Password Administration Policy

Version 9

Document Information

Name of the document	Password Administration
Release date	19-Dec-2018
Owned by	Mayank Baghel
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	13-Nov-2018	Initially Drafted
2	10-Dec-2018	Final
3	15-Dec-2020	Reviewed and no change
4	02-Dec-2021	Reviewed and no change
5	04-Mar-2022	Updated Document Information
6	02-Mar-2023	Reviewed and no change
7	24-Sep-2024	Updated Document Information
8	24-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	29-May-2026	Reviewed and updated

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	CTO	Approved	04-June-2026

Table of Contents

Overview

Use of User IDs and passwords is a standard way of protecting personal information. Rezolve.ai, for business uses, takes appropriate measures to ensure that passwords provide a level of protection. This policy will apply to all applications, systems, and networks.

Policy Detail: Use of Passwords

Passwords will be used in combination with User IDs to grant access to applications, systems, and networks.

Confidentiality

Passwords will be unique per individual. It is the individual's responsibility to ensure the privacy of the passwords.

The following activities are prohibited:

- Disclosing passwords to other users
- Obtaining other individual's passwords
- Using another individual's password to login as that individual

Password Strength

Passwords should be complex so that they cannot be guessed easily. Following restrictions should be applied to passwords:

- Password must be at least 8 characters in length
- Password must be a mix of alpha and numeric characters and contain at least one special character
- Passwords should be case sensitive
- Password for Production and Development systems or accounts must be different where possible
- Sensitive passwords must not be stored in unencrypted format
- Password change is necessary for system superuser accounts when employee leaves

Expiration of Passwords

1. All system admin passwords for database administrators will change every 30 days.
2. For all applications that store PII/ePHI or other Protected Information, password should be changed minimally every 90 days.

Failed Password Lockout

Where possible, all systems detect for intruder attempts for password guessing. The system disables passwords after 5 incorrect attempts. If an employee's password becomes disabled, the system will disable that user's account for a period of 2 hours. After 2 hours, the account will become active again. The system administrator can also reset the password on the account to eliminate the 2-hour wait while the account is disabled.

NOTE – Next review cycle for this policy is **March 2027**. Management can review policy any time and can make changes depending on the situation.
All documents related to policies and procedures – any reference to Actionable Science is as good as Rezolve.ai.