ANTRIM COUNTY
PASSWORD POLICY
Adopted: October 13, 2016

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 of Antrim County's entire network. As such, all Antrim County employees are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

2.0 Objective

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 Antrim County facility, has access to the Antrim County network, or stores any non-public Antrim County information.

4.0 Policy and Procedures

4.1 General

- All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.
- 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 and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

4.2.1 Password Construction Requirements

a. Passwords must be a minimum of 8 characters in length
b. Not be a dictionary word or proper name.
c. Not be the same as the User ID.

d. Incorporate a minimum complexity that includes the following characteristics:
   i) at least one lower case letter (a-z)
   ii) at least one upper case letter (A-Z)
   iii) at least one number (0-9)
   iv) at least one punctuation or non-alphanumeric characters (e.g. ! @ # $ % ^ & * ( ) _ - + = { } [ ] ;: ; " ` | \ / ? < > , .).
e. Expire within a maximum of 90 calendar days.
f. Not be identical to the previous ten (10) passwords.
g. Not be displayed when entered.

4.2.2 Password Deletion

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

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

4.2.3 Password Protection Standards

All passwords are to be treated as sensitive, confidential Antrim County information.

Here is a list of "Do Not's":

- Do not reveal a password over the phone to anyone
- Do not reveal a password in an email message
- Do not reveal a password to your supervisor
- Do not reveal a password with anyone, including administrative assistants or secretaries.
- Do not talk about the specifics of a password in front of others
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- Do not share a password with family members
- Do not reveal a password to a co-worker while on vacation
- Do not use the "Remember Password" feature of applications
- Do not write passwords down and store them anywhere in your office.
- Do not use the same password for Antrim County accounts as for other non-Antrim County access

If someone demands a password, refer them to this document or have them call the Information Technology Department.

If an account or password is suspected to have been compromised, report the incident to the Information Technology Department and change all passwords.

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

4.3 Remote Access Users

Access to the Antrim County networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user ID are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

5.0 Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Elected officials who violate this policy may be subject to various levels of restricted access to the county network up to and including termination of access.

6.0 Review

The Information Technology Department shall review this policy as needed or at least once every 3 years.