



ACCESS CONTROL 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

<input type="checkbox"/>	Public
<input checked="" type="checkbox"/>	Internal
<input type="checkbox"/>	Confidential
<input type="checkbox"/>	Restricted

Table of Contents

1. PURPOSE	5
2. OBJECTIVES	5
3. SCOPE	5
4. POLICY STATEMENT	5
4.1 Account Management	5
4.2 Access Enforcement	5
4.3 Information Flow Enforcement	6
4.4 Segregation of Duties	6
4.5 Least Privilege	6
4.6 System Use Notification	6
4.7 Concurrent Session Control	6
4.8 Session Lock	6
4.9 Remote Access	7
4.10 Wireless Access	7
4.11 Access Control for Mobile Devices	7
4.12 Use of External Information Systems	7
4.13 Use of External Information Systems	7
4.14 Privilege Access Management	7
4.15 Management of secret authentication information of users	7
4.16 Shared responsibility matrix	8
4.17 Information access restriction	8
4.18 Password Management	8
4.19 Access Revocation	8
5. ROLES & RESPONSIBILITIES	8
6. APPLICABLE STANDARDS	8
7. REFERENCE POLICIES & PROCEDURES	9
8. IMPLEMENTATION PROCEDURES	9

9. EXCEPTIONS(S)	9
10. ISO CONTROL MAPPING(S)	10

1. Purpose

The purpose of this policy is to establish the access control for user account management, access control enforcement, access monitoring, separation of duties, and remote access management through the establishment of an Access Control program. The program helps Trianz implement best practices about logical security, account management, remote access and mitigate associated risks.

2. Objectives

The objective of this policy is to minimize the security risk of unauthorized access to physical and logical systems operated by Trianz.

3. Scope

The scope of this policy is applicable to all Trianz managed business systems, Trianz provided Client Services & Trianz developed products. The scope includes Information Technology (IT) resources, Cloud services owned or managed by Trianz.

4. Policy Statement

The following subsections outline the Access Control policy statements that constitute Trianz policy. Entire Trianz business system, Delivery teams & Products are bound to adhere to this policy.

4.1 Account Management

- Identification of account types must be done (i.e., individual, group, system, application, guest /anonymous, and temporary).
- Providing access to the system must be based on (1) valid access authorization, (2) intended system usage, and (3) other attributes as required by the organization or associated missions / business functions.
- Reviewing accounts must be done on a periodic basis.

4.2 Access Enforcement

- All Trianz managed systems must enforce approved authorizations for logical access to the system in accordance with applicable policy.

4.3 Information Flow Enforcement

- All Trianz managed systems must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems.

4.4 Segregation of Duties

- Segregation duties of individuals must be done as necessary to prevent malicious activity without collusion.
- Segregation of duties must be documented.
- Implementation of segregation of duties should be done through assigned information asset access authorizations.

4.5 Least Privilege

- All Trianz managed systems and applications must employ the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

4.6 System Use Notification

- An approved system uses notification message or banner is to be displayed before granting access to the system that provides privacy and security notices consistent with regulations, standards, and policies.

4.7 Concurrent Session Control

- All Trianz managed systems must limit the number of concurrent sessions for each system account to the minimum needed for information assets.

4.8 Session Lock

- Trianz managed systems must prevent further access to the information assets by enabling session lock.

4.9 Remote Access

- All Privileged users must connect to servers, devices, applications via Arcon privileged access management (PAM) console.

4.10 Wireless Access

- It is to be assured that Wireless Access is secure and must be monitored on a regular basis.

4.11 Access Control for Mobile Devices

- Access control for mobile devices must be monitored and in case of any vulnerability must be fixed immediately.

4.12 Use of External Information Systems

- Use of External Information Systems must be thoroughly verified before use.

4.13 Use of External Information Systems

- Designated individuals will be authorized to post information into an organizational information system that is publicly accessible.

4.14 Privilege Access Management

- All privileged users must login to their servers, network devices, applications, web consoles to perform their duties from the Arcon PAM utility and no direct access like RDP/MSTSC are allowed.
- Privileged access shall be valid for a limited time period only.
- Privileged access roles and access rights shall be implemented and consistently followed.

4.15 Management of secret authentication information of users

- Allocation and use of secret authentication information shall be controlled.

4.16 Shared responsibility matrix

- Shared responsibility matrix should have explicit mention of access control responsibilities.
- Access control responsibilities must be reviewed and approved periodically.

4.17 Information access restriction

- Access to the information shall be restricted and controlled.

4.18 Password Management

- Password Management must be done as per the “Password Security Policy.”

