Database Credentials Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	29/01/2019
V 0.2	Andrew Clarke	Recommendations from AF (Dev)	05/02/2019
V 1.0	Andrew Clarke	Approved InfoSub Committee	15/04/2019

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering Database Access controls.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Chief Information Security Officer / Chief Information Officer	Responsible for approving exceptions to the Database Access Policy
Systems Manager	Is responsible for maintaining and managing Database Access policies on IT systems and infrastructure.
Network Manager	Is responsible for maintaining and managing Database Access policies on network systems.
Head of Development and Application Services	Is responsible for maintaining and managing Database Access policies on application and web systems.
Application Owners	Is responsible for maintaining and managing Database Access policies on applications.
Cyber & Information Security Manager	Is responsible for maintaining Database Access policy best practice and ensuring compliance with legislative and regulatory requirements.
All Users	Are responsible for ensuring Database Access are chosen that remain compliant with this Policy.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A9 – Access Control
ISO 27001:2013 Conformance Control	Information Classification Objective A.9.3.3 Password Management System

1.4 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 Brunel University Network. This policy applies to all software (programs, modules, libraries or APIS that will access a Brunel University production database. It is recommended that similar requirements be in place for non-production servers and mobile environments since they don't always use sanitised information.

1.5 References

BUL-POL-9.3.3 - Password Policy

1.6 Policy Objectives

Database authentication credentials are a necessary part of authorising 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 University.

1.7 Policy Overview

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 Brunel University's networks.

Software applications running on Brunel University'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.

1.8 Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an ongoing basis by Brunel University London. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from Brunel University London intranet (IB) or other relevant communication media on an ongoing basis and accept the terms and conditions contained therein.

2.0 Database Access controls Policy

2.1 General

In order to maintain the security of Brunel University'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. Database credentials must not be stored in a location that can be accessed through a web server.

2.2 Specific Requirements

Storage of Data Base User Names and Passwords

- Passwords MUST NEVER be stored in clear text in any application or on any system.
- Passwords MUST NOT be transmitted in clear text format over the network, and NEVER together with the User ID in the same message or email.
- Passwords MUST be stored as a HASHED[1] string using either MD5, SHA-1 or SHA-2 algorithms with SALT[2] for additional security.
- If Hashing cannot be done, (i.e. when it is a necessity to decrypt the password) the password must be encrypted using FIPS 140-2 Compliant Algorithms (BUL-POL-10.1 - Cryptographic Policy) i.e. Symmetric Key - AES, Triple-DES, Escrowed Encryption Standard; Asymmetric Key (public-key) DSA, RSA, ECDSA
- 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 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.
- Configuration of a Database-driven web application must ensure that it is not possible to retrieve content of files containing credentials through the web servers.
- Access to the database must not be permitted based exclusively on a remote user's authentication on the remote host. (This precludes the use of Oracle OPS$ authentication.)
- Passwords or pass phrases used to access a database must adhere to the University *Password Policy*.
- Authentication Credentials must not appear in source code of a compiled

[1] Hashing is an ideal way to store passwords, as hashes are inherently one-way in their nature. By storing passwords in hash format, it's very difficult for someone with access to the raw data to reverse it (assuming a strong hashing algorithm and appropriate salt has been used to generate it).
[2] Salting is the randomising of the hashes by appending or prepending a random string.

application as per Good Software Development Practice. However, in the case of an application written in an interpreted language, in lieu of a dedicated configuration parser, a source code file containing credentials but no code may be referenced by the application.

Retrieval of Database User Names and Passwords

- Where possible, the memory containing the user name and password must be released or cleared when no longer required. This is typically enforced by the OS upon termination of the process.

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. This is to ensure that potential disruption is avoided when either credentials are updated or compromised.
- All database users, standard and administrative, are to be configured in accordance with the BUL-POL-AUP - Acceptable Use Policy principle of least privilege (PoLP) which is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work. Under PoLP, database users will be granted permission to read, write or execute only the files or resources they need to do their jobs: In other words, the least amount of privilege necessary. Administrative privileges are only given to those authorised by IS, College IT or InfoSec with justifiable reasons.
- 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.

3.0 University Confidential Information and MS Access

University Confidential Information including Personal Data and Personal Sensitive Data must not be stored in local, unsecure, MS Access databases.

MS Access is not secure (admin security for an Access dB is flawed, Password-protecting the Admin account gives an extremely false sense of security).

4.0 Policy Compliance

4.1 Compliance Measurement

The Cyber & InfoSec team 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.

4.2 Exceptions

Any exception to the policy must be approved by the CISO or CIO advance.