

Policy Name:	Password Policy				
Revision #:	0.9	Effective:	July 28, 2021	Page	1 of 2

1.0 PURPOSE AND SCOPE

The purpose of this policy is to prevent the unauthorized use of organization accounts, whether they be on company-owned computer workstations, servers, network devices, web applications and other systems, and whether they be user, administrative or service accounts. This policy establishes standards for strong passwords and the protection of user and system accounts. The policy applies to all of the organization's information systems that contain the organization's data, such as computers, servers, cloud and SaaS systems, mobile devices, and systems administered by third parties on the organization's behalf.

2.0 ACCOUNT TYPES

Accounts are categorized as follows. Each category may have different password requirements.

- User accounts in Active Directory – accounts that normal, non-administrative users of the organization use to log in to organization systems and applications
- User accounts not in Active Directory - accounts that normal, non-administrative users of the organization use to log in to organization systems and applications
- Service accounts in Active Directory – accounts that are in Active Directory that have elevated privileges to one or more systems or applications

3.0 POLICY

3.1 User, Administrative, and Service Accounts in Active Directory

- Passwords must be at least 15 characters in length.
- Passwords may not be based on personal information such as birthdays, addresses, names, etc.

3.2 User and Accounts not in Active Directory

- Passwords must be at least 15 characters in length.
- Passwords may not be based on personal information such as birthdays, addresses, names, etc.
- Users can choose to have these passwords match their active directory passwords.

3.3 General Password Rules

- Passwords may never be written down anywhere that is not physically secured, such as a locked file cabinet or safe. (No sticky notes!)
- Password can never be included in unencrypted e-mails or other form of electronic communications.
- Never reveal your password to anyone over the phone, including help desk personnel.
- Do not share your passwords with assistants, coworkers, family members, or friends. All passwords must be treated as company confidential.
- Do not store your passwords in any portable electronic device such as tablets or cell phones unless it is a secure, encrypted password management program such as LastPass or SplashID.
- Notify technology services and passwords immediately if there is any suspicion that the password has been compromised.

Policy Name:	Password Policy		
Revision #:	0.9	Effective:	July 28, 2021
		Page	2 of 2

4.0 RELEVANT NIST CONTROLS

- NIST 800-53 - IA3, IA5 – Identification and Authentication: - Authenticator (password) Management; Device
- NIST Cybersecurity Framework - PR-AC - Identity Management, Authentication and Access Control

5.0 IDENTIFICATION AND AUTHENTICATION REVISION HISTORY

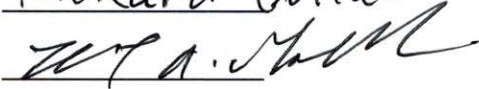
Date	Revision #	Description of Change
2021-06-07	0.9	Initial creation
	1.0	Finalized

6.0 INQUIRIES

Direct inquiries about this policy to: the Chief Financial Officer

7.0 SIGNOFF

This policy is approved by the policy owner, the Chief Financial Officer.

Printed name: Richard Gollub
 Signature: 
 Date: 7.28.2021