

SUPERINTENDENT'S REGULATION 1940-R

DISTRICT COMPUTER PASSWORDS



Approved Upon Superintendent's Initials

4/5/12
Date

I. OBJECTIVE

This regulation includes all Rochester City School District (RCSD) faculty, staff, students and all authorized users 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 RCSD facility or has access to the RCSD network. Each user and/or system administrator on the RCSD network is required to implement the password requirements listed in this document.

II. DEFINITIONS

- A. **Authorized User:** Any individual, whether a District employee or not who has been granted permission to access a District server, workstation, networked device or application
- B. **IM&T:** Information Management & Technology
- C. **Password:** A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.
- D. **Special Account:** An account that is permitted privileges above and beyond those of normal users. Examples of this type of account include: root, super user, supervisor, manager, administrator, oracle, etc.
- E. **Strong Passwords:** A strong password is a password that is designed to be hard for a person, program or automated process to discover. It is normally constructed of a sequence of characters, numbers, and special characters. Typically the longer the password the stronger it is.
- F. **System Administrator:** A person who is responsible for properly maintaining a server, workstation, networked device or application.
- G. **Special Character:** A non-numeric and non-alphabet. Common examples include ~!@#\$\$%^&* ()_+=-`';/.,? .

III. PROCEDURE

- A. All passwords must be strong passwords and must be constructed using the following rules.
 - 1. Contain a minimum of eight (8) characters in length
 - 2. Contain characters from at least three of the following four categories:
 - a) English uppercase characters (A through Z)
 - b) English lowercase characters (a through z)
 - c) Base 10 digits (0 through 9)
 - d) Special Characters (e.g., !, \$, #, %)
- B. Passwords **MUST NOT** contain or be:
 - 1. The user's account name or parts of the user's full name that exceed two consecutive characters
 - 2. A dictionary-word spelled forward or backwards.
- C. **Account Lockouts:** Account will be locked after 10 failed attempts to logon. Users are encouraged to use the self-help password reset function before they fail the 10th attempt.
- D. **Password Expiry:** Passwords will expire every 90 days. You will be reminded that your password is near its expiration date to give you an opportunity to change it before it expires.
- E. **Password Retention:** The system remembers the last 6 passwords used and will prevent them from being reused.
- F. **Penalties:** Failure to follow these requirements may result in revocation of privileges to the District Network.
- G. **Screen Lock:** All computers or electronic devices that access District resources such as email, applications, or data, must have an Auto Screen Lock (or equivalent function) active. It must be set so that after 15 minutes of inactivity the Screen Lock will "lock out" anyone attempting the use the computer or device until the appropriate password or passphrase is entered

IV. AUDITING

Passwords will be audited on a periodic or random basis by the IM&T Security Office or their delegates for compliance purposes. If a password is found to not be in compliance with the above guidance during one of these scans, the user will be required to change it. If a password is revealed to have been compromised the user will also be required to change it.