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 critical to the company’s ability to store and query customer information. Because employees worldwide rely on this system, it directly supports customer acquisition and business growth. However, keeping the server publicly accessible introduces significant risks to data confidentiality and integrity. If disabled, business operations would be disrupted, potentially leading to financial loss, reputational damage, and regulatory violations. This assessment aims to evaluate vulnerabilities and provide guidance for securing the server.

Risk Assessment

Threat source	**Threat event**	**Likelihood**	**Severity**	**Risk**
Malicious hacker	*Unauthorized data exfiltration (customer info theft)*	*3*	*3*	*9*
Insider threat	*Misuse of database access (alteration of records)*	*2*	*3*	*6*

Natural disaster	*Database server outage (coastal power disruption)*	*1*	*2*	*2*

Approach

I selected these three threats because they represent the most realistic and impactful risks for the business. External hackers are the greatest concern due to the server being open to the public, making data theft highly likely. Insider misuse is also a key risk, given that employees regularly access sensitive data. Finally, while less likely, natural disasters could disrupt availability, and identifying this ensures the company is aware of environmental risks.

Remediation Strategy

To mitigate these risks, the company should immediately restrict public access and enforce the principle of least privilege by requiring role-based database access. Implementing multi-factor authentication (MFA) and encryption will further protect sensitive data from unauthorized use. To address insider risks, enable regular auditing and logging of all database queries. For natural disasters, establish backups and disaster recovery plans to maintain data availability. Collectively, these layered defenses strengthen confidentiality, integrity, and availability of business-critical data.