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 program or application that will access a database running on one of the City's networks.

Computer programs running on the City's networks often require the use of one of the many internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable 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 programs and applications that will access a City, multiuser production database using a stored credential. 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 a user. This policy does not apply to interactive end-user or administrative passwords used to access City applications or databases which are covered by Rule 2.05 END USER & ADMINISTRATIVE PASSWORDS.

Administrative Rule

General
In order to maintain the security of the City's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text.

Specific Requirements

Storage of Database User Names and Passwords
- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world/everyone readable.
- 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.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP 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.
- Database credentials must not be stored in a location that can be accessed externally through a web browser.
- Passwords or pass phrases used to access a database must adhere to BTS Rule 2.05: USER & ADMINSTRATIVE PASSWORDS.

Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
- The scope into which you may store database credentials 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 user name and password) and any functions, routines, or methods that will be used to access the credentials.
- 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 User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by BTS Rule 2.05: USER & ADMINSTRATIVE PASSWORDS.
- Database user names and passwords used by programs, such as a web server connecting to a database, must not also be used for interactive sessions by end users or system operators.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with BTS Rule 2.05: USER & ADMINSTRATIVE PASSWORDS. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

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.