	Policy Title		
			IT: Password Policy
	Control Number	**Policy Date**	**Revision Date**
	SC006	03/04/2024	New

Purpose

The purpose of this policy is to outline the password policy at Scotland County. These rules are in place to protect the employee and Scotland County. Inappropriate use of passwords exposes Scotland County to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of passwords for information, electronic and computing devices, and network resources to conduct Scotland County business or interact with internal networks and business systems, whether owned or leased by Scotland County the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Scotland County and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Scotland County policies and standards, and local laws and regulation. cotland County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Scotland County.

Overview

This policy states the requirements for securing and the proper use of passwords while accessing workstations or mobile devices within Scotland County networks and /or in storing Scotland County information.

Guidelines

User/Password Characteristics

- All Scotland County user accounts MUST be unique, and traceable to the assigned user. Scotland County will take appropriate measures to protect the privacy of user information associated with user accounts. Users shall not use the same password for Scotland County accounts as they would for personal accounts. The use of group accounts and group passwords is not allowed, unless specifically approved by Scotland County Manager.

- VC3/Scotland County will verify a user's identity prior to resetting their password or in the absence of the user, the user's manager may request to have the password reset.

- Users will be granted the minimum access required to perform their specific tasks. Granting access levels to resources shall be based on the principle of least privilege, job responsibilities, and separation of duties. The level of minimum access requires the recommendation of the user's manager, and the evaluation of the information system owner. The information system owner will have final determination as to the level of a user's access for their system.

- Accounts will be disabled after 30 days of inactivity. Users planning to deploy to field operating locations or to be away from their working office for other approved periods of extended absence should coordinate their absence with the managers to ensure proper disposition of the account.

- All requests for temporary user accounts shall provide an expiration date to be applied at the time the account is created. Where this isn't possible, a manually controlled mechanism can be used. The system owner will monitor temporary access to ensure activities comply with the intended purpose.

- The use of shared logins or automatic logon software to circumvent password entry shall not be allowed, except where a specific business need exists, and where the business has determined that configuring individual names accounts is not viable. The use of shared logins or automatic logins is not allowed, unless specifically approved by the Scotland County Manager. If approved, passwords for these accounts shall be kept in a secure password manager.

- Each individual assigned a user account and password is responsible for the actions taken under said account and must not divulge that account information to any other person for any reason.

- All user-level passwords must be changed every 90 days. Passwords must never be stored in clear text in any file in any format on any device within the Scotland County infrastructure, nor may they be stored in clear text on personal computers, laptops, mobile devices, etc.

- Passwords must be at least 14 characters, not contain the user's account name or parts of the user's full name that exceed two consecutive characters, strong in nature and adhere to the following criteria. Passwords MUST contain characters from three of the following categories: English uppercase characters (A through Z), English lowercase characters (a through z), Base 10 digits (0 through 9), Non-alphabetic characters (for example, !, $, #, %).

- Avoid using individual words from any dictionary. Whenever possible use pass phrases or substitution ciphers for your password. Example: It was the best of times, it was the worst of times = Iwtb0t,iwtw0t.

- Passwords must never be sent in unencrypted electronic communications.

- Vendor/System passwords should not be the default passwords provided by the Vendor/System and follow criteria above.

Compliance

The Management team 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.

Exception

Any exception to the policy must be approved by the County Manager, the IT Services provider and/or IT Personnel in advance.

Disciplinary Action

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