**Vulnerability Assessment Report**

**3rd May 2025**

# 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 database server is highly valuable to the business as it stores and manages mission-critical data, including customer records, financial data, and operational logs. It supports various business applications and ensures data consistency, availability, and integrity across departments.
* Securing the data on the server is crucial to protect sensitive business and customer information from unauthorized access, data breaches, and tampering. A data compromise could lead to legal consequences, financial loss, and a damaged reputation.
* If the server were disabled, the business could experience significant disruptions in operations, loss of productivity, and inability to serve customers. Such an outage could also result in lost revenue and stakeholder trust

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *E.g. Competitor* | *Obtain sensitive information via exfiltration* | *1* | *3* | *3* |
| *Employee* | *Disrupt mission-critical operations* | *2* | *3* | *6* |
| *Customer* | *Alter/delete critical information* | *1* | *3* | *3* |

# Approach

Risks considered the data storage and management methods of the business. The likelihood of a threat occurrence and the impact of these potential events were weighed against the risks to day-to-day operational needs.

# Remediation Strategy

To mitigate the identified risks, the following security controls and strategies are proposed:

* **Authentication & Authorization**: Implement strong user authentication with complex password policies and multi-factor authentication (MFA). Enforce role-based access controls (RBAC) to ensure users only have access to the data they need for their job.
* **Auditing**: Enable detailed logging and auditing mechanisms for all access to the MySQL database to detect unauthorized attempts and support forensic investigations.
* **Encryption**: Use **TLS** for all data in transit to enhance security beyond deprecated SSL protocols. Ensure encryption is enforced on all network communications to and from the database server.
* **IP Allow-listing**: Restrict incoming traffic to the database server by allowing only known IP addresses from corporate offices or VPN endpoints. This reduces the surface area for internet-based attacks.
* **User Privilege Review**: Regularly audit user accounts and permissions to revoke unnecessary privileges and reduce the risk of internal misuse.
* **Patch Management**: Apply security patches and system updates regularly to mitigate known vulnerabilities in the OS and database software.