**Vulnerability Assessment Report**

**23rd July 2024**

# 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 2024 to August 2024. [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Purpose

Consider the following questions to help you write:

* *The server is valuable to the business because it holds their database of information.*
* *This data needs to be secured because it could have PII.*
* *The business would not be able to continue operations if they were to lose connection to the server.*

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Employee* | *Obtain sensitive information by using their login credentials* | *2* | *2* | *4* |
| *Communication* | *An email could be sent to the wrong recipient with internal-only documents* | *3* | *3* | *9* |
| *Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |

# Approach

Employees are a risk because they are given access to information with their credentials. They can relay this information either accidentally or purposefully. Communication is a risk as emails or text messages can be sent to the wrong person or seen by threat actors if they are not encrypted. Competitors are a risk because if they see internal-only documents they could take the idea.

# Remediation Strategy

Make sure employees only have access to information they absolutely need following the principle of least privilege. Emails should be encrypted when going to someone outside of the business to verify nothing is seen by someone who should not have access. Ensure vulnerability assessments are completed frequently so there are no back doors.