DATABASE CREDENTIALS CODING POLICY

Document Name:	**Database Credentials Coding Policy**	
Current Version:	V1.4	
Prepared by:	Shuila Binti Mohd Shahid	**Signature:** 
Approved by:	Barry Chai, CTO	**Signature:** 
Last Updated:	26th February 2024	
Confidentiality Level	Confidential	

Database Credentials Coding Policy

1. Overview

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

2. 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 TimeTec Cloud's AWS networks.

Software applications running on TimeTec Cloud's networks may require access to one of the many internal database servers. In order to access these databases, a program shall 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.

3. 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 TimeTec Cloud AWS Network. This policy applies to all software (programs, modules, libraries or APIs that will access a TimeTec Cloud, 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.

4. Policy

General

In order to maintain the security of TimeTec Cloud's AWS databases, access by software programs shall be granted only after authentication with credentials. The credentials used for this authentication shall not reside in the main, executing body of the program's source code in clear text. Database credentials shall not be stored in a location that can be accessed through a web server.

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 shall 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 shall 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 shall be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password shall be released or cleared.

- The scope into which you may store database credentials shall be physically separated from the other areas of your code, e.g., the credentials shall be in a separate source file. The file that contains the credentials shall 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 shall not reside in the same browsable 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 shall 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 shall have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process shall include a method for restricting knowledge of database passwords to a need-to-know basis.

Coding Techniques for implementing this policy

- Please refer to the following Google Doc for the best coding practices for TimeTec Cloud.
  - https://docs.google.com/spreadsheets/d/1YEYYvCfMpmfCZIg68R_hGoUw9Qc66fSzwUVycm-i4qc/edit?usp=sharing
- Developer Guide
  - https://drive.google.com/open?id=10QiiMceAV6z9vQAf9X459OAvPi6S2ak5s6d8QXrWWbM

- .Net Secure coding guideline
- OWASP Secure Coding Practices-Quick Reference Guide | OWASP Foundation

5. Policy Compliance

5.1. Compliance

The IT Operation will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.1. Exceptions

Any exception to the policy must be approved by the CTO in advance.

5.2. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Revision History

Version	Date of Change	Prepared by	Summary of Change
1.0	1st August 2017	Barry Chai	1st Baseline
1.1	13th August	Barry Chai	Added Google Doc URL & Developer's Guide for the coding technique.
1.2	27th October 2017	Barry Chai	● Remove "Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host." ● Updated the URL for the coding guide
1.3	27th September 2022	Shuila Mohd Shahid	Added reference for coding guideline ● .Net ● OWAPS
1.4	26th February 2024	Shuila Mohd Shahid	Change to 'may' to 'shall'