



# FERRIS STATE UNIVERSITY



## **Database Security Policy**

By. Jack Pfleghaar

# Contents

Introduction .....3

Security Management.....3

Physical Security .....3

Network Security.....4

Database Security .....4

Access Control.....4

Data Access.....5

Auditing and Logging.....5

Summary.....5

## Introduction

The purpose of this policy is to establish a comprehensive security framework to be used on the database systems, production data, device logs, and operational configurations for this company. This policy is designed to use Defense in Depth by applying multiple layers of security and protection. This spans the management, physical, network, and database security domains to fully safeguard the databases against internal and external threats such as negligence or malware.

## Security Management

Effective database security begins with strong security management processes. This is why governance responsibilities are defined to ensure accountability at every level. The Database Administrator (DBA) is to be seen as the data custodian and should be responsible for implementing technical controls, managing permissions, and maintaining the integrity of the data inside the database. The Information Security Officer (ISO) should ensure that compliance with internal standards and external regulations is being upheld. Departmental database owners are responsible for their own database aligning with the companies' organizational policies.

Any persons who request to access the database are required to complete an annual cybersecurity and insider threat awareness training. This training reinforces the importance of recognizing threats and how they can impact our security. Any changes to the database structure or user permissions must go through the company's Change Management Process (refer to SQL Server Backup, Recovery, and Turnover Management page 14) and must be approved prior to implementation. The database system is also required to adhere to all corporate information security policies.

## Physical Security

The physical protection of database servers and other related infrastructure is essential to preventing unauthorized access and ensuring system availability. Database servers are to be housed in secure data centers equipped with restricted badge access, video surveillance, and environmental controls such as temperature monitoring and fire suppression in the case of emergency. The only personnel authorized to enter the server room are approved IT workers. Any visitors are to be logged, escorted, and have managerial approval.

To follow best practice procedures, the database server is to be hosted on dedicated hardware separate from the organizations web server. This air gap will work to minimize exposure by preventing external-facing systems from directly accessing the data storage layer. All database backups are to be physically stored and secured as well. All portable media containing database backups or other information are to be encrypted and stored in a secured facility. There must be redundant power supplies and backup generators available in the event of an outage.

## **Network Security**

Network security controls are essential in providing additional security by restricting access to database servers through secure and segmented networks. The network architecture should follow a three-tier design that separates the web application layer, the application logic layer, and the database layer. The database should reside on an internal network segment that is protected by firewalls and is isolated from public access. Web servers will be placed within a demilitarized zone (DMZ) and all communication between the web server and database will occur through encrypted channels over restricted ports.

Any and all traffic between the network layers will be monitored by an intrusion detection and prevention system (IDS/IPS) which will analyze packets for signs of suspicious or irregular behavior. This will work hand in hand with a Network Access Control (NAC) to ensure that only approved devices will be able to communicate with the database network. No database servers are permitted to have direct internet access to prevent unauthorized data exfiltration.

## **Database Security**

All database management systems must be configured according to vendor specific hardening guidelines and conduct system patching on a monthly basis. Any critical updates must be applied within no more than fourteen days of the patch release. Any sensitive data must be protected by the use of encryption using AES-256. Any confidential data elements such as passwords or encryption keys must be hashed or encrypted within database tables to prevent the disclosure in the event of unauthorized access.

## **Access Control**

Access control policies are essential to ensuring that only known authorized users are able to view or manipulate database data. Authentication and authorization processes must follow the principle of least privilege and role-based access control. Access should be granted based on the users job rather than on preference or request. Roles are predefined as database administrators, analysts, engineers, and application service accounts with each having permissions limited to the specific actions required for their respective duties.

Multi-factor authentication (MFA) is required for all access. Passwords must be at a minimum twelve characters long and contains uppercase, lowercase, numbers, and special symbols ('!@#\$\$%^&\*'). Default vendor credentials are to be disabled immediately after installation to prevent exploitation. Access reviews are to be performed quarterly to detect and remove unnecessary privileges, accounts, and to prevent creeping authority.

## Data Access

Data access procedures are designed to minimize the ability of SQL injection attacks and unauthorized manipulation. Application-level interaction must occur using stored procedures or parameterized queries rather than direct SQL execution. This prevents the execution of malicious code into the query through SQL injection and maintains consistency in data handling. Views will be created to limit user visibility to only the tables necessary for their assigned roles to reinforce the principle of least privilege. Embedded SQL statements within application code are prohibited under all means necessary.

## Auditing and Logging

Comprehensive auditing and logging are critical. All database activity must be logged, including both successful and failed login attempts, privilege escalation, database changes, insert or deletions, and more. Logs are timestamped and stored in a secured facility to preserve integrity and are to be retained for a minimum of one year. All logs are to be aggregated and analyzed through a Security Information and Event Management (SIEM) system, which will provide real-time anomaly detection. Automated alerts are configured to notify the ISO and DBA of suspicious activity such as the ones previously stated. Audit logs are reviewed on a weekly basis to identify any policy violations. This ensures that any potential threats are detected before they can cause harm.

## Summary

This policy employs multiple reinforcing layers of security to ensure the safety of any and all database systems. Physical controls safeguard the hardware and prevent unauthorized access. Network security isolated the database from public-facing systems and enforces encrypted communication. And database controls ensure that if one layer is compromised there are additional barriers in place. By integrating these measures, we can maintain that the security of our database maintains its ability to defend against internal and external threats.