TRIANZ℠

Backup and Restoration 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 **4**

2. OBJECTIVE **4**

3. SCOPE **4**

4. ROLES & RESPONSIBILITIES **4**

5. POLICY **5**

5.1 Back up and Restoration Cycle 5

5.2 Data Back Up 6

5.3 Data Restoration 7

5.4 Validation and Testing 8

5.5 Archives 8

5.6 Disposal 8

6. MEASUREMENT AND REPORTING **8**

7. COMPLIANCE **8**

8. EXCEPTIONS(S) **9**

9. ISO CONTROL MAPPING(S) **9**

1. Purpose

The purpose of this policy is to identify and establish processes, procedures and good working practices for the backup and timely recovery of Trianz's & client's information and data existing in both electronic and physical form within Trianz Managed Systems.

2. Objective

The objective of the policy is to ensure that optimum backup and proper restoration is provided to physical and logical systems operated by Trianz.

3. Scope

The scope of this policy extends to the back up of all important information and data regardless of the form it takes - including the recovery of IT systems and supporting infrastructure. This policy applies to data available on premises and data in the cloud environment, wherever applicable.
The policy applies to all Trianz managed products and services.

4. Roles & Responsibilities

Sl No.	Item	Roles	Responsibility
1	Data Back up	IS Operations /Project team /Product team	• Ensure that Trianz data is securely maintained and is available for backup. • Ensure that data backup and restoration should follow Trianz backup and restoration procedure while taking backup.

2	Data Encryption	IS Operations. /Project team /Product team	⊠ Data must be encrypted while taking backup, wherever applicable.
3	Data Restorations	Function Owner	⊠ IS/Project/Product Support team restores the sample data, monthly once from any one of the backups taken during the month.
4	Audit & Compliance	InfoSec & Data Privacy Assurance	⊠ Data and restoration process to be checked yearly basis.
5	Breach of Policy	HR	⊠ HR takes necessary action in case of any breach of policy as per the disciplinary action mentioned in the HR Policy.

5. Policy

5.1 Back up and Restoration Cycle

The standard back up cycle is defined in the Backup and Restoration procedure is daily, weekly and Monthly.

5.2 Data Back Up

- IS Operations, delivery teams and product teams are responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed in line with Trianz's Disaster Recovery Procedures and Data Retention policies.

- All data shall be systematically backed up and updates which may be required in the event of system re-installation and/or configuration.

- The backup files must be encrypted and appropriately labelled wherever applicable. Any system used to manage backed-up files should enable storage of date/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media.

- All encryption keys should be kept securely at all times with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster.

- If data to be backed up contains any Personal Data or Personal Sensitive Data or Personally Identifiable information, it needs to be anonymized (unidentifiable) or erased, depending on the legal and regulatory requirements, as practical and as applicable.

- A recording mechanism must be in place and maintained to record all backup information such as function, data location, date, type of backup (e.g. Incremental, Full etc…) including any failures or other issues relating to the backup job.

- Copies of backup media must be removed from devices as soon as possible when a backup or restore has been completed.

- Access to the on-site backup location (On premises or cloud) and must be restricted to authorized personnel only.

- Data stored on-prem or cloud shall be backed up based on defined frequency.

- Backup media must be protected in accordance with the Data Protection and Media Handling Policies.
- Backup data/media no longer required must be clearly marked and recorded for secure disposal and with due environmental consideration.

5.3 Data Restoration

- Function Owner's must request data (files) to be restored by contacting the IS Operation's Service Desk, Project/Product infra management team, preferably by raising a service ticket using the IS Service Desk online facility. Only files which the user is authorized to access will be provided from the restore.
- IS Operation's Service desk Team will need to verify that the user has permission and/or authorization to view or obtain restored copies of file/s and/or folder/s. Content will be restored to the same source folder or the same area, so any requestor will need access to that folder/area to access the restored files.
    - Function Owner's requesting a restore/s are required to provide as much information about the data (file/s) as necessary – this will include:
    - The reason for the restore.
    - The name of file/s and/or folder/s to be restored.
    - Original location of file/s and/or folder/s - the Service Desk will provide guidance to the User on how to find this out.
    - Date, day or time of deletion/corruption or nearest approximation.
    - The last date, day or time which the User recalls the data (files) being intact and accessed/used successfully.
    - All backup and recovery (restore) procedures must be documented and made available to Data Centre personnel responsible for carrying out data (file) restores.
    - Requests from third party software/hardware vendors for file or system restores for the purpose of system support, maintenance, testing or other unforeseen circumstance should be made under the supervision of the Server Support Team via the IS Operations Service's Service Desk.

