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?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

"The database server serves as the backbone of our marketing operations, storing and managing essential information such as customer details, campaign records, and performance analytics. This data drives decision-making, enables targeted outreach, and helps measure results. Given its importance to business growth and strategy, safeguarding the server is a top priority to ensure both security and reliability."

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Hacktivist	*Conduct Denial of Service (DoS) attacks.*	*1*	*3*	*3*

System Administrator	*Install persistent and targeted network sniffers on organizational information systems.*	*2*	*3*	*6*
employee	*Disrupt mission critical operations*	*1*	*2*	*2*

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

“Securing the database server requires a comprehensive access control strategy. Authentication, authorization, and auditing must be enforced to ensure that only validated users with approved roles can connect. Strong password enforcement, role-based access control (RBAC), and multi-factor authentication (MFA) should be mandatory to minimize privilege misuse. All data transfers must be encrypted using TLS protocols, eliminating reliance on deprecated standards such as SSL. Network access should be restricted through IP allow-listing, permitting connections only from trusted corporate networks and blocking all unauthorized traffic from external sources.”