



ACCESS CONTROL 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

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

Table of Contents

1. INTRODUCTION	5
2. OBJECTIVES	5
3. SCOPE	5
4. ENTRY CRITERIA	5
5. INPUTS	5
6. PROCESS DESCRIPTION (PROCEDURE)	5
6.1 Account Management	6
6.2 Access Enforcement	6
6.3 Information Flow Enforcement	6
6.4 Segregation of Duties	7
6.5 Least Privilege	7
6.6 System Use Notification	7
6.7 Concurrent Session Control	7
6.8 Session Lock	7
6.9 Remote Access	8
6.10 Wireless Access	8
6.11 Access Control for Mobile Devices	8
6.12 Use of External Information Systems	9
6.13 Publicly Accessible Content	9
6.14 Privilege Access Management	10
6.15 Management of secret authentication information of users	10
6.16 Shared responsibility matrix	11
6.17 Information Access restriction	11
6.18 Use of Privileged utility programs.	12
6.19 Password Management	12
6.20 Access Revocation	12
7. EXIT CRITERIA AND OUTPUT	12

8. ROLES AND RESPONSIBILITIES	12
9. PREREQUISITES	13
9.1 Resource	13
9.2 Training	13
9.3 Reference Policy, Process, Procedure, Templates, Checklist	13
10. ACRONYMS/ABBREVIATIONS	13
11. MEASUREMENT	14
12. STANDARDS ADDRESSED	14
13. ISO CONTROL MAPPING(S)	14

1. Introduction

- Access control is a fundamental component of information security that dictates only authorized users to allow access to use company's information and resources.
- Access control system provide quick, convenient access to those persons who are authorized, while at the same time, restricting access to unauthorized people.

2. Objectives

- The objective of this procedure is to establish controls to ensure authorized user access and prevent unauthorized access to Information systems

3. Scope

- This procedure is applicable to all Trianz Business systems, Trianz Products & Trianz managed services including Cloud, networks and networked services established and managed by Trianz.

4. Entry Criteria

- New user registration request received with necessary approvals
- Users/Associates are On-Boarded or User/Associates are ready to be off-boarded (Resigned Users)
- Systems are deployed

5. Inputs

- User access details

6. Process Description (Procedure)

- All Trianz managed systems must develop, adopt or adhere to a formal, documented access control procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

6.1 Account Management

- Identify account types (i.e., individual, group, system, application, guest/anonymous, and temporary).
- Establish conditions for group membership.
- Identify authorized users of the information asset and specifying access privileges.
- Require appropriate approvals for requests to establish accounts.
- Establish, activate, modify, disable, and remove user accounts.
- Specifically authorize and monitor the use of guest/anonymous and temporary accounts.
- Notify account managers when temporary accounts are no longer required and when information asset users are terminated transferred, or information assets usage or need-to-know/need-to-share changes.
- Deactivate temporary accounts that are no longer required and accounts of terminated or transferred users.
- Grant access to the system based on (1) valid access authorization, (2) intended system usage, and (3) other attributes as required by the organization or associated missions / business functions.
- Review accounts on a periodic basis or at least bi-annually.

6.2 Access Enforcement

- Enforce approved authorizations for both logical & Physical access to the system in all Trianz business systems (including Network protection)
- Identify secure areas and enforced with secure access

6.3 Information Flow Enforcement

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

6.4 Segregation of Duties

- Segregation duties of individuals as necessary, to prevent malicious activity without collusion.
- Implement Segregation of duties through assigned information asset access authorizations
- Ensure Segregation of Development environment, Production environment, testing environment basis of the user's roles
- Ensure Segregation of duties are documented

6.5 Least Privilege

- Ensure only authorized people are using all Trianz business systems, applications
- Ensure user access control matrix is reviewed on quarterly basis by the approved stakeholders.

6.6 System Use Notification

- Ensure approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with regulations, standards, and policies.
- Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information asset.

6.7 Concurrent Session Control

- Ensure limitation of number of concurrent sessions for each system account to the minimum needed for information assets by all the Trianz business systems.

6.8 Session Lock

- All Trianz managed systems shall be prevented further access to the information asset by initiating a session lock after 300 seconds of inactivity.

- In addition, Trianz managed systems must retain the session lock until the user reestablishes access using established identification and authentication procedures

6.9 Remote Access

- Ensure Privileged users shall Connect to servers, devices, applications or similar privileged access management (PAM) console.
- Document allowed methods of remote access to the information assets through implemented SSL VPN.
- Establish usage restrictions and implementation guidance for each allowed remote access method.
- Monitor for unauthorized remote access to the information asset through Forti Analyser / MDR (Managed Detection & Response)
- Authorize remote access to the information asset prior to connection through Trianz LDAP Server
- Enforce requirements for remote connections to the information asset.
- Ensure Cloud infrastructure is accessed over an encrypted secure channel.
- All remote users must follow the remote working guidelines as defined in the blue book.
- Ensure client's Cloud infrastructure is accessed over an encrypted secure channel, with prior authorization from respective Service delivery manager.

