TRIANZ℠

User Responsibilities 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. Objective

The objective of this document is to ensure that Information Asset users are aware of their responsibilities for maintaining effective access controls particularly regarding the use of password and security of user equipment.

2. Scope

This document is applicable to all users of information assets at Trianz.

3. Responsibilities

3.1 Password Use

- Users shall be issued with a unique user ID and initial password to logon to the local system.
- At the time of the first login, the user shall change the password as per the password rules given below.
- The password must have alphanumeric characters and be non-dictionary. It must consist of a minimum of 8 characters.
- Password shall be a mix of uppercase alphabets, lowercase alphabets, numbers and/or some special characters.
- Password must be changed as per Password Security Policy.
- The user shall not share individual user passwords to any other users.

3.2 Clear desk and Clear Screen

- The employees will lock away all confidential and valuable documents (paper and magnetic) in cabinets or desk drawers (as appropriate) when the desk is unattended for an extended period - for example when away for meetings, at lunch times, or overnight.
- All wastepaper, which has any information or data on, must be placed in the confidential waste shredding bins located in each area. Under no circumstances should this type of wastepaper be thrown away with normal rubbish in the bins under each desk or the unclassified paper recycling bins.

- Personal computers and computer terminals and printers should not be left logged on when unattended and should be protected by key locks, passwords, or other controls when not in use.
- The employees will lock the PCs, when away from the desk using "Cltr + Alt + Delete" and will log off computers and laptops when unattended. The password –protected screensaver can be invoked and at cease of work, the employee will close all the applications and log off/shutdown the workstation/laptop and lock the laptop away or secure it through the use of a cable lock.
- All PCs, Laptops and workstations will be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes.
- The employees shall not store any video/audio/games etc on their computers.
- Incoming and outgoing mail points and unattended fax should be protected.
- Photocopiers should be locked (or protected from unauthorized use in some other way) outside normal working hours.
-
- The following guidelines should be applied:
- The users should not store confidential information on the personal computers. File servers should be used to store confidential information since appropriate access restriction can be applied for such confidential data. Availability of information is also ensured by regular backup at the server level
- Sensitive or classified information, when printed, should be cleared from printers immediately.
- The user should immediately collect the printouts from the network printers. The user should check the contents of the printout for completeness. In case the printing is incomplete and the user does not wish to continue printing, then he/she should press the 'Cancel Job' button to cancel the current print job. In case the job is not canceled

even after pressing the button (it may happen) then he/she should contact Facilities immediately.

- Every employee should make sure that there is no document kept in his/her desktop, before handing over the keys of the desk cabinet to administration department. Administration department hold no responsibility of any document kept inside the desk and if any document is found in the desk, it will be shredded without any prior approval.
- The following control measures should be undertaken by the users to secure their personal computers from unauthorized access:
- Users should terminate their logon session if they are leaving the computer unattended for long duration.
- Power on passwords should be used to prevent unauthorized booting of the computer
- Hard disk of the personal computer should not be shared. If in case sharing is required, then specific folder should be shared by using a sharing password.
- Standard screensaver and wallpaper supplied by the organization should be used in the organization.
- The users are not permitted to change the display settings set by the IT Team.
- For Cloud services, it is the responsibility of the administrator/user assigned to manage a specific cloud instance/virtual machine with above stated security measures where applicable.

4. Security and Data Privacy Role - Delivery

Ensure Compliance to Infosec Policies and Procedures
Ensure Compliance to Data Privacy Policies and Procedures
Ensures compliance to Client Specified Security Controls as defined in MSA and SOW
Ensures compliance Client Specified Data Privacy Controls as defined in MSA and SOW
Ensures Standards and regulatory compliances as per Client and Trianz
Ensures readiness for both Internal, External Audits and Client Audits
Ensures Infosec compliance as per the Security Controls specified below
SECURITY CONTROLS
Asset Management
Asset Inventory Maintenance (Client Assets)
Asset Risk Management
Asset Inventory Maintenance (Trianz Assets) of Derived Data Like Log files
Asset location Decision
Multi Tenancy and Client Data Isolation for cloud Projects only
Zoning
Filtering Incoming and Outgoing traffic
Web Application Firewall
Access Management
User Based Access control
User Access Management
Privileged Access Management
Root Admin

Inactivation
SSO
MFA
Password Management
Encryption of Data
At Rest
Database
Backup
Volume
Transmission
Key Management
Data retention and Disposal
Retention period definition
Secure Disposal
Patch Management and Malware Protection
Backup Management
Backup Location Decision
Frequency Decision
Incremental backup
Full backup
Log management
Access to Logs
Audit of Logs
Hardening
Server

Application
OS
Vulnerability and Penetration Assessment
Network Security
Licensing
Trainings
Change Management
Configuration Management
Incident Management
Security controls contract Compliance
Secure ODC (Secure ODC maintenance, if applicable)
BCP Testing & Reporting (if applicable)
Secure SDLC (if applicable)
Data Privacy -
Privacy by Design
Data Diagnostics
Personal Data Inventory
Data Privacy impact Assessment (Data Diagnostics, Data Inventory, Data flows)
Data Privacy Risk Management
Data Privacy Breach notification
Data Protection Contract commitments compliance
Vendor Management
Vendor Management (Agreements signing like NDA, DPA, Supplier Agreement, Vendor security Assessment)

