**Vulnerability Assessment Report**

**5th June 2024**

# 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 used daily by employees to access records that assist in the process of prospecting for new customers and help the business grow. It’s important to secure the data on the server to prevent potential attacks that could interrupt daily operations. A server outage would not only stagnate the current customer count but also cost the business through the payroll of the incapacitated remote workforce.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Competitor* | Obtain sensitive information via exfiltration | *1* | *2* | *2* |
| *Employee* | Disrupt mission-critical operations. | *2* | *3* | *6* |
| *Hacker* | Conduct Denial of Service (DoS) attacks. | *2* | *3* | *6* |

# 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.

The three threat sources listed were chosen based on the potential incentives the various entities may have in exploiting the current vulnerability. A malicious competitor may have interest in gaining access to the database so they might try to take potential or established customers. An employee may accidentally or intentionally make a change that disrupts business operations because proper security controls are not implemented to limit access. Lastly, hackers across the world currently have access to the database since it’s public which opens it up not only to the previously mentioned threat events but also more technical attacks like DoS.

# 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.