This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the

Database Security Standard Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press "Ctrl" + "H" keys simultaneously.
- Enter "<organization name>" in the Find text box.
- Enter your organization's full name in the "Replace" text box.
- Click "More", and make sure "Match case" is ticked.
- Click "Replace All".
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This standard aims to define the detailed cybersecurity requirements related to <organization's name>'s Database Management System (DBMS) هي in order to minimize cybersecurity risks resulting from internal and external threats at <organization's name>.

The requirements in this standard are aligned with the Database Security Policy and the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This standard covers all <organization name>'s information technology assets (including DBMS) and applies to all personnel (employees and contractors) in <organization name>.

Standards

1	Secure Hardening Configuration
Objective	To define basic DBMS security requirements to ensure that the DBMS is securely designed, configured, and operated.
Risk Implication	Faults in DBMS configuration and weak designs are among the top reasons leading to security vulnerabilities that can be exploited to jeopardize the confidentiality, integrity, and availability of <organization name>'s data.
Requirements	
1-1	Naming conventions must be different to distinguish between production and non-production servers.
1-2	DBMS servers must be dedicated and must not host any other functionality such as "Web or Application Tier" or "Domain Services."

1-3	Default database table names must be changed; must not be limited to the tables only & address all default configurations.
1-4	Only stored and available procedures for the application must be used to make transactions or queries from the database.
1-5	DBMS servers links (such as creating connections or interfaces) must be isolated between production and non-production DBMS(s).
1-6	Data validation must be used to ensure the integrity of stored data.
1-7	Database fields must be limited to specific ranges of input and queries. In addition, dual input, or other input checks (such as Boundary Checking and Content Inspection/URL Filtering) must be used to limit transactions such as: • Missing and/or incomplete data • Out of range values • Unauthorized or inconsistent data • Invalid characters in data fields • Exceeding upper or lower date volume limits
1-8	Access to all DBMS configuration files, as well as to the source code of applications/scripts stored in the database, must be controlled, and monitored.
1-9	An accurate inventory of all databases and their contents must be maintained and regularly updated & reviewed.
1-10	Data stored in databases must be labeled using predefined types of security labels as per <organization name>'s relevant policies and procedures; and related controls must be applied.
2	**Audit Logs**
Objective	To generate DBMS logs for critical security events, and record and secure them on the DBMS to help with future investigations, tracking, and verifications.

Risk Implication	Insufficient audit logs limit <organization name>'s ability to detect security compromises, incidents, and issues and track them on the DBMS, and undermine its ability to determine the causes of such security compromises. Failing to properly secure audit logs on the DBMS can lead to tampering with logs, thereby impacting their integrity.
Requirements	
2-1	All DBMS clocks must be synchronized with centrally trusted Network Time Protocol (NTP) source.
2-2	Logs must be appended to the operating system logs or be self-contained within the DBMS.
2-3	Audit records containing detailed information must be generated to establish the identity of any user/subject or process associated with the event.
2-4	The following DBMS activities must be recorded and logged at minimum mention changes on DB record level and the timestamp of the event: • All raised system alarms or errors • Start up • Shutdown • The creation, alteration, or deletion (drop) of databases, and any database storage structures, tables, indexes, accounts and objects • Enabling and disabling of audit functionality • Granting and revoking of DBMS system level privileges • Any action that returns an error message because the object referenced does not exist • Any action that renames a DBMS object • Any action that grants or revokes object privileges from a DBMS role or account • All modifications to the data dictionary or DBMS system configuration

	• Audits of all DBMS connection failures where possible. DBA must ensure that both successful and unsuccessful connection attempts are audited • Stating a threshold and triggering alert of failed logon attempts, and password locks • Attempts to add, modify or delete privileges/permissions • Deletion of categories of information (such as classification levels/security levels) • Abnormal command (command calling another command, etc.) • Disabling or modifying DBMS's logs
2-5	An immediate real-time alert must be raised to appropriately support individuals with all audit failure events requiring real-time action(s).
2-6	Audit features in the DBMS must be protected against unauthorized removal.
2-7	DBMS must be configured to send the event logs to SIEM in accordance with the <organization name>'s approved cybersecurity event and logging standard.
3	Other Standards
Objective	To implement all database security standards and requirements to ensure the highest protection levels.
Risk implication	Failure to implement all security standards and requirements exposes <organization name> to increasing database security risks.

Requirements	
3-1	The following standards must be implemented: 1- Identity and access management standard 2- Disaster recovery and backup standard 3- Cryptography standard 4- Server security standard 5- Physical security standard

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>
2- **Standard Review and Update:** <cybersecurity function>
3- **Standard Implementation and Execution:** <information technology organization>
4- **Standard Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.
2- All employees at <organization name> must comply with this standard.
3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.