**Vulnerability Assessment Report**

**29th January 2025**

# System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

# Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Purpose

The database server is a critical asset to the business, storing valuable customer data, sales records, and other operational data. Securing the data on the server is crucial to prevent unauthorized access, data breaches, and potential financial and reputational losses. If the server were disabled, the business would experience significant disruptions, including loss of customer trust, operational downtime, and regulatory non-compliance penalties.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Cybercriminal* | *Launch a SQL injection attack* | *2* | *3* | *3* |
| *Insider* | *Unauthorized data modification or deletion* | *2* | *3* | *2* |

# Approach

Risks were considered in relation to the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs. The assessment prioritized threats based on their potential impact and probability of occurrence.

# Remediation Strategy

* **Authentication and Authorization:** Implement strong authentication mechanisms, including role-based access control (RBAC) and multi-factor authentication (MFA) to ensure that only authorized users access the database server.
* **Encryption Enhancements:** Enforce encryption for data in motion using TLS instead of SSL to enhance security.
* **IP Restrictions:** Implement IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.
* **Regular Audits:** Conduct periodic security audits and vulnerability scans to identify and mitigate potential security gaps.
* **Access Logging and Monitoring:** Enable real-time logging and anomaly detection to track and respond to suspicious activity on the database server.
* **Incident Response Plan:** Establish a robust incident response plan to mitigate risks in case of a security breach.