[Company Logo]

PASSWORD MANAGEMENT POLICY

The purpose of Password Management Policy and Process is to ensure that security practices are introduced and maintained by all employees with respect to password-protected information infrastructure.

Document Owner
Head of IT/Security

[Company Logo]	**CONTROLLED DOCUMENT** **Password Management Policy**	Document: Password Management Policy Developed by: Reviewed by: Approved by:

Password Management Policy

For

[Company Name]

Version: 1.0
Date: 01/01/0000
Next Review Date :

Note: Verify with the Policy Owner if this is the correct and latest version before use.

Revision History

Rev. #	Date	Modification Details	Page#	Suggested By	Reviewed By	Approved By
1.0		First Draft	NA			

Table of Contents

[Company Logo]	**CONTROLLED DOCUMENT** **Password Management Policy**	Document: Password Management Policy Developed by: Reviewed by: Approved by:

Purpose

The purpose of the Password Management Policy and Process is to ensure that security practices are introduced and maintained by all employees with respect to the password-protected information infrastructure.

Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by [Company Name]. Password Management Policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any [Company Name] facility, or has access to the [Company Name] network. All users (employees, contractors, vendors, or others) of IT resources are responsible for adhering to this policy.

Objective

The objective of the Password Management Policy is to:

1. To establish a standard for the creation of strong passwords.
2. To ensure the protection of those passwords and the frequency of password changes.
3. To set rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.
4. To ensure that Password management standards are followed by all employees.
5. To ensure the password is complex.
6. To ensure the password complexity rule is followed.
7. To ensure passwords are unique.

Responsibility & Accountability

Adherence to Password Management Policy is the responsibility of the entire [Company Name] and its affiliates, subsidiaries, personnel, third-party consultants, contractors, vendors, and any individual or entity that is provided access to the [Company Name]'s information resources.

The Top Management / CISO will be accountable for the overall Password Management Policy.

Non-Compliance

Any Non-Compliance with this Password Management Policy will be dealt with Disciplinary Action as decided by the organization and respective authorities.

Exceptions

Not Applicable.

Policy Statement

For users having accounts for accessing systems/services:

- Users shall be responsible for all activity performed with their personal user IDs. Users shall not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.
- All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every three months). Users shall not be able to reuse previous passwords.
- Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers, and characters.
- All access codes, including user ID passwords, network passwords, PINs, etc., shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information.
- All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords.
- Passwords must not be communicated through email messages or other forms of electronic communication, such as phone to anyone.
- Passwords shall not be revealed on questionnaires or security forms.
- Passwords of personal accounts should not be revealed to the controlling officer or any co-worker, even while on vacation, unless permitted to do so by the designated authority.
- The same password shall not be used for each of the systems/applications to which a user has been granted access, e.g., a separate password to be used for a Windows account and a UNIX account should be selected.
- The “Remember Password” feature of applications shall not be used.
- Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.
- First-time login to systems/services with administrator-created passwords should force changing of password by the user.
- If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.
- The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

Policy for constructing a password: All user-level and system-level passwords must conform to the following general guidelines described below.

- The password shall contain more than eight characters.
- The password shall not be a word found in a dictionary (English or foreign).
- The password shall not be a derivative of the user ID, e.g., <username>123.
- The password shall not be slang, dialect, jargon, etc.
- The password shall not be a common usage word, such as names of family, pets, friends, co-workers, fantasy characters, etc.
- The password shall not be based on computer terms and names, commands, sites, companies, hardware, or software.
- The password shall not be based on birthdays and other personal information such as addresses and phone numbers.
- The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc., or any of the above spelled backwards.
- The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g.,!@# $%^&*()+|~-=\`{}[]:";'<>?,./).
- Passwords shall not be such that they combine a set of characters that do not change with a set of characters that predictably change.

Suggestions for choosing passwords

Passwords may be chosen such that they are difficult to guess yet easy to remember. Methods such as the following may be employed.

- String together several words to form a passphrase as a password.
- Transform a regular word according to a specific method, e.g., making every other letter a number reflecting its position in the word.
- Combine punctuation and/or numbers with a regular word.
- Create acronyms from words in a song, a poem, or any other known sequence of words.
- Bump characters in a word a certain number of letters up or down the alphabet.
- Shift a word up, down, left, or right one row on the keyboard.

Password Protection Standards

Do not use your User ID as your password. Do not share [Company Name] passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential [Company Name] information.

Here is a list of "do not's"

- Don't reveal a password over the phone to anyone
- Don't reveal a password in a mail message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to a co-worker while on vacation
- Don't use the "Remember Password" feature of applications
- Don't write passwords down and store them anywhere in your office.
- Don't store passwords in a file on ANY computer system unencrypted.

Conclusion

This document provides an Overview of the Password Management Policy & its deliverables, the project team participants, and their roles and responsibilities. It is intended to assist Application Managers and developers of [Company Name] applications and to ensure a consistent approach to password management.

<<< End of Document >>>