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 essential to the business because it stores both temporary and valuable data. Protecting this data is crucial to prevent the loss of critical information and to guard against potential cyberattacks. If the server were to go offline, it could disrupt business operations, directly affecting the company's workflow and productivity.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Advanced Persistent Threat (APT)	*Unauthorized access to steal or alter data*	*3*	*5*	*15*
Malware	*Infection with malware that damages or disrupts service*	*4*	*4*	*16*
Faulty power supplies	*Server downtime due to power failure*	*2*	*4*	*8*

Approach

The risks were evaluated by considering the business's data storage and management methods. The likelihood of threat occurrences and the potential impact of these events were carefully weighed against the operational requirements and day-to-day needs of the organization.

Remediation Strategy

To address the identified risks, the implementation of strong authentication, authorization, and auditing controls is essential. This includes enforcing multi-factor authentication (MFA) and role-based access control (RBAC) to limit user privileges according to the principle of least privilege. Encrypting data in transit with TLS protects against interception, while IP allow-listing restricts access to trusted corporate locations. Additionally, applying defense-in-depth strategies, such as network segmentation and regular patch management, helps mitigate malware infections and reduce the impact of power failures.