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

Purpose is to consider all the potential threats vectors that might affect the organization day to day organization. A server hardware might fail causing critical service to halt. An insider threat might exploit organization from the inside causing organization to be breached of their sensitive information

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*1*	*3*	*3*
Employee	Employee might accidentally or purposely exposed sensitive organization data	1	2	*2*
Hacker	Might conduct DoS or or MITM	1	3	3
Storage	Might fail due to unhandled circumstances	1	3	3
Insider	Infiltrate organization to obtain	1	3	3

	sensitive information			
Power Outages	Halt critical business operation	1	3	3
Malware	Disruption to operations and infiltration to data of the organization	1	3	3

Approach

The vulnerability assessment considered possible threat sources that might disrupt the organization day to day operation. This includes employees as they are the one who have access to the organization operations, two is the hardware as it might fail due to unseen circumstances even though unlikely but not zero.

Remediation Strategy

Make sure that staff have only the minimum level of access to resources that is sufficient to do their functions. Make sure that one employee should not handle multiple tasks or access on their own preventing one user from misusing their access, this practice the principle of separation of duties. Implement Defense-in depth making sure that there are multiple layers of security defending against adversaries.