



# Policy & Procedure

## INFORMATION SYSTEM PASSWORDS

Supersedes:

Date Approved: May 16, 2014

Approved:

David Montgomery, CAO

Page 1 of 1

### Purpose

Passwords are the primary form of user authentication used to grant access to the City of Duluth's information systems. To ensure that passwords provide as much security as possible they must be carefully created and used. Without strict usage guidelines the potential exists that passwords will be created that are easy to break thus allowing easier illicit access to the City of Duluth's information systems, thereby compromising the security of those systems.

### Scope

This Password Policy applies to all information systems and information system components of the City of Duluth. Specifically, it includes:

- Mainframes, servers and other devices that provide centralized computing capabilities.
- SAN, NAS and other devices that provide centralized storage capabilities.
- Desktops, laptops and other devices that provide computing capabilities.
- Routers, switches and other devices that provide network capabilities.
- Firewalls, IDP sensors and other devices that provide dedicated security capabilities.
- Applications and Systems that provide data and user interface capabilities.

### Policy

1. Passwords must be constructed according to set length and complexity requirements. As such passwords must be 8 characters in length and must include three of the following character types: Upper Case Letter, Lower Case Letter, Number or Special Character (@!#\$).
2. Passwords will have both minimum and maximum lifespan. As such, passwords must be replaced at a maximum of 90 days and at a minimum of 2 days.
3. Passwords may not be reused any more frequently than every 10 password refreshes. Reuse includes the use of the exact same password or the use of the same root password with appended or pre-pended sequential characters.
4. Passwords are to be used and stored in a secure manner. As such, passwords are not to be written down or stored electronically. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
5. Passwords are to be individually owned and kept confidential and are not to be shared under any circumstances.
6. Passwords used for non-City systems and applications (websites/personal e-mail) shall not have the City e-mail address as a username along with the same password as any work related passwords

### Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation could result in/or up to written reprimand, suspension or termination.