**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](https://docs.google.com/document/d/1Fc4L2azQlnUM-8r43PU9mYlT30BnxTwdjAMqpT7JeZk/edit?resourcekey=0-Q-XglnC3Li7JPK2hIvMkVg#heading=h.hvbcmqwzo9do) is used to guide the risk analysis of the information system.

# **Purpose**

*The security of the database server is a valuable asset to the company as it centralized computer system that stores the information of many of the company’s assets and customer data. Securing the database server would be beneficial not only to the business in the long run but to clients who use the platform. A failure to secure the database server and the likelihood of it being disabled would impact the platform for everyone due to the fact it is being used regularly and also it would be causing a disruption of marketing operations.*

# **Risk Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| *Hacker* | *Obtain sensitive information via exfiltration* | *3* | *3* | *9* |
| *Employee* | *Disrupt critical operations* | *2* | *3* | *6* |
| *Customer* | *Alter/Delete critical information* | *1* | *3* | *3* |

# **Approach**

*The risk selection was based on data storage and management procedures by the business. Potential threat sources and events were finalized using the likelihood of a security incident* given the open access permissions of the information system. The severity of potential incidents was weighed against the impact on day-to-day operational needs.

# **Remediation Strategy**

Authentication, authorization and auditing are implemented to ensure that the system is secured by allowing only authorized users to access the database server. Included security controls are 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 allows-listing to corporate offices to prevent random users from the internet from connecting to the database