TRIANZ℠

Business Continuity 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

This policy is defined to have an organization-wide Business Continuity Management Systems (BCMS) Program (the "BCMS Program") aligned to the requirements of ISO 22301: 2012 International Standard for Business Continuity Management systems, ISO 20000-1:2018 IT Service management and ISO 27001:2022 Information Security Management Systems and minimize risk to Trianz operations, resources, reputation, and shareholder value.

2. Objective

1. To focus proactively on defining processes and procedures that enable essential ICT functions to continue during and after a significant event. Also effectively respond to emergency events which have potential to affect the company.
2. To Prepare for and respond to all the unforeseen events, minimize the impact of the interruption to mission-critical services and protect the health and safety of Trianz employees and subcontractors, working at Trianz facilities.
3. To establish an Emergency Response and Crisis Management structure across all locations, facilitate local resumption of activities and deployment of supporting or recovery resources.

3. Scope

The scope of this policy is applicable to all People (Trianz employees, contractors, and vendors), Trianz Process, and Information Technology (IT) resources owned, managed, or operated by Trianz across all geographies.

4. Policy Statements

- Trianz shall establish a BCMS framework for the company including its subsidiary operations and operating units to guide its business continuity efforts.

- Trianz shall place high importance on the safety of all its employees and subcontractors working at Trianz facilities.
- Each Trianz location shall, under guidance from top management, implement and document a Business Continuity Plan driven by the crisis management team of the location.
- BC plan establishes a crisis management structure across all Trianz locations to facilitate local resumption of activities and deployment of supporting or recovery resources.
- Trianz shall identify legal, regulatory, contractual commitments related to Business Continuity requirements and ensure compliance against each requirement.
- All Trianz facilities shall undergo a risk assessment to assess the impact of potential risks/disruption scenarios on its business functions, resources, and infrastructure and have in place appropriate procedures to ensure necessary resources are available to withstand the impact of the risk/disruption.
- Trianz shall perform a detailed Business Impact Analysis for all critical business functions, resources, products, infrastructure, ICT functions which, if disrupted, would have a material impact on business operations and reputation of the company.
- Trianz shall establish granular ICT continuity objectives and requirements derived from comprehensive Business Impact Analysis (BIA). These objectives shall ensure the recovery of critical IT systems within defined Recovery Time Objectives (RTOs) through effective redundancy solutions, robust backup procedures, and a designated Disaster Recovery (DR) site."
- Trianz shall, at least on an annual basis, test the Business Continuity Plan(s) including suppliers of critical goods or services (if any) and make modifications where necessary to take account of the test results.
- Trianz shall establish Disaster Recovery (DR) Planning - a key component of BCMS that will focus on the process of restoring critical information systems.
- All associates and other stakeholders shall be made aware of the BC Plans applicable to their sites, departments and their roles following an invocation of the BC Plan.
- This Business Continuity Policy along with the associated Framework and BCMS Program elements shall be reviewed semi-annually or against significant changes to the company’s operating environment.
- Trianz account level BCP coverage shall be only for key strategic accounts and location specific BCP shall cover all Trianz locations.

- Trianz shall conduct BCP tests i.e., Call tree bi-annually and tabletop simulation at least once in a year(depending on the client requirements) for the respective critical strategic projects (and based on the MSA/SOW applicability), products and network level ISP tests for location specific.

5. Roles & Responsibilities

Trianz Business Continuity assurance is responsible for organization wide guidance, policy, and oversight of the BCM program.

1. Trianz Operating Units and locations across geographies are responsible for developing, implementing, maintaining and testing their BCM Program.
2. Each Trianz location will document the Business Continuity Plan in accordance with the approved standardized template provided by the Business Continuity assurance.
3. Each Trianz location shall have a Business continuity Plan to account for life and safety issues including evacuation and shelter-in-place (if applicable) and will document business activities conducted at each location. Responsibility for completing these plans belongs to the Business continuity assurance team.
4. Any client-related BCP/DR requirements shall be governed by the respective client contracts.
5. For account level, product level and project specific BCP, respective delivery manager/project manager shall be responsible for creating, managing, maintaining the BCP program along with the help of delivery assurance. InfoSec BCP SPOC shall assist the delivery in case of any support required in creating the BCP.
6. The Business continuity assurance team is responsible for ensuring that this policy document is reviewed at least annually.

6. Applicable standards

ISO 27001 and ISO 22301	
Clause	**Description**
17 (ISMS)	Information security aspects of business continuity management

7. Reference Policies & Procedures

Document Name
Business Continuity Procedure

8. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Organizational Controls	5.30 ICT readiness for business continuity ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Business Continuity Policy
Technological Controls	8.14 Redundancy of information processing facilities	

9. Exceptions(s)

There is no exception to this policy.

Document Control

Owner:	CISO	**Release ID:**	BCP-POL-051

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	25-Feb-19	Karthik Narasimha	Joshy VM/Karthi k N/Balu Nair		Initial Draft	None
0.2	15-Mar-19	Karthik Narasimha	Phani Krishna		Policy statement	Updated policy statement
1.0	14-May-19	Karthik Narasimha		Ganesh Arunachala	Approved for Baseline	Baselined
1.1	11-May-20	Karthik Narasimha	Balu Nair		Review	Format change

2.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
2.1	13-Jan-2021	Karthik N	Phani Krishna	Phani Krishna	Review	Updated the requirements as per ISO 20000-1:2018 Updated the information classification
3.0	13-Jan-2021	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved for Baselined
3.1	02-June-2021	Karthik N	Karthik N	Phani Krishna	For Review	Updated the Scope and incorporated few format changes. Moved section 5 and 6 to the procedure document.

4.0	02-June-2021	Karthik N	Karthik N	Phani Krishna	For Approval	Approved and baselined
4.1	30-July-2021	Karthik N	Balu N	Phani Krishna	For Review	Changes incorporated as per feedback from Phani.
5.0	30-July-2021	Karthik N	Balu N	Phani Krishna	For Approval	Approved and baselined
5.0	23-Dec-2021	Karthik N	Karthik N		Annual Review	No changes
5.1	13-Mar-2022	Sanjana	Karthik N		For review	The scope has been extended to products and services
6.0	17-Mar-2022	Sanjana	Karthik N	Siva N	For Approval	Approved and baselined
6.1	31-Jan-23	Sanjana	Beniyel S		For review	Extended scope to all Trianz locations, Review period changed from semiannual

						ly to annually.
7.0	31-Jan-23	Sanjana		Karthik N	For approval	Approved and baselined
7.1	22-Feb-23	Kruti, Shalini Kumari	Karthik N		For Review	Call tree test frequency added to bi annually. New template change. Editorial change.
8.0	12-May-23	Kruti	Karthik N	Srikanth M	For Approval	Approved and baselined
8.1	15-Feb-24	Kruti	Beniyel S & Vijaya R		For Review	1. Updated the objective with as per ISO 27001: 2022

						Standard. 2. ISO Mappings has been added.
9.0	23-Feb-24	Kruti	Beniyel S & Vijaya R	Srikanth M	For Approval	Approved and Baselined.
9.1	5-May-25	Vijaya	Balu		For review	Migrated to a new template and yearly Review
10.0	14-May-25	Vijaya	Balu	Srikanth M	For Approval	Approved and Baselined.

Contact Information

Name

Email

Phone

infosec@trianz.com

Thank You