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

- *How is the database server valuable to the business?*
  Since the Database consists of PII & SPII of the customers, it's highly valuable to organization and any security event could have catastrophic effects on business operations.
- *Why is it important for the business to secure the data on the server?*
  The DB holds critical data such as customers PII & SPII. failure to secure the data could result in loss of reputation and fines or legal consequences due to non compliance of regulation.
- *How might the server impact the business if it were disabled?*
  It would disrupt the business operations as the proper function of the business depends on the server.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*
Business partner	*Conduct Denial of Service (DoS) attacks*	*1*	*2*	*2*

Approach

Risks that were measured considered the data storage and management procedures of the business. Potential threat sources and events were determined using the likelihood of a security incident given the open access permissions of the information system. The severity of potential incidents were weighed against the impact on 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.