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 outlined image.

Database Security Policy 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 policy aims to define the cybersecurity requirements related to the protection of <organization name>'s databases to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at <organization name> in order to preserve confidentiality, integrity and availability.

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

Scope

This policy covers all <organization name>'s information and technology assets (including Database Management Systems (DBMSs)) and applies to all personnel (employees and contractors) in the <organization name>.

Policy Statements

1 General Requirements

1-1 DBMSs used in <organization name> must be defined and documented.

1-2 A proper secure environment must be provided for DBMSs to protect them against operational and environmental risks in line with database classification.

1-3 DBMSs technical security standards for <organization name>'s DBMSs must be developed and approved, and they must be implemented by the Database Administrators (DBAs).

1-4 Users' direct access to and handling of databases must be restricted to DBAs only and through applications only based on authorized access while implementing security solutions that limit or prohibit DBAs from accessing classified data, as per <organization name>'s approved Identity and Access Management Policy.

1-5 Database access, review, or modification privileges must be granted according to <organization name>'s approved Identity and Access Management Policy.

1-6 The requirements of all <organization name>'s approved policies related to configuration and hardening security must be implemented, including but not limited to the following policies:

1-6-1 <organization name>'s approved Server Protection Policy.

1-6-2 <organization name>'s approved Malware Protection Policy.

1-6-3 <organization name>'s approved Physical Security Policy.

1-7 Copying or transferring the data of critical systems' databases from the production environment to any other environment must be prohibited unless the necessary tests are conducted.

1-8 Key Performance Indicators (KPIs) must be used ensure the continuous improvement and effective and efficient use of the database protection requirements.

2 Database Hosting Security Requirements

2-1 Business continuity and disaster recovery requirements must be defined for hosted databases in the relevant contracts with the cloud service providers as well as including respective roles and responsibilities regarding plans, backup tests, incident response, and disaster recovery, etc.

2-2 Logical and physical isolation must be provided between <organization name>'s databases and other hosted databases, especially for critical databases, in line with database classification.

2-3 The secure configuration and hardening of <organization name>'s databases must be reviewed periodically, at least once every year.

2-4 Administrative access to databases must be restricted using a solid encryption method, such as the Secure Shell Protocol (SSH), Virtual Private Networks (VPN), the Secure Sockets Layer (SSL),Transport Layer Security (TLS), or a Multi-Factor Authentication (MFA), as per <organization name>'s approved Cryptography Policy.

3 DBMS Change Management Requirements

3-1 Changes to databases (such as database migration and transfer to a production environment) must follow <organization name>'s approved change management process.

3-2 DBMS must be patched and updated as per <organization name>'s approved Patch Management Policy.

3-3 Trusted, approved, and licensed DBMSs must be used upon update or change.

3-4 A clear DBMS disaster recovery plan must be in place, and it must be reviewed and tested annually.

3-5 Service Level Agreements (SLAs) must be signed with vendors for DBMSs in the production environment.

3-6 Hashing and encryption must be applied to databases during transmission and storage as per <organization name>'s approved Classification Policy and Cryptography Policy.

4 DBMS Event Log Monitoring

4-1 DBMS event logs must be enabled and maintained as per <organization name>'s approved Cybersecurity Event Logs and Monitoring Management Policy.

4-2 <cybersecurity function> must consistently monitor database event logs and users' behavior.

4-3 <cybersecurity function> must consistently monitor DBA-related event logs and behavior and review them every six months at least.

5 Operational Requirements

5-1 <information technology organization> must monitor operational DBMSs, and ensure the quality of their performance, their availability, and the availability of sufficient storage capacity, etc. It must also back up the databases.

5-2 Clock Synchronization must be ensured centrally for all DBMSs.

5-3 The requirements of <organization name>'s approved Backup and Recovery Policy must be implemented.

Roles and Responsibilities

1- **Policy Owner:** <head of cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <information technology organization> and <cybersecurity function>

4- **Policy Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy 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- <head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.

2- All personnel of <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action according to <organization name>'s procedures.