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]
- Functional separation between database servers and web servers [Recommended]
- Communications between database servers and web servers [Recommended]
- 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]

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