BTS-2.05 - User & Administrative Passwords

USER & ADMINISTRATIVE PASSWORDS

Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.05

Purpose

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may easily result in the compromise of the City's entire network. As such, all City employees (including contractors and vendors with access to City systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, the association of passwords with user accounts and the frequency of password changes.

The scope of this policy includes all personnel 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 City facility, has access to the City network, or stores any non-public City information.

Administrative Rule

• Each approved City user is to be issued a unique user account and password. In general, sharing of user accounts and passwords is prohibited. BTS will work with bureaus who request an exception to this rule or to assist them in implementing more secure methods to address requirements met by sharing user passwords.

• All shared administrative or system-level passwords (e.g., root, enable, administrator, application administration accounts, etc.) must be changed at least once every 90 days or immediately when an employee with knowledge of the password terminates employment with the City or is reassigned to responsibilities in which such knowledge is no longer required.

• All user-level passwords (e.g., network login, email, web, desktop computer, etc.) must be changed at least every 90 days. Note: User accounts with access to data protected under legal regulations such as Criminal Justice Information Systems (CJIS) Policy, etc., may be subject to more restrictive password requirements.

• User accounts that have system or administrative level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user. Additionally, all such passwords must be changed at least once every 90 days.

• System level/administrative access and general user access must be conducted via separate and unique user accounts. Systems operators must not use system or administrative level accounts for general office use (reading email, browsing the internet, etc). General office access must be accomplished via non-system level accounts. This does not apply to users specifically granted administrative level access to their personal workstation.

• Passwords must not be inserted into email messages or other forms of electronic communication. Leaving a password as a message on a users confirmed voicemail is acceptable, however care must be taken to make sure such passwords are not overheard by anyone other than the intended recipient.

• Where supported by the system, all passwords must be at least 8 characters in length and contain at least 3 of the following 4 characteristics:

o Lowercase letters (ex. a, b, c)
o Uppercase letters (ex. A, B, C)
o Numbers (ex. 1, 2, 3)
o Special characters (ex. !, @, #)

• Where supported by the system, all accounts must be automatically locked out after no more than 6 incorrect password attempts within a 30 minute time window and must remain locked for a minimum of 30 minutes unless unlocked by authorized BTS support personnel.

• Where supported by the system, all new passwords must not be a repeat of a previously used password within the last 10 password change events.

• Where supported by the system, all workstations and file servers must implement an automatic password protected screen saver after no more than 15 minutes of keyboard or mouse inactivity.

• Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

- When a user account is created with a default password, or is reset by authorized BTS personnel, the password must be set to expire and be changed at the next logon.

- If someone demands you reveal your password, do not do so. Refer them to this document or have them call the BTS Helpdesk in order to appropriately request access to City information systems and/or data.

- If an account or password is suspected to have been compromised, report the incident to BTS Helpdesk and change all passwords immediately.

Guidelines

Password Construction

Passwords are used for various purposes at the City. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection and network equipment logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "portland ", "seattle ", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords

Password Protection

Do not use the same password for City systems as for other non-City systems (e.g., external email, etc.). Where possible, don't use the same password for various City access needs. For example, select one password for a specific application and a separate password for the network system. Also, select a separate password to be used for a Windows account and a Unix account.

Here is a list of "don’ts":

- Don't reveal a password over the phone to anyone
- Don't reveal a password in an email message
- Don't reveal a password to your boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members or friends
- Don't reveal a password to co-workers while out sick, traveling or on vacation

In general, it is not advised to use the "Remember Password" feature of applications (e.g., Internet Explorer, etc) as these leave your password vulnerable on the systems they are stored. This is of particular concern on shared systems such as kiosks. Where a City application has a specific ability to retain a password, this function may be used understanding the above mentioned risks.

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on any computer system (including a portable computing device) without BTS approved encryption technologies.

Compliance
Password cracking or guessing, using commonly available methods, may be performed by the Information Security Office on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it immediately.

HISTORY

Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.