TRIANZ℠

Password Security 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 a standard for the creation of strong passwords, protection of those passwords and the frequency of change.

2. Objective

Ensure standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.

3. Scope

This policy covers all employees, including contract employees who are responsible for one or more accounts (e.g., Email, Server accounts, System accounts, etc.) or have access to any resource that requires a password.
The policy applies for all the stakeholders of internal Trianz products and services.

4. Policy Statements

4.1 Password Construction Requirements

- Passwords shall be a minimum of eight characters in length for all users.
- Passwords shall consist of at least three of the following four-character sets:
- Lowercase alpha characters (e.g., a, b, c, d, e)
- Uppercase alpha characters (e.g., A, B, C, D, E)
- Numbers (e.g., 1, 2, 3, 4, 5)
- Special symbol or punctuation characters (e.g., !, @, #, $, %, &, *, _, +, ~, . ,>)
- Passwords must not be the same as the User ID.
- Passwords must expire within a maximum of 42 or fewer days but not “0”.
- Ensure 'Minimum password age' is set to 1 or more day(s) but not “0”.
- Passwords must not be identical to the previous EIGHT (8) passwords.
- Passwords must not be transmitted in clear or plain text outside Trianz.
- Passwords must not be visible while typing.
- Passwords must not contain series of same letters.
- Ensure passwords reset is done only on authorized user’s request.

4.2 Password Creation

- All user-level and system-level passwords must confirm to the Password Construction Requirements given in section 4.1.
- Users must not include Personal information such as name, phone number, social security number, Date of Birth or Addresses in passwords.
- User accounts that have system-level privileges granted through group memberships or programs (E.g., Sudo) must have a unique password from all other accounts held by that user to access system-level privileges.

4.3 Password Change

All system-level passwords (E.g., root, NT admin, application administration accounts, etc.) must be dual controlled & changed at least once in 42 or fewer days but not "0".

All user-level passwords (E.g., Email, web, desktop computer, etc.) must be changed at least once in 42 or fewer days but not "0".

All password change procedures must include the following:

- Authentication of the user prior to changing the password (acceptable forms of authentication include answering a series).
- The new password must comply with password strength requirements associated with the data classification for the service in question.

4.4 Password Protection

- User is responsible for the security of user password(s), and accountable for any loss/compromise.
- Passwords must not be shared with anyone and need to be treated as sensitive, Confidential Trianz information.
- Any user suspecting that his/her password may have been compromised must change the password immediately and report the incident to is@trianz.com and copy to itservicedesk@trianz.com
- Passwords must not be inserted into email messages, and other forms of electronic communication.

- Passwords should not be revealed to anyone (including administrative assistants, secretaries, managers, co-workers while on vacation, and family members) over the phone, on questionnaires.
- Users should not write passwords down and store them anywhere in your office, in paper, computer system or mobile devices (phone, tablet) without encryption.
- Users should not use the "Remember Password" feature of applications (for example, web browsers).
- Password shall get locked after 5 unsuccessful attempts.
- Vendor or service accounts default passwords shall be removed from computer systems prior to deployment and new passwords are to be implemented on all systems immediately upon installation.

4.5 Roles and Responsibilities

Roles	Responsibilities	Internal/External
All Associates	Change of the password as per the policy Security of the Password	Internal
IS Operations Team	Password Policy deployment Reset the password based on the request from the User	Internal
Product/Project Manager	Publishes and maintains policy guidelines for the creation, safeguarding, and control of the passwords	Internal
InfoSec & Compliance Team	Audit Password policy adherence during the internal audit	Internal

5. Applicable Standards

ISO 27001:2022
ISO 27701:2019

6. ISO Control Mapping

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Organizational Controls	5.17 Authentication Information	Password Security Policy

7. Reference Policies & Procedures

Access Management Policy
Access Management Procedure

8. Implementation Procedure

ISO Operation Procedure

9. Exceptions(s)

Exceptions to the Change management policy will require formal written approval from the Information Security Assurance Team.
Refer to *Exception Handling Policy.*

Document Control

Owner:	CISO	**Release ID:**	PSP-POL-0039

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	13-Oct-17	Roshni Madhusoodan	Shishir Kumar Singh		For Review	Creation of Password Policy
1.0	13-Oct-17	Roshni Madhusoodan	Shishir Kumar Singh		For Approval	Approved and Baselined
1.1	16-Feb-18	Kamadev Pradhan	Joshy VM		For Review	Updated as per the standard & inclusion of metrics
2.0	19-Feb-18	Siva Krishna	Gangadhar AKA	Ganesh Arunachala	Approval for Baseline	Updated as per enforced AD Group policy
2.1	10-May-20	Balu Nair	Phani Krishna		Annual Review	Modified the document with new template
3.0	14-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
3.1	27-Aug-20	Balu Nair	Rajesh B		For Review	Modified section 3.1 by adding Password age – CIS best practices
4.0	27-Aug-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined

4.1	2-Feb-21	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Review	Updated with new Information Classification
5.0	2-Feb-21	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
5.1	03-Jul-21	Balu Nair	Phani Krishna	Phani Krishna	As part of Annual review and inputs from external audit	Migrated to the new template.
6.0	30-Jul-21	Balu Nair	Phani Krishna	Phani Krishna	Approved for Baseline	Baselined
6.0	04-Jan-22	Sanjana	Balu Nair	Siva N	For Review	Reviewed and no changes in the document
6.1	14-Mar-22	Sanjana	Balu Nair	Siva N	For Review	The scope has been extended to products and services
7.0	21-Mar-22	Sanjana	Balu Nair	Siva N	For Approval	Approved and Baselined
7.1	03-May-23	Shalini, Asha Veeramallu	Balu Nair	Srikanth	For Review	Field 4.1, 4.4 and field 8 is updated New template change
8.0	08-May-23	Shalini	Balu Nair	Srikanth	For Approval	Approved and baselined
8.1	15-Feb-24	Vijaya	Balu Nair	Srikanth	For review	Updated the section ISO Control Mapping aligning to ISO 27001:2022

9.0	23-Feb-24	Vijaya	Balu Nair	Srikanth	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	For Approval	Approved and baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com