IT
PASSWORD POLICY

1 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to Mister Car Wash systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords

This policy is based on the standard template issued by the SANS Institute, a cooperative research and security education organization (https://www.sans.org) and the Payment Card Industry Data Security Standard (PCI DSS) (https://www.pcisecuritystandards.org).

2 Purpose

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

3 Scope

The scope of this 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 Mister Car Wash facility, has access to the Mister Car Wash network, or stores any non-public Mister Car Wash information.

4 Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines (Appendix A).

4.1.2 Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.

4.1.3 It is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

4.1.4 Do not use vendor-supplied defaults for system passwords and other security parameter.

4.2 Password Change

4.2.1 In order to comply with PCI regulations in the Cardholder Data Environment (CDE),

4.2.1.1 passwords must be changed every 90 days

4.2.1.2 passwords cannot be the same as any of the last 4 passwords used

4.2.2 Passwords must also be changed when there is reason to believe a password has been compromised.

4.2.3 Password cracking or guessing may be performed on a periodic or random basis by Mister IT or their delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Mister Car Wash information.

4.3.2 Passwords must not be inserted into email messages or other forms of electronic communication with any user or system identifying information.

4.3.3 Passwords may be stored only in “password managers” authorized by the organization.

4.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

4.4.1 Application developers must ensure that their programs contain the following security precautions:

4.4.2 Applications must support authentication of individual users, not groups.

4.4.3 Applications must not store passwords in clear text or in any easily reversible form.

4.4.4 Applications must not transmit passwords in clear text over the network.

4.4.5 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Multi-Factor Authentication

4.5.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

5 Policy Compliance

5.1 Compliance Measurement

Mister IT will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the IT Department in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

None

7 Definition and Terms

7.1 *Multi-factor (MFA):* method of authentication requiring more than one form of validation to verify the user's identity for a login or other transaction.

7.2 *Password manager:* a software application or a hardware device that is used to store and manage a person's passwords. Typically, stored passwords are encrypted.

Appendix A
Password Construction Guidelines

1 Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords.

2 Purpose

The purpose of this guidelines is to provide best practices for the created of strong passwords.

3 Scope

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. 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 Statement of Guidelines

4.1 Passwords must be at least 9 characters, however we recommend a minimum of 14 characters.

Strong passwords are long, the more characters you have the stronger the password. We highly encourage the use of passphrases, which are passwords made up of multiple words. Examples include “It’s time for vacation” or “block-curious-sunny-leaves”. Passphrases are both easy to remember and type, yet meet the strength requirements.

Poor, or weak, passwords have the following characteristics:

- contain eight characters or less
- contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters
- contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321

5 are some version of “Welcome123” “Password123” “Changeme12