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 server is how the company deals with any digital assets or network communication. The server may hold invaluable customer information as well as internal information that is important. If the server were to be completely disabled this would nearly cease all functions to an e-commerce company.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Customer	*May alter or delete critical information.*	*1*	*3*	*4*
Employee	*May accidentally access critical systems.*	*2*	*2*	*6*
Hacker	*May obtain sensitive information.*	*2*	*3*	*8*

Approach

I began my evaluation upon the risks that were most representative of the organization's internal and public operations and then considered a malicious risk as well. I then compared the likelihood of a security incident happening (under open access permissions) with the incident's severity. Based on these considerations I evaluated the total criticality of the risks and their prevention.

Remediation Strategy

There are multiple things that should be implemented to remediate these obvious vulnerabilities. Applying defense in depth through any and all means via perimeter layering authentication and network access authorization (perhaps through a further implementation of firewalls on the remote server). It is also important that we only allow specified workers access to various parts of the database and servers, limiting access to critical server infrastructure that should not be available to external personnel such as customers or malicious actors.