QUADRANT RESOURCES Pvt.Ltd.
ACHIEVE MORE TOGETHER

Password Policy

Version 1.0

Version #	Date (DD-MMM-YYYY)	Details of the Changes	Modified By	Reviewed & Approved By
1.0	1 Sep 2020	First Release	SK Javed	Sridhar Reddy
1.0	10 Oct 2021	Reviewed No Changes Made	SK Javed	Sridhar Reddy
1.0	5 Oct 2022	Reviewed No Changes Made	SK Javed	Sridhar Reddy
1.0	5 July 2023	Reviewed No Changes Made	SK Javed	Sridhar Reddy
1.0	10 Jun 2024	Reviewed No Changes Made	Manu Mitragotri	Sridhar Reddy

Contents

1 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.

2 Scope

The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the Quadrant domain. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

3 Policy Guidelines

Principles and Guidelines to be followed:

- Password Complexity: Require passwords to be complex and difficult to guess. Encourage the use of a combination of uppercase and lowercase letters, numbers, and special characters.
- Password Length: Set a minimum password length to ensure an adequate level of security. The length should be sufficient to prevent easy brute-force attacks. Common recommendations suggest a minimum of **Eight characters, but longer passwords are generally more secure.**
- Password Expiration: Implement password expiration to ensure that passwords are regularly updated. The frequency of password changes can vary depending on the organization's risk appetite, but common recommendations range from **30 days**.
- Password History: Enforce a password history policy to prevent users from reusing previously used passwords. **History is set to 6 Passwords.** This measure helps to enhance security and minimize the risk of compromised accounts.
- Account Lockouts: Implement mechanisms to prevent brute-force attacks by locking user accounts after a **5 failed login attempts**. This discourages attackers from repeatedly guessing passwords.
- Two-Factor Authentication (2FA): Implement use of two-factor authentication for added security. 2FA combines something the user knows (password) with something the user possesses (e.g., a mobile device or hardware token).
- Password Storage: Store passwords securely using appropriate cryptographic hashing algorithms. Avoid storing passwords in plaintext or using weak hashing mechanisms.
- User Education and Awareness: Provide training and awareness programs to educate users about password best practices, such as not sharing passwords, avoiding common passwords, and recognizing phishing attempts.
- Regular Reviews and Audits: Conduct periodic reviews and audits of password policies and practices to ensure compliance with the policy and identify areas for improvement.

4 Responsibilities

- All individual users having accounts for accessing systems/services in the Quadrant domain, and system/network administrators of Quadrant servers/network equipment's shall ensure the implementation of this policy.
- All designers/developers responsible for site/application development shall ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.