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

> *The database server is valuable to the business because it contains customer information and employee information. The server stores customer information, and if it is stolen, this will cause cybercriminals to have an upper-hand. It is important to conduct this security analysis to prevent harm to the server.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration.*	*3*	*3*	*9*
Customer	*Alter or delete critical information.*	*1*	*3*	*3*
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*

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. The threat events were selected because of the possibility of them taking place. When sensitive information is obtained through exfiltration, it is a significant business risk because money could be stolen from customers. When customers alter critical information, it is a significant business risk because it affects the integrity of the information. And when customers delete critical information, it is a significant business risk because critical information is always needed. Lastly, when employees disrupt mission-critical operations, it is a significant business risk because there needs to be business continuity.

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.