

2.1	24-Feb-2022	Kruti	Karthik		For Review	The scope has been extended to products and services
3.0	18-Mar-2022	Kruti	Siva N	Siva N	For Approval	Approved and baselined
3.1	03-May-2023	Shalini, Rama Madhavan	Balu Nair	Srikanth	For review	Reviewed and No changes Migrated to new template
4.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
4.1	15-Feb-24	Shalini	Vijaya	Srikanth	For Review	Mapped with new ISO control 7.10
5.0	23-Feb-24	Shalini	Vijaya	Srikanth	For Approval	Approved and Baselined
5.1	28-May-25	Kruti	Vijaya		For Review	Migrated to new template
6.0	29-May-25	Kruti	Vijaya	Srikanth	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com