TRIANZ℠

SYSTEM AND SOFTWARE CHANGE MANAGEMENT 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

The purpose of this policy is to establish management direction and high-level objectives for change management and also to ensure controlling the changes to the organization, business processes, information processing facilities and systems that affect information security.

Various controls are categorized to mitigate the risk as follows:

- Information being corrupted and/or destroyed;
- Computer performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Exposure to reputational risk
- Any changes that are being done in cloud service are not affecting the cloud services.

2. Scope

This policy applies to all parties operating within the Trianz's network environment or utilizing Information Resources, Cloud service provisioning and Cloud service consumption. It covers the data networks, LAN servers and personal computers (stand- alone or network-enabled), located at Trianz offices and company production related locations, where these systems are under the jurisdiction and/or ownership of Trianz including cloud environment, and any personal computers, laptops, mobile device and or servers authorized to access the Trianz's data networks and Cloud Networks. None of the employees is exempted from this policy.

3. Policy

Changes to information resources shall be managed and executed according to a formal change control process. The control process shall ensure that the changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

4.Roles & Responsibilities

Sl. No	Item	Roles	Responsibility
1	Change Manageme nt	Cloud Service Provider	Shall have the responsibility and authority tocause this policy to be implemented and maintained **As a Cloud Service Provider**: Shall provide the following: ➢ Categories of changes ➢ Planned Date and Time of Changes ➢ Technical description of changes to the Cloud Service and underlying systems Notification of Start and Completion of the Changes ➢ In case the service is dependent on Peer Cloud Service Provider, ensure that change is informed to cloud service customer
2	Change Manageme nt	Cloud Service Customer	**As a Cloud Service Customer**: Shall take into consideration of any changesthat would impact any of the services provided by the Cloud Provider
3	Audit & Compliance	InfoSec Assurance	Annual Policy & Compliance Review

Roles & Responsibilities for ISO 20000-1:2018 (Service Management System: Please refer to System and Software Change Management Procedure).

5. Operational Requirements

5.1 Change Documentation

All change requests shall be logged whether approved or rejected on a standardized and central system. The approval of all change requests and the results thereof shall be documented. A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorization and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorized personnel. All the change items shall be included in either MSA or SLA.

5.2 Change Classification

All change requests shall be prioritized in terms of benefits, urgency, effort required and potential impact on operations.

5.3 Change Testing

Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

5.4 Changes affecting SLA’s

The impact of change on existing SLA’s shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

5.5 Approval

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorized user, the impact assessment was performed and proposed changes were tested. All major changes shall be informed to information security and data privacy assurance team and seek approvals if necessary.

5.6 Communicating changes

All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

5.7 Change Implementation

Implementation shall only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

5.8 Roll-Back Procedure

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. (*Added for clarification*)

5.9 Emergency Changes

Specific procedures to ensure the proper control, authorization, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

5.10 Verification of Changes

All changes shall be verified during and after implementation. On unsuccessful implementation, fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes, as the case may be.

5.11 Communication of Changes

All changes are communicated to all stakeholders that information security requirements have been met.

6. Monitoring

Reporting metrics, documentation templates and change implementation reports are described in the approved and published Trianz Change Management Procedure. Change implementation reports should be generated and maintained by the IT team, which will be used to summarize the outcome of the changes implemented. These reports shall be made available to Information Security and Internal Audit upon request.

7. Compliance

Any person, subject to this policy, who fails to comply with the provisions as set out above or any amendment thereto, shall be subjected to appropriate disciplinary or legal action in accordance with the Trianz Disciplinary Code and Procedures. Company Information Security policies, standards, procedures and guidelines shall comply with legal, regulatory and statutory requirements.

All changes shall adhere to the policy to ensure the reliability of the systems and applications.

8. Exceptions(s)

Exceptions to the System and Software change management policy shall follow the Exception handling policy.

9. ISO Control Mapping(s)

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological	8.32 Change management Control Changes to information processing facilities and information systems shall be subject to change management procedures.	System and Software Change Management Policy

Document Control

Owner:	CISO	**Release ID:**	SSCM-POL-0044

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Introduction /Reason for Change	Change Description
0.1	13-Oct-2017	Roshni Madhusoodan	Shishir Kumar Singh	-	Creation of Change Management Policy	Initial Draft
1.00	14-May-18	Kamadev Pradhan	Balu Nair	Ganesh A	Approved by Ganesh	Baselined
1.01	29-Apr-19	Balu Nair	Joshy VM	-		• Trianz logo is replacedwith new logo • Information classification modified
2.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	• Baselined

3.0	22-Nov-2019	Vijaya Rajeswari V	Phani Krishna	Vivek Sambasivam	Updated the policy to align to Standards – ISO 27017	- Updated the Purpose, Roles & Responsibilities and Section 5-Operational Procedures
3.1	12-May-20	Balu Nair	Phani Krishna			- Migrated to the new template
4.0	14-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
4.1	29-Jan-21	Vijaya Rajeswari	Phani Krishna		For Review	Policy is aligned to ISO 20000-1:2018 Standard,
						Information classification updated
5.0	29-Jan-21	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
5.1	21-Dec-21	Vijaya Rajeswari	Karthik N		For Review	Formatting changes

6.0	13-Jan-22	Vijaya Rajeswari	Karthik N	Sivaramakrishnan N	For Approval	Approved and Baselined
7.0	11-Apr-23	Vijaya Rajeswari, Pallavi Chakrabarty	Karthik N		For Review	Updated section 5.5 (Approval) New template change
8.0	12-May-23	Vijaya Rajeswari	Karthik N	Srikanth M	For Approval	Approved and Baselined
8.1	11-Feb-24	Shalini	Vijaya	Srikanth M	For Review	Mapped with new ISO 27001 2022 controls
9.0	23-Feb-24	Shalini	Vijaya	Srikanth M	For Approval	Approved and Baselined
9.1	28-May-25	Kruti	Vijaya		For Review	Migrated to new template
10.0	29-May-25	Kruti	Vijaya	Srikanth M	For Approval	Approved and Baselined

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com