Administrative Regulations
Office of the Mayor
Title: ELECTRONIC SYSTEMS - USER PASSWORDS
A.R. Number: 2.8 **Effective Date:** 2/1/2009 P**age:** 1 of 3
Supersedes: N/A **A.R.:** N/A **DATED:** N/A

I. PURPOSE

The purpose of this policy is to establish a standard for the creation of strong user passwords in the operation of electronic information systems, the protection of those passwords, and the frequency of change. Passwords are an important aspect of computer security. They are the front line of protection for the City of Richmond's (COR) electronic information systems. A poorly chosen password may result in the compromise of the COR's entire organizational network. As such, all COR employees and anyone with access to the COR's electronic systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

II. SCOPE

The scope of this policy includes all employees who have or are responsible for an account (or any form of electronic access that supports or requires a password) on any system that resides at any COR facility, has access to the COR's network, or stores any non-public COR information. The term password applies to User passwords, Application passwords and System level passwords.

III. POLICY

A. General Password Guidelines

1. Passwords are used for various purposes at the COR. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and system level protection. The password must meet the following basic and complexity requirements to ensure that they are strong passwords. All complexity requirements are automatically enforced when passwords are created. The rules enforced are:
    a. May not be based on the user's account name.
    b. Contains at least eight characters.
    c. Contains characters from three of the following four categories:
        i. Uppercase alphabet characters (A–Z)
        ii. Lowercase alphabet characters (a–z)
        iii. Arabic numerals (0–9)
        iv. Non-alphanumeric characters (for example, !$#,%)

2. Passwords cannot be changed to any of the previous 24 passwords which have been used.
3. Passwords can only be changed once a day. If you must change the password more than once, notify your automation coordinator, who, in turn, will notify the DIT help desk or DIT security desk for assistance.
4. All passwords (e.g., email, web, desktop computer, etc.) must be changed periodically according to each system's policy. e.g. Mainframe: every 40 days, Domain (network): every 40 days.
5. Passwords may not be written down or stored on any unencrypted electronic media.
6. All PCs, laptops, and workstations will be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging off (control-alt-delete) when the host will be unattended.

B. Password Protection Standards

1. Do not use the same password for COR accounts as for other non-COR access (e.g., ATM, bank accounts, online purchasing or access, etc.).
2. Where possible, do not use the same password for various COR access needs. For example, select one password for the mainframe and a separate password for the domain.
3. User logons will automatically be revoked if not used for 60 days.
4. User logons will automatically be deleted if revoked for 60 days.

C. Application Development Standards

1. Application developers must ensure their programs contain the following security precautions:
2. Must not store passwords in clear text or in any easily reversible form.
3. Must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

D. Resetting passwords

1. An employee, contractor, or anyone who has been issued a COR User logon has forgotten their password or who have revoked their user logon because of entering incorrect passwords must call the DIT help desk to request the password be reset.
2. In the case of **Application User Passwords**, the employee must submit the reset request to the department Automation Coordinator owning and maintaining the application. It is the responsibility of client departments to ensure an Automation Coordinator and back up Automation Coordinator for the Application User Accounts.

IV. RESPONSIBILITIES

Employees are held responsible to protect their passwords according to this policy. Employees are not to share COR passwords with anyone, including administrative assistants, secretaries, DIT network engineers, or even the DIT Security Administrator. All passwords are to be treated as sensitive, confidential COR information. If an employee suspects their password, or anyone else's password has been compromised they must report this possibility to the DIT Help Desk and their supervisor immediately.

Any employee, contractor, or anyone who has been issued a COR User logon found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

V. DEFINITIONS

Terms	**Definitions**
Application Administration Account	Any account that is for the administration of an application (e.g. Oracle database administrator, ISSU administrator).
User passwords	A unique part of the client's login to allow access to an electronic information network or an application.

V. DEFINITIONS *(continued)*

Terms	**Definitions**
Application User passwords	Application User passwords are unique to an individual and maintained by the Automation Coordinator in the client's department. They are typically part of logins in purchased applications or applications built by DIT; but with the functionality for the client department to administer the users.
Application passwords	Application passwords are unique to a computer application. They are part of the application's login to access application data or permission data from inside a program and invisible to the client
System passwords	System passwords are unique to a piece of hardware or networking device. They are part of the networking staff's login to allow access to system files/configuration/permissions.
Strong passwords	Strong passwords not easily deciphered by anyone except the owner of the password.

VI. REGULATION UPDATE

The Department of Human Resources and the Department of Information Technology shall be responsible for modifications to this Policy.

APPROVED:

MAYOR