Vulnerability Assessment Report

8th October 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

Our database server is our technological workhorse for the business. It allows our staff to be de-centralized and work from any location, and it allows our staff to easily find potential customers and clients. Without it we do not have a business.

It is important to secure data on this server for a multitude of reasons, all of which are severely important. Securing data makes us compliant to regulations and laws that otherwise will fine the company for failing to comply. It will also keep our internal information safe from competitors, and protect sensitive information we keep about potential and current clients. If our clients' data were leaked or taken from us from a malicious actor, we could lose their business, garner the attention of lawmakers, and risk our reputation as a brand.

Keeping our servers public and unsecured also opens our servers to other attacks that could disable the servers entirely. Such attacks would mean that our staff would be unable to work from their locations or do their jobs at all. It would effectively shut our business down entirely.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
E..g Competitor or online hacktivist	*Conduct Denial of Service (DoS) attacks.*	*1*	*3*	*3*
Employees, either purposefully (disgruntled) or accidentally	*Disrupt mission-critical operations.*	*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.