Standard for Databases

Objective

In accordance with the Information Security and Acceptable Use Policy, all databases owned or managed by the University of Texas at Dallas must be adequately protected to ensure confidentiality, integrity, availability, and accountability of such systems. Databases normally provide a data storage mechanism as a back-end to an application that provides access to the data. In addition to electronic data storage, databases typically are associated with management systems which organize data into a collection of schemes, tables, queries, reports, views and other objects.

Physical Location

All production databases should be operated on dedicated servers in rooms that meet the applicable minimum standards defined in the Standard for Server Rooms.

Support Requirements

All production databases must have a valid support contract or, in the case of open-source software, be commercially or community supported.

Patching

Security patches for all Database Management Systems (DBMS) must be installed in a timely manner, depending on the likelihood and impact of vulnerability exploitation.

Network Connectivity

Databases should not be accessible directly from the public Internet; on-campus connectivity should be limited to only necessary hosts and/or networks when feasible.

Authentication and Access Control

LDAP or Windows domain credentials are recommended instead of local user accounts. Administrative access should be conducted via individually-assigned accounts, rather than shared group accounts. If local accounts are used, password complexity requirements must be configured to be equivalent or stronger than those required for the NetID system. Authentication must be conducted over encrypted channels. Default accounts should be disabled when feasible. If default accounts are used, passwords must be changed and meet minimum complexity standards.

Database Permissions

It is recommended to configure database permissions for users based on the principle of least privilege, thus granting the minimum access necessary to fulfill business operations. Security permissions should be as specific as possible—i.e. row-level permissions rather than table-level permissions, when feasible. Use of roles is recommended when supported by the DBMS.

Database Encryption

Databases storing Confidential Data elements should use encryption methods to protect those elements while at rest, when supported by the DBMS. Alternatively, the application may be configured to encrypt stored data. Database connections must be configured to encrypt Confidential Data in transit using a minimum of 128-bit encryption. 256-bit encryption is recommended where feasible.

Logging

Database activity must be logged and retained for a minimum of 90 days to facilitate troubleshooting and investigations. The following types of activities must be logged:

- Successful and unsuccessful login attempts
- Any database modification operation, such as insertion, updates, or deletion of data, changes to database structure, etc. Logging of read / query activity of Protected Health Information (PHI) is required for databases containing HIPAA data; Logging of read / query access to confidential data is recommended when feasible.

Database logs should also be sent to a centralized logging server to reduce storage requirements on local systems and reduce feasibility of log tampering.

Backup / Recovery

Backup and recovery procedures meet the necessary requirements for data owners and custodians, be documented, and be tested at least annually. Backup media should be encrypted if transported or stored outside of a UTD facility.

Mock Data

When feasible, mock data should be used within non-production environments including development, test, quality assurance, sandbox, and training systems. If mock data is not feasible, the database must meet the security requirements for a production database.

Incident Management

System owners are required to report any suspicious activity to the Information Security Office for investigation.

Business Continuity Planning / Disaster Recovery

All mission-critical systems must be covered by an applicable Business Continuity Plan (BCP) and Disaster Recovery (DR) plan.

Exemptions

In the event that compliance with this database standard cannot be met, please contact infosecurity@utdallas.edu to submit an exemption request which will be approved or denied by the CISO. Denied exemption requests may be appealed to the UTD President for final decision.