Database Administration Guidelines

This document provides database management guidelines that serve as a foundational framework for ensuring that government institutions handle their data effectively, securely, and in compliance with regulatory standards. These guidelines encompass various principles, practices, and protocols aimed at optimizing database performance, safeguarding sensitive information, and fostering transparency and accountability.

    - Network separation [Recommended]
    - Separation of development, testing and production database servers [Mandatory]
    - Security hardening [Mandatory]
    - Access control [Mandatory]
    - Default passwords[Mandatory]
    - DBMS Versions and security updates [Mandatory]
    - Encryption [Mandatory]
    - Protecting database contents [Mandatory]
    - Monitoring and database events logging [Recommended]
    - Security standards and guidelines [Mandatory]

- Database maintenance
    - Performance monitoring and tuning [Recommended]
    - Change management [Mandatory]
    - Documentation [Mandatory]

- 7 Disaster recovery and business continuity management
    - Data backup and recovery strategy process [Mandatory]

- Data retention
    - Data retention policies [Mandatory]
    - Data purging [Recommended]

Introduction

In today's digital age, where information is pivotal for decision-making and public service delivery, government institutions are increasingly reliant on database management systems to manage and maintain vast amounts of data efficiently as part of digitisation. Whether it's citizen information, financial records, or administrative data, the integrity, security, and accessibility of these databases are critical for the functioning of government agencies.

This document provides database management guidelines that serve as a foundational framework for ensuring that government institutions handle their data effectively, securely, and in compliance with regulatory standards. These guidelines encompass various principles, practices, and protocols aimed at optimizing database performance, safeguarding sensitive information, and fostering transparency and accountability.

Scope and applicability

These guidelines aim to provide best practices for effective Database Management Systems (DBMS) implementation and maintenance within Government institutions. They encompass various aspects of database administration, including planning, design, security, performance and disaster recovery. They apply to all Government institutions in Rwanda and all IT staff and contractors responsible for implementing and managing database systems should comply with the guidelines.

Selecting a DBMS

Government institutions should follow the software lifecycle guidelines when procuring and implementing database management systems. In particular, the following should be considered when selecting a DBMS:

Data model [Recommended]

Determine the appropriate data model for your DBMS such as relational or NoSQL based on the nature of the data and how it will be used. Relational DBMS tend to be used for structured data while NoSQL supports unstructured or semi-structured data.

DBMS Choice [Mandatory]

- Evaluate different DBMS technologies based on the institution's requirements. Consider factors such as scalability, performance, data consistency, and data security when choosing technologies.
- It is recommended that Government institutions in Rwanda should choose mature systems such as PostgreSQL, SQL, MySQL, MongoDB or Oracle DBMS. The acquisition process should follow the RISA Software Lifecycle management guidelines.

Database storage and hosting

The following guidelines on storage and hosting should be followed when implementing DBMS systems:

Database hosting location [Mandatory]

Database systems and applications should be hosted in the data hosting environment officially adopted by the Government as guided by RISA. The institution should ensure that they subscribe to a minimum hosting plan that includes daily backups and disaster recovery services.

Migration of critical database systems [Mandatory]

For critical database systems and applications hosted on premises, the government entity should immediately consult RISA to devise a road map for migration to the official Government hosting environment .

Non critical database systems [Recommended]

For other systems and applications deemed non-critical and kept on premises, entities are required to implement appropriate measures to secure them and to develop and follow an appropriate backup and recovery process

Security and data privacy

Government institutions should follow RISA security and data privacy guidelines when deploying database management systems. In particular, the following guidelines should be followed:

Data validation [Mandatory]

When capturing new data in a DBMS, data validation must be used to ensure the DBMS’s stability and integrity of stored data

Functional separation between database servers and web servers [Recommended]

Due to the higher threat environment that web servers are typically exposed to, hosting database servers and web servers within the same operating environment increases the likelihood of database servers being compromised by malicious actors. This security risk can be mitigated by ensuring that database servers are functionally separated from web servers.

Communications between database servers and web servers [Recommended]

Data communicated between database servers and web servers, especially over the internet, is susceptible to capture by malicious actors. As such, it is important that all data communicated between database servers and web servers is encrypted.

Network separation [Recommended]

Placing database servers on the same network segment as user workstations can increase the likelihood of database servers being compromised by malicious actors. Additionally, in cases where databases will only be accessed from their own database server, allowing remote access to the database server poses an unnecessary security risk.

Separation of development, testing and production database servers [Mandatory]

Using production database servers for development and testing activities could result in accidental damage to their integrity or contents. Therefore development, testing and production database servers should be separated.

