**Vulnerability Assessment Report**

**1st 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

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?*

*The database is valuable for the business as it stores all the information that is important to the activity of the business. It keeps records of all the workers, customers, and confidential documents, making it a very important source of information. It is important for the business to secure the data in the server because the business can be severely affected if the company cannot maintain a form of confidentiality, integrity, and availability, in order to be trusted by anyone, as the company is trusted to hold onto the important information with dedicated and secure procedures. This is why lack of security is a financial risk as well to the company, which is why it is super important to maintain security.*

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Outsider* | *Obtain sensitive information through hacking into the “public” database.* | *2* | *2* | *4* |
| *Software* | *The db relies on other servers which means that since it’s public. If an outsider infiltrates into the network, they can do so through the other server connections that the database has.* | *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.