**Vulnerability Assessment Report**

**27th December 2023**

# 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. The document alongside this document “NIST SP 800-30 Rev. 1” is used to guide the risk analysis of the information system.

# Purpose

A centralized computer system, the database server, is utilized for the storage and management of large volumes of data, including customer, campaign, and analytic data that can be analyzed to monitor performance and customize marketing efforts. Due to its frequent usage in marketing operations, it is crucial to ensure the security of this system.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Hacker* | *Steal confidential data* | *2* | *3* | *6* |
| *Employee* | *Cause disruption to essential operations.* | *2* | *3* | *6* |
| *Customer* | *Modify or delete crucial data* | *1* | *3* | *3* |

# Approach

The risks that were assessed took into account the data storage and management protocols of the organization. Potential threats and events were identified based on the probability of a security breach given the open access permissions of the information system. The severity of probable incidents was evaluated against the effect on the organization's daily operational requirements.

# Remediation Strategy

To ensure that only authorized users access the database server, it is crucial to implement authentication, authorization, and auditing mechanisms. This involves enforcing strong passwords, role-based access controls, and multi-factor authentication to limit user privileges. Additionally, data in motion should be encrypted using TLS instead of SSL. To prevent random internet users from connecting to the database, IP allow-listing should be employed, restricting access to corporate offices only.