**Vulnerability Assessment Report**

**19th November 2023**

# 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 Nov 2023 to January 2024. [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

Consider the following questions to help you write:

* *How is the database server valuable to the business?*
* *Why is it important for the business to secure the data on the server?*
* *How might the server impact the business if it were disabled?*

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Employee* | Alter/Delete critical information | *2* | *3* | *6* |
| *Sytem Administrator* | Perform reconnaissance and surveillance of organization |  |  |  |
| *Advanced Persistent Threat* | Install persistent and targeted network sniffers on organizational information systems. | *3* | *3* | *9* |
| *Hacker* | Conduct Denial of Service (DoS) attacks. | *3* | *3* | *9* |
| *Hacker* | Conduct "man-in-the-middle" attacks. | *3* | *3* | *9* |

# Approach

Risks considered 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.

# Remediation Strategy

Implementation of authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. This includes using strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent random users from the internet from connecting to the database.