Marquistech – Password Policy

Owner	:	Information Security Officer
Reviewer	:	Sudarshan Kadam
Approver	:	Deven Potdar
Version & Status	:	1.6, Approved

1. Purpose

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

2. Scope

This policy applicable to all employees, contractors, and consultants who handle Marquistech assets including those who have access to sensitive information or sensitive information entrusted to Marquistech.

3. Policy

a) 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. 123.
   - 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, 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., !@# $%^&*()_+|~-=\` {}[]:";'<>?,./).

b) 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.

- Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.
- All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone, including co-workers. These shall be treated as sensitive, confidential information. A
- Passwords must not be communicated though 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 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 an 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.

4. Responsibilities

All individual users having accounts for accessing systems/services in the Marquistech domain, and system/network administrators of servers/ network equipment shall ensure the implementation of this policy.

5. Revision History

Version	Reviewer	Date
1.6	Deven Potdar	8th May 2023
1.6	Sudarshan Kadam	11th April 2024
1.5	Deven Potdar	8th May 2023
1.4	Sudarshan Kadam	2nd February 2022
1.3	Deven Potdar	5 January 2021
1.2	Deven Potdar	1 April, 2020
1.1	Deven Potdar	05 September, 2019

1.0	Deven Potdar	26 July, 2019