BTS-2.06 - Database Passwords

DATABASE PASSWORDS
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.06

Purpose
This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a software program or application that will access a database running on a City network or on City Technology Resources hosted outside of City networks.

Technology applications and services often require the use of database servers. To access these databases a software application or service must authenticate to the database by presenting authorized credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

This policy applies to all technology applications and services that access City Technology Resources production databases using stored credentials. An example of this scenario is a web server or batch processing system authenticating to a database server for the purpose of processing database queries on behalf of an Authorized User. This policy supersedes Bureau of Technology Services (BTS) Administrative Rule 2.05 AUTHORIZED USER & ADMINISTRATIVE PASSWORDS.

Database Password strength is governed by BTS Administrative Rule 2.05 AUTHORIZED USER & ADMINISTRATIVE ACCOUNT PASSWORDS, and *City of Portland Information Security Standards, section 4.2 Password Requirements.* BTS will work with bureaus who request an exception to this rule or to assist in implementing secure methods to address database password requirements.

Administrative Rule

General
To maintain the security of the City's internal or hosted databases, access by technology software applications and services must be granted only after authentication with valid credentials. The credentials used for this authentication must not reside in the main, executing body of the software application or service's source code in clear text. Stored authentication credentials must remain encrypted.

Specific Requirements

Storage of Database Usernames and Passwords
1. Database usernames and passwords must be stored in a file separate from the executing body of the program's code. This file must not be world/everyone readable.

2. Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
3. Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP (Lightweight Directory Access Protocol) server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
4. Database credentials must not be stored in a location that can be accessed externally through a web browser.
5. Passwords or pass phrases used to access a database must adhere to BTS Rule 2.05: AUTHORIZED USER & ADMINSTRATIVE PASSWORDS.

Retrieval of Database Usernames and Passwords

1. If stored in a file that is not source code, then database usernames and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the username and password must be released or cleared.
2. The scope into which database credentials may be stored must be physically separated from the other areas of code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the username and password) and any functions, routines, or methods that will be used to access the credentials.
3. For languages that execute from source code, the credentials' source file must not reside in the same browse-able or executable file directory tree in which the executing body of code resides.

Access to Database Usernames and Passwords

1. Each technology application and service function accessing a City managed or hosted solution (SaaS) database must have unique database credentials. Sharing of credentials between programs is not allowed.
2. Database passwords used by programs are system-level passwords as defined by BTS Rule 2.05: AUTHORIZED USER & ADMINSTRATIVE PASSWORDS.
3. Database usernames and passwords used by technology software applications, services or programs, such as a web server connecting to a database, must not also be used for interactive sessions by end users or system operators.
4. Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with BTS Rule 2.05: AUTHORIZED USER & ADMINSTRATIVE PASSWORDS. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.
5. Access to database usernames and passwords MUST be from a limited number of authorized administrative endpoints and use MFA unless by exception.

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 Information Security Standards

History

Authorized by Ordinance No. 179999 passed by Council March 15, 2006 and effective April 14, 2006.
This rule was reviewed as part of a periodic review and remains unchanged, 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.