PASSWORD POLICY

Oneview Corporate Advisors Private Limited

CIN: U74999MH1976PTC407933

Registered Address:
619 & 620, 6th Floor,
The Summit Business Bay, 266/1-172, Gundavali, Andheri Kurla Road,
Andheri (East), Mumbai - 400 093

Correspondence Office:
18, Deshapriya Park Road, Kolkata - 700 026.

Table of Contents

1) INTRODUCTION

This Password Policy ("Policy") adopted by Oneview Corporate Advisors Private Limited (herein after referred to as "OCAPL" or "the Company",) establishes the minimum requirements and best practices for the creation, usage, storage, and management of passwords across the organization. It is designed to ensure that all users—including employees, contractors, and third-party service providers—adhere to strong authentication standards when accessing the organization's systems and information resources.

2) PURPOSE:

The purpose of this Policy is to establish standardized requirements for the creation, use, management, and protection of passwords to safeguard the organization's information assets and systems from unauthorized access.

3) SCOPE:

This guideline applies to employees, interns, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties who are granted access to the organization's information systems and resources. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

4) POLICY STATEMENTS

4.1 Password Construction Guidelines

i. Have minimum length of eight characters
ii. Must contain of alphanumeric characters
iii. Contain both upper- and lower-case alphabets
iv. Contain at least one numeric character (for example, 0-9)
v. Contain at least one special character (for example, $%^&*() _+|~-=\` {} []:";'<>? /)
vi. Password should not be same as user ID
vii. Should not contain dictionary-based words or proper names, including foreign language, or exist in a language slang, dialect, or jargon
viii. Should not contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters
ix. Should not contain characters in sequential patterns such as aaabbb, qwerty, zyxwvuts, or 123321
x. Should not be transmitted in clear or plain text
xi. Interactive login: Should prompt user to change password before expiration to five days. When their password expiration date is five or fewer days away, users will see a dialog box each time that they log on to the domain.

4.2 Password Deletion Guidelines

All user accounts and passwords that are no longer needed, must be deleted or disabled immediately. This includes, but not limited to:

i. User retires, quits or dismissed from his service
ii. Default password should be changed immediately on all systems
iii. Contractor's account should be disabled immediately after their service is no longer needed

4.3 <u>Password Protection Guidelines</u>

i. Do not use your user ID as password
ii. Do not share your password with anyone, including your manager, administrative assistant, or secretary
iii. Do not share your password over phone to anyone
iv. Do not reveal password in an email message
v. Do not talk about password in front of others
vi. Do not hint at format of password (e.g., "My Pet Name")
vii. Do not share your password with colleague while on vacation
viii. Do not use "Remember Password" feature of browsers or any other applications
ix. The Retention period of the logs shall be decided by the Designated Officer.

If someone demands to share password, refer them to this document or ask them to call IT Security Head.
If an account or password is suspected to be compromised, report this incident to Head of Department, Head of IT or Head of IT Security & Governance.