
# Database Credentials Standard

*(Last Updated April 2025)*

## Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Bitra Immigration and Border Services's (BIBS) networks. Software applications running on BIBS's networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

## Scope

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the BIBS Network. This policy applies to all software (programs, modules, libraries or APIS that will access a BIBS, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they don't always use sanitized information.

## Safeguards

### General

In order to maintain the security of BIBS'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 or easily reversible encryption. Database credentials must not be stored in a location that can be accessed through a web server. Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

**Specific Requirements**
Storage of Data Base Usernames and Passwords

- Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
- Database credentials may reside on the database server. In this case, a hash function 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 may not reside in the documents tree of a web server.
- Passwords or pass phrases used to access a database must adhere to the Password Policy.

**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 your 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 browsable or executable file directory tree in which the executing body of code resides.

**Access to Database Usernames 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 the Password Policy.

Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Users and/or software accessing sensitive data must be subjected to proper access control and should not be able to perform privileged operations that are out of scope of said user and/or software.

**Coding Techniques for Implementing this Policy**
*[Add references to your site-specific guidelines for the different coding languages such as Perl, JAVA, C and/or Cpro.]*

## Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.