- Personnel accessing backup media for the purpose of a restore must ensure that any media used is returned to a secure location when no longer required.
- A log must be maintained to record the use of backup media whenever it has been requested and/or used from secure storage.

5.4 Validation and Testing

- IS Operations/Project, Product infra management team being responsible for periodic testing of Backup and recovery services.
- Function owners are responsible to confirm the data restoration validation to IS Operations.

5.5 Archives

Data archival to be conducted as per the Data Retention policy.

5.6 Disposal

Backup data/media shall to be disposed in a secure manner.

6. Measurement and Reporting

Frequency and type of data backup must be measured and reported. Frequency can be daily, weekly or monthly depending on the criticality and technical feasibility. Type of data backup can be full, differential and incremental, based on the project/function requirements. Data restoration must be based on the project requirements and technical feasibility.

7. Compliance

Data backups & restoration process must be audited as part of the internal audits, as per the audit calendar.

8. Exceptions(s)

Exceptions to this policy requires formal written approval from the Information Security Assurance Team.

9. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technological controls	8.13 Information backup Control Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Back up and restoration policy

Document Control

Owner:	CISO	Release ID:	BCRS-POL-048

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Introduction /Reason for Change	Approver	Change Description
0.1	09-Jan-2018	Roshni, Kamadev Pradhan	Gangadhar Aka, Joshy VM, Balakrishnan Nair, Vishwanath MS	Initial		Initial Draft
1.00	20-Jun-2018	Kamadev Pradhan		Approval for Baseline	Ganesh AJ	Baseline
1.1	13th Nov	Anitha Ravindran	Phani Krishna	Added requirements based on 27018		Added backup for data that has Personal Data
2.0	22 Nov	Anitha Ravindran	Phani Krishna			Baselined Version
2.1	12-May-20	Karthik N	Balu Nair	Review		Formatting changes
3.0	14-May-20	Karthik N	Phani Krishna	For Approval	Phani Krishna	Approved and Baselined
3.1	19-May-20	Karthik N	Srilakshmi	Review comments from DA		Changes made in section Measurement and reporting, compliance and roles and responsibilities.
4.0	19-May-20	Karthik N	Anitha Ravindran	For Approval	Phani Krishna	Approved and Baselined

4.1	01-Feb-21	Karthik N	Pranesh K and Siva Krishna	For Review		Updated the policy by adding cloud elements of backup.
5,0	01-Feb-21	Karthik N	Pranesh K and Siva Krishna	For Approval	Phani Krishna	Approved and Baselined
51	13-Oct-2021	Pranesh K	Pranesh K &Siva Krishna	For Review		Changes made in the section 2
6.0	02-Nov-2021		Pranesh & Siva	For Approval	Sivaramakrishnan N	Approved and Baselined
6.1	21-Dec-2021	Karthik N	Karthik N	For Review		No changes
7.0	13-Jan-2022	Karthik N	Sivaramakrishnan N	For Approval	Sivaramakrishnan N	Approved and Baselined
7.1	12-Mar-2022	Sanjana,	Karthik N	For review	Sivaramakrishnan N	The scope has been extended to products and services
8.0	18-Mar-2022	Sanjana	Karthik N	For Approval	Sivaramakrishnan N	Approved and baselined
8.1	06-April-2023	Krutideepta, Pallavi Chakrabarty	Karthik N	For Review	Srikanth M	New template change
9.0	12-May-2023	Krutideepta	Karthik N	For Approval	Srikanth M	Approved and baselined
9.1	19-Feb-2024	Beniyel S	Vijaya R	For Review		ISO Control Mapping has been added.
10.0	23-Feb-2024	Beniyel S	Vijaya R	For Review	Srikanth M	Approved and baselined

10.1	16-Apr-2025	Vijaya	Balu	For Review		Migrated to a new Template and yearly review
11.0	14-May-2025	Vijaya	Balu	For Approval	Srikanth M	Approved and baselined

Contact Information

Name

Email

Phone

infosec@trianz.com

Thank You