St Clair County Password Policy

Policy #66

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise St Clair County's entire network. As such, all St Clair County employees (including contractors and vendors with access to St Clair County systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

2.0 Purpose

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

3.0 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 St Clair County facility, has access to the St Clair County network and/or ALEA/NCIC network or stores any non-public St Clair County ALEA-based Criminal Justice Information (CJI).

4.0 Policy

4.1 General

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot reuse the past 10 passwords.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level, system-level, and ALEA/NCIC access level passwords must conform to the guidelines described below.

4.2 Guidelines

Password Construction Requirements:

i. Be a minimum length of eight (8) characters on all systems.
ii. Must include 3 out of 4 of the following
    a. Capital letter
    b. Lowercase letter
    c. Number
    d. Special character (!#$@%^*&)

iii. Not be a dictionary word or proper name.
iv. Not be the same as the User ID.
v. Expire within a maximum of 90 calendar days.
vi. Not be identical to the previous ten (10) passwords.
vii. Not be transmitted in the clear or plain text outside the secure location.
viii. Not be displayed when entered.
ix. Ensure passwords are only reset for authorized user.

4.3 Password Deletion

All passwords that are no longer needed must be reset, deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment.
- Contractor accounts, when no longer needed to perform their duties.

When a password is no longer needed, the following procedures should be followed:

- Employee should notify his or her immediate supervisor.
- Contractor should inform his or her point-of-contact (POC).
- Supervisor or POC should send an email to helpdesk@stclairco.com or call 205-594-2496.
- A St Clair County Information Technology supervisor will then reset, disable or delete the user's password, depending on the situation, and delete or suspend the user's account.
- A second individual from that department will check to ensure that the password has been reset, disabled or deleted and user account was deleted or suspended.

4.4 Password Protection Standards

Do not use your User ID as your password. Do not share St Clair County passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential information.

Here is a list of "do not's"

- Don't reveal a password over the phone to anyone
- Don't reveal a password in an mail message
- Don't reveal a password to the boss
- Don' talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to a co-worker while on vacation
- Don't write passwords down and store them in clear view of anyone.
- Don't store passwords in a file on ANY computer system unencrypted.

If someone demands a password, refer them to this document or have them call Information Technology Manager or Assistant Manager.
If an account or password is suspected to have been compromised, report the incident to Information Technology Department and change all passwords.

4.5 Remote Access Users

Access to the St Clair County network via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required).

5.0 Penalties

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

Approved: March 22, 2022
Effective Date: May 2, 2022

Paul Manning 3/23/2022

Paul Manning, Chairman