MARCO'S MANAGED SERVICES PASSWORD STANDARDS

The following are minimum standards for passwords for all Designated Users covered under a Marco Product Agreement.

Password Requirements

Passwords must meet the following minimum requirements for length and complexity:

- Be at least 10 characters in length
  - Requirement is reduced to 8 characters in length when MFA is also being used
  - Any industry regulated or governed by a law that mandates specific configurations, processes or procedures must be at least 16 characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)
- May not contain all or part of a user's username or ID
- May not be based on personal information such as name, birthday, address, phone number, etc.
- May not be based on company name, season, or geographic location
- May not be used for any other account on any other information system
- May meet or exceed Client's regulatory requirements
- May not be found in the dictionary

Enforcement of the minimum requirements is limited to software authentication solution used.

The list of requirements above follows industry best practices from CIS Top 20 v7.1 and NIST CSF v1.1. It does NOT guarantee that an account cannot be compromised.

Password length and complexity determine the maximum time a password should be used. Multi-Factor Authentication ("MFA") does not sufficiently replace strong passwords. Strong passwords and MFA work together to strengthen and protect an organization's authentication.

Domain Password Expiration

Passwords will be required to change at a minimum interval of every 180 days, including accounts previously set to "Never Expire". Any service account in which a password is entered on a one-time basis during initial set up will not expire but will follow the above complexity requirements. If a password is exposed beyond its creator, the creator will change the password.

Domain Account Lockout

If a user fails 10 consecutive login attempts, the account will automatically be locked. Failed login attempts are typically indicative of a forgotten password or an attempt by an unauthorized party to log in. Users who experience an account lockout should contact the Marco Support Desk and request a password reset. Users who request password resets will be expected to verify their identity for the Support Desk.

Password Communication

Marco will communicate passwords using secure methods (via phone or encrypted email). Marco will never call a user and ask them for their password. Marco will request that the user change their password upon first login after a password reset or if a Marco employee learns a user's password for any reason.

Request to Waive

A Client may request a waiver to this policy by submitting a written request. This request will be reviewed by Marco and a response with any conditions or caveats will be provided for written signoff.

Effective: February 25, 2022