**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 purpose of this vulnerability assessment is to identify weaknesses in the organization’s access controls, particularly regarding the public-facing database server. This database contains critical business information, sensitive employee and customer data, and is essential to daily operations. If left unsecured, attackers could steal or misuse private information, disrupt services, or damage the company’s reputation. Protecting the confidentiality, integrity, and availability of this system is vital to maintaining business continuity.

# Risk Assessment

| **Threat source** | **Threat event** | **Likelihood** | **Severity** | **Risk** |
| --- | --- | --- | --- | --- |
| *Hacker* | *Attackers misuse publicly available database to commit identity theft* | *3* | *3* | *9* |
| *Employee* | *Disgruntled employee abuses access to damage company reputation or leak sensitive data* | *2* | *3* | *6* |
| *Database* | *Database deletion or corruption causes prolonged downtime, disrupting business continuity* | *2* | *2* | *4* |

# Approach

The greatest risk stems from the database being publicly accessible, which exposes it to malicious actors. Human-driven threats can lead to a wide range of consequences, such as identity theft, data leaks that harm the company’s reputation, financial losses if sensitive PII/SPII is exposed, legal and compliance penalties, and operational disruption from data manipulation or deletion. Additionally, the organization’s heavy reliance on a single database introduces technological risks. If the database becomes unavailable—through downtime, corruption, or attack—the business could face severe disruption to its day-to-day operations. This dependency represents a single point of failure that must be addressed.

# Remediation Strategy

The main strategies for securing the database should revolve around the principles of least privilege, separation of duties, and defense in depth. First, the database should no longer be publicly accessible and must be protected with strong passwords and multi-factor authentication for all users. Access should be role-based, ensuring employees only have the permissions they need for their specific job functions, and general users should be limited to read-only access while administrative privileges are restricted. Network protections, such as a firewall and segmentation from public-facing systems, should be implemented to reduce exposure to unauthorized actors, while audit logging and monitoring should be used to track access and detect suspicious activity. All sensitive data should be encrypted both in transit and at rest, and regular backups should be maintained in secure locations. Finally, it is essential to keep the database and supporting systems updated with the latest patches, disable unused services and accounts, and establish a response plan for any security incidents. By layering these measures, the organization can mitigate human, insider, and technological risks and better protect critical information.