# Vulnerability Assessment Report

6th 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 June 2023 to August 2023. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

## Purpose

The goal is to improve the security of the remote database server, as it stores relevant PII for potential customers. The company must maintain this data secure because it would affect business productivity if all the leads were to be deleted/stolen. There can also be fines/penalties for mishandling clients' PII.

## Risk Assessment

| Threat source | Threat event | Likelihood | Severity | Risk |
|---|---|---|---|---|
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Disgruntled Employee* | *Permanently delete all database records* | *1* | *3* | *3* |
| *Hacker* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |

## Approach

Risks considered are 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. Conducting incremental, differential, and full backups as appropriately required.