

Quality Document		Kinyo Virginia, Inc.		
Database Credentials Policy			Issue: ITP007	
Date: 05/05/2022	Approved: F. Koshiji	Issued By: I.T. Department	Revision: 001	Page: 1 of 1

1. Overview

Database authentication credentials are necessary part of authorizing application to connect to internal databases, however, incorrect use, storage and transmission of such credentials could lead to compromise of 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 password (database credentials) for use by program that will access a database running on one of Kinyo networks.

3. Scope

This policy is direct at all systems implementer and applications that will access a production database server on the Kinyo network. This policy applies to all software (programs, modules, libraries or APIS that will access a Kinyo), multi-user production database.

4. Policy

To maintain the security of Kinyo internal databases, access by software programs must be grant only after authentication with credentials.

Access to Database Usernames and Passwords

- Database passwords used by programs are system-level passwords as defined by the Password Policy.
- I.T. department must have a process in place to ensure that database passwords are control and changed in accordance with the Password Policy, ITP012. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

5. Policy Compliance

5.1 Compliance Measurement

The I.T. team will verify compliance to this policy through various methods, including but not limit to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exceptions to the policy must be approved by the I.T. team in advance.