**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/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?usp=sharing&resourcekey=0-3GRRWAd8HryVgof-Jc33yA) is used to guide the risk analysis of the information system.

# Purpose

The server is routinely used by company employees to query relevant information to find new clients for the business. If the server were to become compromised or taken offline the business could suffer stalled productivity resulting in a loss of revenue as well as a loss of brand recognition and trust which could impact future business opportunities. Additionally, given the business’ remote working environment and employees accessing the server from around the world the business could be subject to litigation or reprimand if found in violation of international data protection laws, such as the GDPR.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| Hacker/Hacktivist | Obtain sensitive information via exfiltration | 3 | 3 | 9 |
| Employee | Obtain sensitive information unrelated to job function | 2 | 3 | 6 |

# Approach

Utilizing the NIST SP 800-30 Rev. 1 as a reference guide and narrowing the assessment to remain within the scope of access control systems the risks outlined in the risk assessment are most likely to be human by nature. Data within the database is accessible to anyone with knowledge of its existence. The threat of hackers/hacktivists is likely and could hold serious consequences to the business such as failure to comply with data privacy laws, ransomware attacks, exposure of sensitive information and the loss of brand trust. Additionally, unrestricted access to employees could result in sensitive data being exposed, misused (intentionally or unintentionally) and could violate data privacy regulations.

# 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.