**Vulnerability Assessment Report**

**1st January 20XX**

# 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

Many of the employees of the company work from remote locations all around the world. The company uses a server which runs a database software. Employees regularly access this database server to better connect with customers and increase the business for the company. This database has always been open to the public, as a result, anyone even from outside the company can access the database and the sensitive information inside it. This is a direct violation of the privacy of customer’s data. Also, the competitors can access this data to get the insight information on how the business is operated which can in turn be used to harm the company.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Power Outages* | *Disrupt mission-critical operations.* | *3* | *3* | *9* |
| *Employee* | *Alter/Delete critical information* | *3* | *2* | *6* |
| *Processing* | *Disrupt mission-critical operations.* | *1* | *3* | *3* |

# 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.