6.10 Wireless Access

- Establish usage restrictions and implementation guidance wireless access.
- Monitor for unauthorized wireless access to the information asset.
- Authorize wireless access to the information asset prior to connection.
- Enforce requirements for wireless connections for the information asset.

6.11 Access Control for Mobile Devices

- Establish usage restrictions and implementation guidance for organization-controlled mobile devices.

- Authorize connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information assets.
- Monitor for unauthorized connections of mobile devices to organizational information assets.
- Enforce requirements for the connection of mobile devices to organizational information assets.
- Disable information asset functionality that provides the capability for automatic execution of code on mobile devices without user direction.
- Issue specially configured mobile devices to individuals traveling to locations (international locations which are considered sensitive by the Department of State) that the organization deems to be of significant risk in accordance with organizational policies and procedures.

6.12 Use of External Information Systems

- All Trianz managed systems must establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information assets, allowing authorized individuals to:
 - Access the information asset from the external information systems.
 - Process, store, and/or transmit organization-controlled information using the external information systems.
 - Maintain Non-Disclosure and Confidentiality agreements with Cloud Service Providers, before hosting on public cloud.

6.13 Publicly Accessible Content

- Designate individuals authorized to post information onto an organizational information system that is publicly accessible.
- Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
- Review the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system.

- Review the content on the publicly accessible organizational information system for nonpublic information.
- Removes nonpublic information from the publicly accessible organizational information system, if discovered.

6.14 Privilege Access Management

- Ensure all the privileged users are login to their servers, network devices, applications, web consoles to perform their duties from the implemented PAM utility only.
- Users may request privileged access from IS team/PAM Admin and IS team need to ensure they provide appropriate access to PAM portal to the user with proper approvals. PAM admin will create the privilege account based on the approval.
- Privileged access should be valid for specified amount of time only.
- Establish system in place for monitoring privileged activity.

6.15 Management of secret authentication information of users

- Ensure allocation and use of Secret authentication information shall be controlled
- The cloud service customer will use the authentication techniques (Multi factor authentication) for authenticating the cloud service administrators of the cloud service customers to the administrative capabilities of a cloud service according to the identified risks.
- Cloud service provider should provide the authentication techniques (Multi factor authentication) for authenticating the cloud service administrators of the cloud service customers to the administrative capabilities of a cloud service, according to the identified risks
- Secret authentication information to remote users shall be distributed through SMS.
- In case of change or termination of the IT administrator, the Server and confidential passwords will be still maintained by PAM tool in encrypted format and it can be obtained using break glass tool

6.16 Shared responsibility matrix

- All cloud service provisioning and consumptions should have shared responsibility clearly defined and documented and agreed among all the cloud service participants.
- Ensure responsibility matrix should have explicit mention of access control responsibilities and make sure that the access control responsibilities are reviewed on periodic basis.

6.17 Information Access restriction

- Access to information and application system functions will be restricted in accordance with the access control policy.
- Restrictions to access will be based on individual business application requirements and in accordance with the defined access control policy.
- Cloud related information with respect to the consumer and provider will be restricted in accordance with the defined access control policy.
- Users with privileged access have a responsibility to protect the CIA of any information that they come across is being violated while performing their duties.
- Users with privileged access are responsible for complying with all applicable policies, and procedures.
- PAM Admin from IS team will maintain the master list of privileged user account list.
- Making additions, or deletions of privilege user accounts requires prior approval from the PAM admin.
- Access to mail server is restricted to IT System Administrator and above.
- Access to Domain Controllers is restricted to IT System Administrator and above
- Application Servers access is restricted to IT System Administrator and above.
- Default read only access to removable devices is given users who are managers and above. Other users below managers shall be provided access based on the approval from CIO/ CISO
- Print Servers access is restricted to IS System Administrator and above.

6.18 Use of Privileged utility programs.

- The use of utility programs that might be capable of overriding system and application controls are restricted and tightly controlled.
- Where the use of utility programs are permitted the cloud service customer will identify the utility programs to be used in its cloud environment and ensure that they do not interfere with the controls of the cloud service.
- As a cloud service provider, any use of utility programs that are capable of bypassing normal operating or security procedures are strictly limited to authorized personnel.

6.19 Password Management

- Refer to the “Password Security Policy”

6.20 Access Revocation

- The access rights of all users to information and Trainz systems shall be removed upon termination of their employment, contract or in case of Internal Transfer

7. Exit Criteria and Output

- Access given to the all Authorized users.
- Filled User Access matrix for projects and Functions is available

8. Roles and Responsibilities

Roles	Responsibilities	Internal/External
All Associates/Users	Review the Access control Matrix as per the procedure	Internal
IS Operations Team/Project/Product Cloud management team	Ensure only Authorized people access the Trianz managed systems	Internal

	Cross check the Access to the Trianz managed System based on ACM.	
Project/ Product manager	Ensure the principles of least privilege and separation of duties are followed.	Internal
InfoSec & Data privacy assurance Team	Review and approve the exceptions based on the business criticality.	Internal

