TRIANZ℠

Backup And Restoration 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 Backup and restoration process is to ensure backup of all required information and verification of backup at periodic intervals

2. Acronyms/Abbreviations

Acronym/Abbreviation	Expansion
CM tool	Configuration Management tool

3. Objective(s)

- To ensure timely availability of information assets so that business interruptions are minimized
- To control and optimize the information back up process

4. Scope

This procedure is applicable to all the information back up and restoration activities performed at Trianz

5. Roles and Responsibilities

Role	Responsibility	Internal/External
IS Manager	☒ Provides approval on any user request for issue of backup data and data restoration	Internal

Systems Administrator	• Implement backup and restoration activities as per process • Update relevant backup logs and restoration logs • Maintain and store backed up files as specified by process	Internal
Project Manager/ Delivery Manager	• Provides approval on any user request for backup data and data restoration • Initiates the Project Archival process	Internal
Users	☒ Request their manager for approval to back up important data on the File Server	Internal

6. Prerequisites

6.1 Resource

- Knowledge in Windows and other tools to Back up Applications
- Knowledge on Back up policies
- Knowledge on Back up devices

6.2 Training

- Awareness on Backup process
- Blue Book processes

7. Entry Criteria

- Scheduled backup
- Backup/ Restore is requested by a user

8. Inputs

- Schedule Backup

- Requested Backup/Restoration: Email from user requesting the backup, with an approval from manager

9. Process Description

- Backup copies of Information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific (information assets, software, and systems). policy on backup.

9.1 Back Up Tasks

- Server backups will be taken regularly as per the business requirements.
- Daily incremental backup will be taken from Monday to Saturday
- Daily snapshots with full backups will be taken on cloud infrastructure.
- Once the backup is taken and the log is updated, alert mail will be generated.

Refer Appendix A for Backup log format

9.2 Backup Scope

- Fileservers – users and project data
- All Production servers
- All Production Networking and Security Devices
- For Cloud Services, data backup is taken over cloud storage, ex: AWS Glacier/S3 or Azure Backup etc

9.3 User Requested Back Up

- User has to request for Backup data with approval of concerned PM, Based on the request, the backup is taken by the IS Team and IS

Manager should approve any user request for issue of backup data and data restoration

- All such cases will be maintained in Backup log

9.4 Backup of User Data

- Employees are responsible for uploading files that they wish to be backed up to the server (they need to place the files in their respective projects directory on file server)
- These project directories are backed up by the IS Team as defined above
- As an etiquette, unwanted / personal files are not to be placed on the server for backup, they will be deleted without intimation

9.5 Project End Backup and Archival

- On completion of a project or in the case of a project being aborted halfway, the Project Leader/PM initiates the Project Archival process. The Project Leader should complete the following before the actual Archival begins:
- All project related documents and code checked into the CM Tool of that project
- All other information related to the project, but that which cannot be added to the Configuration Management Tool should be stored in a shared folder. This will also be archived along with CM Tool database
- Project archrivals will be a part of monthly, and yearly backups and will be stored/archived in Cloud/Server
- CM of other project / A person who is familiar with configuration management process will perform configuration management audits
- A user can request for the restoration of a part or the whole of a backup unit
- Restore and ensure resilience of the data and provide access to the user

- All restorations are to be approved by email by the concerned manager with proper restoration details.
- The IS Team will make an entry in the backup log/restore log noting the request. After the restoration is complete, the IS Team will intimate the requestor.

9.6 Backup Verification

- Daily backup logs will be verified by IS team.
- An entry to the success of this operation is made in the backup log

9.7 Back-up Restoration

- Restoration shall also be performed based on project teams request.
- For all network and security devices which are on production environment restoration test shall be performed once in six months.

10. Output

Repository at cloud.

