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 the 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?*

The purpose of this assessment is to determine whether the proper steps and regulations are being followed to ensure the privacy of the database servers is securely protected. If disabled, data may be lost or destroyed. Certain services may be rendered unavailable for a time and the data of employees and customers may be at risk.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Customer	*Delete important information*	*1*	*3*	*3*
Disgruntled Employee	*Obtain unauthorized access to sensitive information*	*2*	*3*	*6*
Hacker	*Obtain sensitive information via*	*3*	*3*	*9*

	exfiltration			

Approach

Risks were identified based on the more sources that can negatively impact business operations and data management. The likelihood of these sources occurring was weighed against the severity of the impact they may have on the business.

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.