# Vulnerability Assessment Report

1st January 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 2024 to August 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

## Purpose:

- *Database is the most important asset to the organization as it contains most of the user credentials and other important information regarding the organization business plans, employee data and other financial information.*
- *When a business asks for the information from the users , it is the organization's responsibility to keep the data safe as the user trusts the business and shares their own personal and private information with the business. These are sensitive data and should be protected by any business as many regulatory agencies have applied multiple compliance to be followed.*
- *If the server is disabled the users may not be able to login to their accounts and the business will be unable to sever its services.*

## Risk Assessment

| Threat source | Threat event | Likelihood | Severity | Risk |
|---|---|---|---|---|
| *Human* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Environmental Sources* | *Threats that arise from accidental, non-human factors.* | *1* | *3* | *3* |

| | | | | |
|---|---|---|---|---|
| *Technical Sources* | *Threats that originate from non-human factors. For example, failures of equipment due to aging,resource depletion, or other circumstances.* | *2* | *2* | *4* |

## 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.