11. Exit Criteria

Back up / Restoration is complete as per plan

12. Measurement

- No of Successful Backups vs No of Backups taken
- No of Successful Restorations done vs No of successful Backups

13.Standards Addressed

ISO 9001:2015, ISO 27001:2022, ISO 27017:2015, ISO 27018:2019, ISO 27701:2019,ISO 20000-1:2018 Standards

14. ISO Control Mapping

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.	Backup and Restoration Procedure

Document Control

Owner:	CISO	**Release ID:**	BUR-PROC-0040

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			Baseline is approved by Zulfikar Deen.	Approved Baseline.
0.01	14- May 09	Bharateesh a B R			Risk Assessment and Risk Treatment Plan	Consolidated the procedure used for information back up and provided more clarity on frequency, type of back up
1.00	03-Jun-09	Balu Nair			Approval for Baseline	Baselined
1.01	13-May-10	Balu Nair			QMG review	Formatted the document Updated properties
2.00	19-May-10	Balu Nair			Request for baseline	Baselined

2.01	24-May-11	Srilakshmi			QMG Review	Modified release id in header and cover page to make consistency
3.00	24-May-11	Srilakshmi			Approval for Baseline	Baselined
3.01	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
4.00	3-Aug-11	Sudharsana			Request for baseline	Approved and Base lined
4.01	16-Nov-11	Gangadhar			Review by Gangadhar	Simplified the Process (modified Section 5.0 to section 5.5
5.00	21-Nov-11	Gangadhar			Request For approval	Base lined
6.00	29-Nov-11	Sudharsana			QMG Review	□ Standard document template is used Modified 5.1 section to

						have more clarity
7.00	08-Nov-12	Balu Nair			Standardization of Blue Book Process Assets	Modified the template format Changed the Logo
8.00	22-Jan-13	Srilakshmi			QMG Review	Modified Tile of the document in the cover page
9.00	07-May-14	Jyosthna			Internal Audit Cycle 04/2013	• Modified 5.4 section Naming convention for Backup Media • Referred Restore log in section 5.9 Modified Trianz Logo
9.01	14-Oct-16	Sriharsha			Addition of Cloud services as scope of Certification.	Backup scope modified to include Cloud services under the section 5.2

						Trianz Logo changed
10.0	07-Dec-16	Balu Nair			Approved by CISO	Approved
10.1	29-Apr-19	Balu Nair	Joshy VM			Information classification modified
11.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
11.1	11-May-20	Karthik N	Balu Nair		Review	Integrated with new template
12.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
12.1	28-May-20	Vijaya Rajeswari/ Pranesh Kulkarni	Gangadhar Aka, Balu Nair	Phani Krishna	Inputs from External Audit	• Sections “Storage and Location and Naming Conventions for Backup Media are removed • Tapes are removed as they are not currently used. • Restoration frequency is

						changed from monthly to Six months for Network/Security devices which includes Firewall.
						Standards addressed section is updated
13.0	3-Jun-20	Vijaya Rajeswari/ Pranesh Kulkarni	Balu Nair	Phani Krishna	For Approval	Approved and Baselined
13.1	1-Feb-21	Karthik N	Pranesh K and Siva Krishna		For Review	Updated the Policy by considering cloud aspects of backup. Updated the information classification.
14.0	1-Feb-21	Karthik N	Pranesh K and Siva Krishna	Phani Krishna	For Approval	Approved and Baselined,
14.1	02-Novt-2021	Karthik N	Pranesh K/Siva Krishna		For Review	Section 9.2 – Edited: Backup for Networking and Security Devices

15.0	02-Nov-21	Karthik N	Pranesh K/Siva Krishna	Sivaramakri s hnan N	For Approval	Approved and Baselined
15.0	21-12-2021	Karthik N	Karthik N		For Review	No Changes
15.1	14-Mar-2022	Kruti	Karthik N		For Review	The scope has been extended to products and services
16.0	18-March-2022	Kruti	Siva N	Siva N	For Approval	Approved and baselined
16.1	06-April-2023	Kruti, Rama Madhavan	Karthik N		For Review	New measurements have been added. New template change
17.0	09-May-2023	Kruti	Karthik N	Srikanth M	For Approval	Approved and baselined
17.1	15-Feb-2024	Beniyel S, Aishee G	Balu Nair, Vijaya R			Migrated from standard ISO 27001:2013 to ISO 27001:2022 Added ISO Control mapping in Section 13.1
18.0	23-Feb-2024	Beniyel S, Aishee G	Balu Nair, Vijaya R	Srikanth M	For Approval	Approved and Baselined

18.1	30-Apr-25	Kruti	Balu Nair, Vijaya R		For Yearly Review	Migrated to a new Template.
19.0	14-May-25	Kruti	Balu Nair, Vijaya R	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com