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 purpose of this security assessment is that the database server the company uses has been open to the public for three years. The database is valuable to the company because it is a core functionality to find potential leads, provides remote access to employees globally and any disruption to the server or compromise of its data directly impacts business continuity, revenue generation, and customer trust. It is important to have the server secured as there is a risk of data breach, unauthorized access exposure and compliance violation of data privacy regulations. If the server was disabled, some potential risks would be revenue loss, reputation harm, and clients and employees PPI and SPPI publicly exposed.

Risk Assessment

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