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?*
  It contains information about the business transactions and PII of customers
- *Why is it important for the business to secure the data on the server?*
  To maintain competitive edge in the market and to ensure confidentiality, availability for customers
- *How might the server impact the business if it were disabled?*
  If server were to be disabled then the business cannot operate optimally and serve it servers and fails to maintain the availability in the CIA triad

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Supplier	*Obtain sensitive information of the business dealing and transactions . Use it for personal gain*	*1*	*3*	*3*

Hacker	*Access and modify company data*	*2*	*3*	*6*
System administrator	*Deletion/Failure of the whole system*	*3*	*3*	*9*

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, 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.