4.19 Access Revocation

- Logical access to all associates shall be revoked upon termination or internal transfer.

5. Roles & Responsibilities

Roles	Responsibilities	Internal/External
All Associates/Users	Adhere to the access control matrix.	Internal
IS Operations Team/Project Manager	Validate the access control for the users in the system based on the request.	Internal
InfoSec & Compliance Team	Validate the exceptions from the users.	Internal

6. Applicable standards

- ISO 27001:2013

- ISO 27701:2019

7. Reference Policies & Procedures

- Physical Access Control and Environmental Security Policy
- Policy on the Use of Cryptographic Controls
- User responsibilities Procedure

8. Implementation Procedures

- Access Control Procedure
- Information Security Code of Conduct
- Physical Access Control and Environmental Security Procedure

9. Exceptions(s)

- All exceptions to this policy shall follow "Exception handling Policy.

10. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Organizational Control	5.15 Access control Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Access Control Policy
Organizational Control	5.16 Identity management Control The full life cycle of identities shall be managed	Access Control Policy
Organizational Control	5.18 Access rights Control Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Access Control Policy
Technological Control	8.4 Access to source code Control Read and write access to source code, development tools and software libraries shall be appropriately managed.	Access Control Policy

Document Control

Owner:	CISO	Release ID:	ACP-POL-0027
---------------	------	--------------------	--------------

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.01	28-Apr-15	Sudharsana.cv			Initial Draft	None
1.00	28-Apr-15	Sudharsana.cv			Reviewed and approved	Baselined
1.01	25-Jan-16	Sumanta Bhattacharya and Balu Nair			Client Audit and alignment with shared assessment checklist.	Added References
2.00	08-Feb-16	Balu Nair			Approved by Mahesh (CISO)	Baselined
2.01	24-10-2016	Sriharsha			Cloud process alignment with Trianz	Inclusion of Cloud specific content and updated reference Changed Trianz Logo
3.00	07-Dec-16	Balu Nair			Approved by CISO	Baselined
3.01	29-Apr-19		Joshy VM			Information classification & Trianz Log are modified.

4.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
4.2	24-Oct-19	Karthik	Phani Krishna		Review	Included cloud content. Changes implemented as suggested by Phani
5.0	20-Nov-19	Balu Nair		Vivek Sambasivam	Approved for Release to Blue Book	Baselined
5.1	11-May-20	Karthik N	Balu Nair		For Review	Formatting changes Integrated with new template
6.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
6.1	27-July-2020	Karthik N	Vijaya		For Review	Updated the sections in the policy statement
7.0	30-Jul-2020	Karthik N	Vijaya	Phani Krishna	For Approval	Approve an Baselined
7.1	13-Jan-2021	Karthik N	Phani Krishna		For Review	Updated the remote access session and information classification.
8.0	13-Jan-2021	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and baselined.
8.1	10-Jun-21	Balu Nair	Phani & Vijaya	Phani Krishna	Yearly Review	Completely migrated to the new template and revamped
9.0	30-Jul-21	Balu Nair	Phani Krishna	Phani Krishna	Approved for Baseline	Baselined
9.0	04-Jan-2022	Sanjana	Balu Nair	Siva N	For Review	Reviewed and no changes
9.1	10-Mar-2022	Sanjana	Balu Nair	Siva N	For Review	Updated with access revocation

10.0	20-Mar-2022	Sanjana	Balu Nair	Siva N	Approved for Baseline	Baselined
10.1	10-Mar-2023	Shalini, Pallavi Chakrabarty	Balu Nair	Srikanth	For Review	Reviewed and Arcon tool name is removed New template change
11.0	12-May-2023	Shalini	Balu Nair	Srikanth	For Approval	Approved and baselined
11.1		Aishee	Vijaya V Balu Nair		For Review	Migrated from standard ISO 27001:2013 to ISO 27001:2022
12.0	23-Feb-2024	Aishee	Vijaya V Balu Nair	Srikanth	For Approval	Approved and baselined
12.1	30-Apr-2025	Krutideepta Barik	Vijaya R		For Yearly Review	Migrated to a new Template.
13.0	14-May-2025	Krutideepta Barik	Vijaya R	Srikanth	For Approval	Approved and baselined



Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com



The content in this document is copyrighted; any unauthorized use – in part or full – may violate the copyright, trademark, and other laws. This document may not be modified, reproduced, or publicly displayed, performed, or distributed, or used for any public or commercial purposes. The Trianz name and its products are subject to trademark and copyright protections, regardless of how and where referenced.