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
Gain insight into potential likelihood and severity of risks and helps them make informed decisions about allocating resources, implementing controls and prioritizing remediation efforts. The server contains data that needs to be protected and it is important to secure this data because or regulations as well as preventing damage to rep and preventing monetary losses. Business may be halted, could lose lots of data and face fines and damage to company reputation.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Standard user	*Accidentally leaks private info*	*2*	*3*	*6*
Software	Software is not update to date leading to a vulnerability being exploited	2	3	6
Hardware	Improper storage leads to data being lost	1	2	2

Approach
They have a likelihood of happening, and it is important to address these issues. The leaking of private info could have huge consequences for the company, software that is not up to date could also leave room for malicious attackers to attack. Improper storage could also lead to valuable day to day data that is needed becoming lost and hurting business operations.
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. Ensuring there is a access limit to sensitive files and limiting access to only those who need the files, implementing automatic updates to keep software up to date and ensuring hardware is properly stored and looked after to limit the

loss of data.