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

The database server stores critical customer and business data, supporting essential operations such as lead generation and customer outreach. Securing this server is vital because:

- *A data breach could lead to legal and financial consequences.*
- *Public exposure increases the risk of exploitation.*
- *If the server is disabled or compromised, business operations could halt, leading to revenue loss and damage to the organisations reputation.*

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
External attacker/Hacker	*Unauthorised access to public database*	*3*	*3*	*9*
Malicious insider	*Extraction of sensitive customer data*	*2*	*3*	*6*

Botnet/ automated scan	*Exploitation of known database vulnerabilities*	*3*	*2*	*6*

Approach

The risks were prioritised based on potential impact and the likelihood of occurrence, using expert judgement, known vulnerabilities in public-facing systems and the NIST threat model. The severity of the risks were scored based on the potential for business disruptions and data sensitivity. Limitations include lack of access to historical incident dat and full network logs.

Remediation Strategy

To mitigate identified risks the following actions are recommended:

- ***Restrict Access****: Configure a VPN or allowlisted IPs for remote employee access; remove public exposure.*
- ***Implement Firewall Rules****: Block unauthorised inbound connections to the database server.*
- ***Conduct Regular Updates****: Ensure timely patching of the OS and MySQL.*
- ***Enable Logging and Monitoring****: Deploy intrusion detection to alert on suspicious access attempts.*
- ***Review User Access****: Audit permissions to ensure least privilege is applied.*

These measures will reduce threat exposure, increase system resilience, and help maintain business continuity.