



BTS-2.05 - User & Administrative Passwords

Administrative Rules Adopted by Bureaus Pursuant to Rule Making Authority (ARB)

Search Code, Charter, Policy

Policy category: [Information Security](#)

Policy number: BTS-2.05

Keywords

Search

USER & ADMINISTRATIVE PASSWORDS

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

ARB-BTS-2.05

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.

Revised rule adopted by Chief Technology Officer November 15, 2013.

Revised rule adopted by the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD October 29, 2015.


This rule was reviewed as part of a periodic review and remains unchanged. July 13, 2017.

This rule was reviewed as part of a periodic review and remains unchanged. April 30, 2018.

Revised by Chief Technology Officer October 10, 2018.

This rule was reviewed as part of a periodic review. September 1, 2021.

Related documents

 [BTS-2.05 User & Administrative Passwords Administrative Rule](#) 112.02 KB

BTS-2.05 - Authorized User & Administrative Passwords

AUTHORIZED USER & ADMINISTRATIVE ACCOUNT 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 information technology security. Strong passwords are the front line of protection for Authorized User accounts. A poorly chosen password may easily result in the compromise of the City's entire Technology Resources. As such, all Authorized Users are responsible for taking the appropriate steps, as outlined below, to select and secure strong passwords.

The purpose of this policy is to establish a best practices-aligned standard for the creation of strong passwords, the protection of those passwords, the association of passwords with Authorized User accounts and the requirements for password changes and audits.

The scope of this policy includes all Authorized Users who have or are responsible for a City technology access account, regardless of device used or the location of the access account.

Administrative Rule

Password Standard Update

The City of Portland has updated City Password standards to align with the National Institute of Standards and Technology (NIST) Special Publication 800-63-3 - Digital Authentication Guidelines: <https://pages.nist.gov/800-63-3/sp800-63b.html>, or as revised.

Each Authorized User is issued a unique City domain account and password. In general, sharing Authorized User accounts and passwords is prohibited. The Bureau of Technology Services (BTS) will work with bureaus who request an exception to this rule or to assist in implementing secure methods to address requirements met by sharing user accounts or passwords for limited access use cases.

See *City of Portland Information Security Standards, section 4.2 Password Requirements* for standards and use guidance.

1. Authorized Users are not permitted to reveal their passwords.
2. If an account or password is suspected to have been compromised, an Authorized User must report the incident to the BTS Helpdesk and change the password immediately.

Password Protection

Reuse of City credentials and passwords is prohibited for non-City systems and Internet-based services (e.g., external email, etc.). City domain passwords must not be used for non-City purposes unless these accounts are managed through BTS' enterprise account technologies (e.g. Active Directory (AD), Active Directory Federation Services (ADFS), or Single Sign-On (SSO) services).

Use of a password manager is recommended for secure storage of all City Authorized User passwords and account credentials.

1. KeePass is a BTS-approved standard. Contact BTS HelpDesk for guidance on authorized software installation and appropriate use.

Do not write passwords down or store them anywhere in your workspace. Do not store passwords in a file on any storage device without BTS approved encryption technologies.

Here is a list of "don'ts":

1. Don't reveal a password over the phone to anyone. BTS personnel will never ask for your passwords
2. Don't reveal a password in an email or text message
3. Don't reveal a password to your supervisor
4. Don't talk about a password in front of others
5. Don't hint at the format of a password (e.g., "my family name")
6. Don't reveal a password on questionnaires or forms
7. Use caution when completing on-line forms that request current or new passwords. Submission forms may be intercepted
8. Don't share a password with family members or friends
9. Don't reveal a password to co-workers while out sick, traveling or on vacation

Do not use the "Remember Password" feature of technology applications and services (e.g., Microsoft Edge, etc.) as these leave your password vulnerable on the systems they are stored. This is a high-level security concern on shared systems such as kiosks or on an open wireless (Wi-Fi) network.

Password Discovery and Hardening

Password cracking or guessing 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 Authorized User will be required to change their password immediately.

References

Please refer to the following BTS resources for term definitions, acronyms, and BTS standards used within BTS Admin Rules:

- 1) BTS Technology Definitions –
<https://www.portlandoregon.gov/citycode/article/114449>
- 2) (BTS) Technology Standards Directory (and Acronyms) --
<https://www.portlandoregon.gov/bts/article/44978>
- 3) [City of Portland Security Standards](#)

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.

Revised rule adopted by the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD October 29, 2015.

This rule was reviewed as part of a periodic review and remains unchanged. July 13, 2017.

This rule was reviewed as part of a periodic review and remains unchanged. April 30, 2018.

This rule was reviewed and revised as part of a periodic review. September 2, 2019.

This rule was reviewed and revised as part of a periodic review. June 30, 2020.

This rule was reviewed as part of a periodic review. September 1, 2021.