**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

* The database server that is being assessed for vulnerabilities is important to the organization because it allows us to request data to potentially find new customers.
* This data must be secured and protected because our customers have personal identifying information (PII) that is stored on our servers. Risking this PII can be detremental to our business and also be in breach of data storage compliances.
* If this server was to be disabled, we would cease to be able to carry out daily operations. Our employees could not request the data they need to make business decisions and guide the organization to potential new customers.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Hacker* | *Obtain PII and sensitive data via vulnerabilities* | *3* | *3* | *9* |
| *Employee* | *Accidental or intentional mishandling of data could disrupt daily tasks and operations.* | *2* | *3* | *6* |
| *Customer* | *Alter or delete sensitive data via vulnerable assets that are connected to the database server* | *1* | *3* | *3* |

# Approach

The risks listed here considered the data storage and management procedures of the organization. The threat sources were determined based on the likelihood of a security breach based on the openess of the database server. The severity of these potential threats were determined with daily tasks and operations in mind.

# 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.