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 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?*

It's important to keep the database secure because it contains all our potential customers' information, which could lead to an increase in profits if we studied the database thoroughly. Having that leak out to the public would lead to a breach in privacy for the customers and would allow for other attackers or competitors to grab their data, making them encounter other possible attacks. We would definitely lose the trust of our clients if this were to happen, and we would not meet government regulations.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	Obtain PII via data breach	*2*	*3*	*6*
Employee	*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 (we'll be operating on least privilege principle), and mfa (multi-factor authentication) to lessen the user's privileges. Encryption of data in motion using TLS instead of SSL. IP allow-listing to corporate offices to prevent outside forces from connecting to the database.