5. Security and Data Privacy Role - Functions

Ensure Compliance to Infosec Policies and Procedures
Ensure Compliance to Data Privacy Policies and Procedures
Ensures compliance to Client Specified Security Controls as defined in MSA and SOW
Ensures compliance Client Specified Data Privacy Controls as defined in MSA and SOW
Ensures Standards and regulatory compliances as per Client and Trianz
Ensures readiness for both Internal and External Audits
Ensures Infosec compliance as per the Security Controls specified below
SECURITY CONTROLS
Asset Management
Asset Inventory Maintenance (Client Assets)
Asset Risk Management
Asset Inventory Maintenance (Trianz Assets) of Derived Data Like Log files
Asset location decision
Multi Tenancy and Client Data Isolation for cloud Projects only
Zoning
Filtering Incoming and Outgoing traffic
Web Application Firewall
Access Management
User Based Access control
User Access Management
Privileged Access Management
Root Admin
Inactivation

SSO
MFA
Password Management
Encryption of Data
At Rest
Database
Backup
Volume
Transmission
Key Management
Data retention and Disposal
Retention period definition
Secure Disposal
Patch Management and Malware Protection
Backup Management
Backup Location Decision
Frequency Decision
Incremental backup
Full backup
Log management
Access to Logs
Audit of Logs
Hardening
Server
Application

OS
Network Security
Licensing
Trainings
Change Management
Configuration Management
Incident Management
Security controls contract Compliance
Data Diagnostics
Personal Data Inventory
Data Privacy impact Assessment (Data Diagnostics, Data Inventory, Data flows)
Data Privacy Risk Management
Data Privacy Breach notification
Data Protection Contract commitments compliance
Vendor Management
Vendor Management (Agreements signing like NDA, DPA, Supplier Agreement, Vendor security Assessment)

6. ISO Controls Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Organizational Controls	5.2 Information Security Roles and Responsibilities 5,3 Segregation of duties	User Responsibilities Procedure

Document Control

Owner:	CISO	**Release ID:**	URP-PROC-0057

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.0	26-Feb-07	Jyotessh G Nair			Initial draft	None
0.1	26-Feb-07	Jyotessh G Nair			Review	Review feedback incorporated
1.0	26-Feb-07	Jyotessh G Nair			Baseline is approved by Zulfikar Deen.	Approved Baseline.
1.1	28-Apr-09	Bharateesha B R			Risk Assessment and Treatment Plan	Consolidated the User Responsibilities for Password Use and Clear Desk Clear Screen
2.0	03-Jun-09	Balu Nair			Approval for Baseline	Baselined
2.1	13-May-10	Balu Nair			QMG review	Formatted entire document
3.0	19-May-10	Balu Nair			Request for baseline	Baselined
3.1	24-May-11	Srilakshmi			QMG Review	Modified Release id in header and cover page

4.0	24-May-11	Srilakshmi			Approval for Baseline	Baselined
4.1	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
5.0	3-Aug-11	Sudharsana			Request for baseline	Approved and Baselined
6.0	28-Sep-12	Sudharsana			QMG review	Formatted as per latest template format
7.0	08-Nov-12	Balu Nair			Standardization of Blue Book Process Assets	• Modified the template format • Changed the Logo
7.1	14-Oct-16	Sriharsha				• Modified Clear desk and Clear Screen section by adding cloud services responsibility of the administrator /user. • Trianz Logo is modified
8.0	07-Dec-16	Balu Nair			Approved by CISO	Baselined

8.1	29-Apr-19	Balu Nair	Joshy VM			• Information classification modified • Trianz logo modified
9.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
9.1	15-May-20	Balu Nair	Phani Krishna		Annual Review	Migrated to the New template
10.0	15-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
10.1	3-Feb-21	Vijaya Rajeswari	Phani Krishna		For Review	• Delivery and Function SPOC's roles & Responsibiities for Infosec & Data Privacy are added Information classification updated
11.0	3-Feb-21	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
11.0	3-Jan-22	Karthik N	Karthik N		For Review	No changes
11.1	05-Apr-23	Balu Nair and Asha Veeramallu	Karthik N		As part of Annual Review	Minor changes to the procedure done New template change
12.0	09-May-23	Balu Nair		Srikanth Mantena	Annual Review	Approved and Baselined

12.1	15-Feb-2024	Vijaya	Balu	Srikanth Mantena	For review	Updated the section ISO Control Mapping aligning to ISO 27001:2022
13.0	23-Feb-24	Vijaya	Balu	Srikanth Mantena	For Approval	Approved and Baselined
13.1	28-May-25	Kruti	Vijaya		For Review	Migrated to new template
14.0	29-May-25	Kruti	Vijaya	Srikanth Mantena	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com