9. Prerequisites

9.1 Resource

Access control matrix tool

9.2 Training

Awareness training on access control matrix

9.3 Reference Policy, Process, Procedure, Templates, Checklist

Document Name
Access control Policy
Access control matrix template

10. Acronyms/Abbreviations

Acronym/Abbreviation	Expansion
PAM	Privilege Access Management
ACM	Access Control Matrix
SSL VPN	Secure Sockets Layer Virtual Private Network
MDR	Managed Detection & Response
LDAP	Lightweight Directory Access Protocol
RDP/MSTSC	Remote Desktop Protocol/Microsoft Terminal Services Client
SMS	Short Message Service
CIA	Confidentiality, Integrity and Availability
CIO/CISO	Chief Security Officer/Chief Information Security Officer

11. Measurement

Refer to ICMM

12. Standards Addressed

ISO 9001:2015, ISO 27001:2013, ISO 27701:2019

13. 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 Procedure
Technological	8.4 Access to source code	

Document Control

Owner:	CISO	Release ID:	UAMR-PROC-0056
---------------	------	--------------------	----------------

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	–	–	Initial draft	None
0.01	26-Feb-07	Jyotessh G Nair	–	–	Review	Review feedback incorporated
1.00	26-Feb-07	Jyotessh G Nair	–	–	Baseline is approved by Zulfikar Deen.	Approved Baseline.
1.01	12-May 09	Bharateesh B R	–	–	Risk Assessment and Risk Treatment Plan	Consolidated the controls related to access control
2.00	04-Jun-09	Balu Nair	–	–	Approval for Baseline	Baselined
2.01	13-May-10	Balu Nair	–	–	QMG review	Formatted entire document
3.00	19-May-10	Balu Nair	–	–	Request for baseline	Baselined
3.01	24-May-11	Srilakshmi	–	–	QMG Review	Modified release id in header and

						cover page to make consistency
4.00	24-May-11	Srilakshmi	–	–	Approval Refer Baseline	Baselined
4.01	3-Aug-11	Sudharsana	–	–	QMG review	<ul style="list-style-type: none"> Replace Owner with Management Representative in place of CIO In Document Classification Scheme, "Retention period is 3 Years" row is removed
5.00	3-Aug-11	Sudharsana	–	–	Request for baseline	Approved and Baselined
6.00	22-Aug-12	Sriramya	–	–	Acceliant External Audit, 27-July-12 to 28-July-12 by Dr. Grover - Observation 6.3 (i)	Section 4.3.4 – new section added to included Password Complexity
7.00	14-May-15	Sudharsana	–	–	As per ISO 27001:2013	Added Management of secret authentication information of users section

7.01	27-Apr-17	Kamade v P	–	–	Internal Audit feedback	Modified Privilege Access Management section 4.4
8.00	28-apr-17	Kamade v P	–	–	Reviewed and Baselined	Approved by Ganesh Arunachala
9.00	23-Jun-18	Kamade v Pradhan	Balakrishnan Nair	Ganesh Arunachala	Reviewed the documents	No changes done in the Document
9.01	29-Apr-19	Balu Nair	Joshy VM			<ul style="list-style-type: none"> Information classification modified Trianz logo modified
10.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
10.1		Karthik N	Phani Krishna			Changes implemented post review from Phani
11.0	20-Nov-19	Balu Nair		Vivek Sambasivam	Approved for Release to Blue Book	Baselined
11.1	11-May-20	Karthik N	Balu Nair		Review	<ul style="list-style-type: none"> Roles modified with CIO/CISO Integrated with new template
12.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined

12.1	20-Jan-21	Karthik N	Siva Krishna		For Review	<ul style="list-style-type: none"> Modified the procedure as per Integration. Updated the information classification
13.0	20-Jan-21	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
13.1	21-July-21	Balu Nair	Phani Krishna		Yearly Review	Completely migrated to the new template and revamped
14.0	30-Jul-21	Balu Nair	Phani	Phani	Approved for Baseline	Baselined
14.0	04-Jan-22	Sanjana	Balu Nair	Siva N	For review	Reviewed and no changes in the document
14.1	11-Mar-22	Sanjana	Balu Nair	Siva N	For review	Updated roles and responsibility
15.0	21-Mar-22	Sanjana	Balu Nair	Siva N	For Approval	Approved for Baseline
15.1	03-May-2023	Shalini, Rama Madhavan	Balu Nair	Srikanth	For Review	Arcon PAM tool name is removed New template change
16.0	09-May-23	Shalini	Balu Nair	Srikanth	For Approval	Approved and baselined
16.1	11-Feb-24	Aishee	Vijaya		For Review	Mapped with new ISO 27001, 2022 controls

17.0	23-Feb-24	Aishee	Vijaya	Srikanth	For Approval	Approved and baselined
17.1	29-Apr-25	Kruti	Vijaya		For Yearly Review	Migrated to a new Template.
18.0	14-May-25	Kruti	Vijaya	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.