Security hardening [Mandatory]

The server operating systems that the database is installed upon must be security hardened

Access control [Mandatory]

- Implement strict access controls to restrict access to authorized personnel only
- Access to a DBMS must apply the principle of least privilege and users and applications should only have the permissions required to achieve their role and purpose

Default passwords[Mandatory]

The default passwords for accounts and services such as System Administrator must be changed prior to DBMS being deployed

DBMS Versions and security updates [Mandatory]

- The versions of DBMS used must still be supported by the vendor
- All installations of a DBMS must be up to date with all appropriate security patches prior to deployment

Encryption [Mandatory]

Use strong encryption algorithms to protect sensitive data stored on disks, databases, and other storage systems. Ensure that encryption keys are properly managed and stored separately from the encrypted data.

Protecting database contents [Mandatory]

- Database administrators and database users should know the sensitivity or classification associated with databases and their contents. In cases where all of a database's contents are the same sensitivity or classification, an organisation should classify the entire database at this level and protect it as such.
- Alternatively, in cases where a database's contents are of varying sensitivities or classifications, and database users have varying levels of access to the database's contents, an organisation should protect the database's contents at a more granular level. Restricting database users' ability to access, insert, modify or remove database contents, based on their work duties, ensures that the likelihood of unauthorised access, modification or deletion of database contents is reduced.
- Furthermore, where concerns exist that the aggregation of separate pieces of content from within a database could lead to malicious actors determining more sensitive or classified content, the need-to-know principle can be enforced through the use of minimum privileges, database views and database roles. Alternatively, the content of concern could be separated by implementing multiple databases, each with restricted data sets.

Monitoring and database events logging [Recommended]

- Employ real-time monitoring tools to detect and respond to unauthorized access attempts as they occur. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are useful for this purpose
- Centrally logging and analysing database events can assist in monitoring the security posture of databases, detecting malicious behaviour and contribute to investigations following cyber security incidents.

Security standards and guidelines [Mandatory]

- Ensure compliance to the Minimum Cybersecurity Standards for Public Institutions that are provided by the National Cyber Security Authority
- Ensure compliance with Rwanda’s Data Privacy Law and RISA Security and Data privacy guidelines

Database maintenance

The following are guidelines on management and maintenance of DBMS systems should be adopted:

Database maintenance

Performance monitoring and tuning [Recommended]

- Implement real-time monitoring to promptly detect and respond to performance issues as they arise
- Implement database performance tuning which involves optimizing the configuration, structure, and queries of a database system to achieve optimal efficiency, responsiveness, and overall performance
- Monitor utilization of key resources such as CPU, memory, disk I/O, and network. Resource bottlenecks can significantly impact database performance

Change management [Mandatory]

- Establish a formal process for submitting requesting, approval and implementation of changes to a database
- Document all database changes comprehensively. This includes changes to schema, indexes, stored procedures, triggers, and configuration settings
- Use version control systems for database schema and code changes. This helps track modifications, roll back changes if needed, and collaborate effectively
- Have dedicated testing environments where you can validate changes before deploying them to the production database.

Documentation [Mandatory]

- Maintain accurate and up-to-date database documentation which is crucial for the efficient and effective management of databases within an institution

7 Disaster recovery and business continuity management

Database systems hold critical data of Government institutions and are core to performance and availability of government software systems used to delivery services and automate government processes. It is therefore critical to ensure their continued availability by putting in place suitable disaster recovery and business continuity processes. The following guidelines apply to disaster recovery and business continuity management:

Data backup and recovery strategy process [Mandatory]

- Develop a backup and recovery strategy to prevent data loss in case of hardware failures, errors or disasters
- Specify the acceptable data loss in case of a disruption. This determines how frequently backups need to be taken to minimize data loss
- Determine recovery time objectives (RTO) and recovery point objectives (RPO) for each database. These define the acceptable downtime and data loss limits
- Implement regular and consistent database backups. Use full, differential, and incremental backup strategies based on your RPO and RTO requirements
- Periodically simulate recovery scenarios to ensure that your recovery plan is accurate and effective. Test various scenarios, including partial and complete failures
- Conduct a full recovery test where you simulate a complete system or data loss and use your backups to restore everything. This tests the entire recovery process from start to finish

Data retention

Data retention is the storing and managing of data and records for a designated period. The period is defined based on operational and regulatory requirements. The following guidelines should be followed:

Data retention policies [Mandatory]

- Classify your data into categories based on factors such as sensitivity, importance, and compliance requirements. Different categories may have different retention periods
- Define data retention policies based on the operational needs of the institutions, regulations and storage costs
- Document data retention policies in detail. This should include information about the data categories, retention periods, triggers for retention start, and procedures for data deletion
- Periodically review and update data retention policies to ensure they remain aligned with changing operational needs and evolving regulations

Data purging [Recommended]

Data purging involves permanently deleting data that is no longer required or relevant. Document the procedures for data purging, including who is responsible for initiating purging, how it is executed, and how verification is done