DEVELOPMENT AUTHORITY OF THE NORTH COUNTRY

AUTHORITATIVE POLICY: Information Technology and Security

Board Resolution No.: 2013-10-01

PROCEDURE: 2.3 - Password Management

1.0 Introduction

Policy:
The Authority will require network users to create strong passwords in order to help protect the network from unauthorized use.

Purpose:
To delineate procedures for accessing the Authority IT network and/or accessing the Internet through the Authority IT network.

Scope:
This applies to all personnel with access to Internet and related services throughout the Authority network infrastructure. Internet Related services include all services provided with the TCP/IP protocol, including but not limited to Electronic Mail (e-mail), File Transfer Protocol (FTP), and World Wide Web (WWW) access.

Responsibilities:
All Authority personnel are responsible for knowing and adhering to this password policy and procedure.

The IT Director is responsible for enforcing this procedure.

Definitions:
Technology Resources – All computing, networking, and software applications that can be accessed by authorized Authority users.

User – Anyone with authorized access to the Authority technology resources including permanent and temporary employees or third party personnel such as temporaries, contractors, consultants, and other parties with valid Authority access accounts.

2.0 Procedure - Password Use Policy

2.1 No persons or systems may access Authority data, networks, applications or resources without a unique login and password. User passwords are sensitive, confidential information and must not be shared with others. Passwords are the first line of protection against threats to network security whether threats originate internally or externally.

2.2 If accounts or passwords have been compromised, report the incident to the IT Director and change all passwords immediately.

2.3 If an administrator requires that you login to a machine or service, use precautions so that password(s) are not witnessed.

2.4 Anyone demanding a password must be reported to the Division Manager or Executive Director.

3.0 Minimum/Maximum Password Age

Password age refers to the time during which a password must be used before a new password can be selected. Where technically possible, the minimum password age at Authority is seven days and the maximum is 180 days.

4.0 Password Lockout Policy

Users are locked out of their account after three failed logon attempts. Failed logon attempts are the result of attempting to logon using either a faulty logon ID (user name) or password.

5.0 Temporary Passwords

A first-time Authority computer user (or those requiring a password reset) is given a temporary password that must be changed immediately after the first login.

6.0 Secure Password Guidelines

6.1 Required Password Complexity

The Authority requires using the "strong password" complexity guidelines below. This helps ensure that all systems, intellectual property, and other sensitive data are afforded a proven level of protection. Each user password will be required to meet the following criteria:

- The password must be at least nine characters long.
- Password must contain at least three of the five following categories:
  - English uppercase characters (A-Z)
  - English lowercase characters (a-z)
  - Base 10 digits (0-9)
  - Non-alphanumeric symbols (for example: $, #, or %)
  - Unicode characters

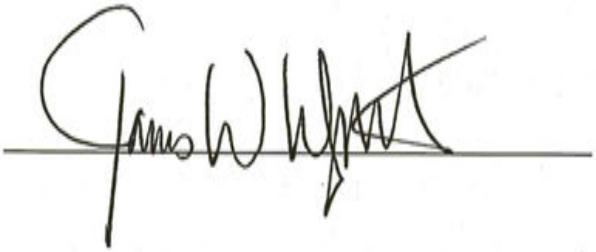
- A password will not be accepted if it contains three or more characters from the user's account name.

7.0 Adopt Secure Password Habits

Poor or weak passwords are those with the highest probability of being guessed or cracked. Security risks can be avoided by not:

- Using a single word found in a dictionary (English or foreign) as a password;
- Choosing easily guessed words such as:
  - names of family, pets, friends, co-workers, fantasy characters, etc;
  - Computer terms and names, commands, sites, companies, hardware, or software.

- Choosing words, such as "Authority, " "newyork," "sanfran," or any derivation;
- Including birthdays or other personal information like addresses and phone numbers;
- Using ordered patterns like aaabbb, qwerty, zyxwvuts, 123321, or the like;
- Choosing passwords that contain any of the above spelled backwards;
- Using passwords that contain standard words preceded or followed by an integer (such as secret1, 1secret, etc.).
- Using the "Remember Password" feature within applications (for example, those available in Internet Explorer, or Google Chrome);
- Writing passwords down;
- Storing passwords in a file on ANY computer system (including PDAs or similar devices) without using encryption methods.

Date Adopted: April 1, 2014 Authorized: 

User Signature _____ Date _____