



Draft

Information Technology Department

Best Practice 12.18

Password Management Policy

Purpose

The conscientious management of administrative password practices is a critical element for information security of the enterprise. The purpose of this policy is to establish a standard for the creation, use, change and protection of strong passwords within the City network and systems.

Applies To

The scope of this policy includes:

- All personnel with an account on any application or system within the City of Grand Rapids
- All individuals who have access to the City of Grand Rapids Network
- All systems that store any non-public information

Policy Statement

Passwords are an essential aspect of computer security and provide an important front-line protection for electronic resources by preventing unauthorized access. Passwords also help the City limit unauthorized or inappropriate access to various resources, including user-level accounts, web accounts, email accounts, and other City application access. Poorly chosen passwords may result in the compromise of City systems, data or network. Therefore, all City users are responsible for taking the appropriate steps, as outlined below, to select appropriate passwords. Contractors and vendors with access to City systems are also expected to observe these requirements.

The Information Technology Department, a City Department and/or system administrator may implement a more restrictive policy on departmental systems where deemed appropriate or necessary for the security of electronic information to protect confidential data.

Practice:

Creation of Passwords

Passwords created by users should conform to the following guidelines:

- Must be different than the user's login name or the reverse of the name and must avoid use of knowledgeable personal information (names of family, etc.).
- Must be at least eight characters.
- Must include at least one or more numeric digit (0-9)
- Must include at least one or more upper and lower case character (a-z, AZ)
- Must include at least one or more special character (for example,* & % \$)

These provisions will be enforced electronically whenever possible.

Changing passwords

Passwords will be required to change once every 90 days. The new password must differ from all passwords used within the past year.

Protecting a password

Protecting passwords should conform to the following guidelines:

- Passwords should be treated as confidential City information
- Passwords should never be written down or posted for reference
- Passwords should not be included in email messages or other forms of electronic communication
- Passwords should not be posted to City websites, portals or other shared storage spaces

Sharing a password

Sharing or allowing another person to use an individual account password is a violation of this policy.

Departmental system account passwords should only be shared with appropriate departmental personnel.

Passwords may be shared via phone when necessary. *However*, users need to beware of "Phishing" or other social engineering scams where a user may have his or her password requested over the phone. Information Technology personnel, as a best practice, do not normally request a user's password over the phone. Phone communications may be necessary with external information technology vendors, and care should be used when these vendors request user account and password information. It is strongly recommended that passwords be changed after allowing use as permitted in this section.

The preferred method for vendor access to departmental systems is to request a temporary or annual account for the vendor from Information Technology. Annual accounts will be set to expire a year from the creation, and will require contact to ITSUPPORT@GRCITY.US to renew the account for another year.

Reporting a password compromise

Any suspected compromise of passwords must be reported immediately to Information Technology at 456-3999 or 456-4357. The password in question should be changed immediately.

Responsibilities of Information Technology Department

Information Technology may require a more restrictive policy, such as stronger passwords, in some circumstances.

Information Technology or its delegates may perform password assessments on a periodic or random basis. If a password is guessed or cracked during one of these assessments, Information Technology will promptly notify the listed contact and require that the password be changed.

Violations of Policy

An individual who violates this policy may immediately lose computer or network access privileges.

Administrative Passwords

Administrative passwords conform to other special considerations. The master enterprise password will only be entrusted to the IT Director and the Network Operations Administrator. All administrative positions within the directory will have individual login and passwords assigned and restricted to support their daily administrative functions only. Other special administrative account considerations are as follows:

- Server administrators will have an individual administrator account which will be restricted to the individual servers within their purview.
- Network administrators will have their individual administrator account placed into the Active Directory Switch Administrators group.
- Desktop administrators will have an individual administrator account placed into the Active Directory Workstation Administrators group.
- Specialized systems (disk systems, etc) will have administrative accounts created which, where possible, will not provide the capability for any single user to change the rights of other accounts. Where this is the case, the Network Operations Administrator will make the determination on the system setup.
- Administrative passwords will follow this password management best practice.
- Only the Network Operations Administrator and the IT Director shall have rights to create new administrative logins.
- A regular audit of administrative logins will be reviewed and approved by the Network Operations Administrator and/or IT Director.