

Risk Assessment Report

Company Name: Bluekyte AI

Company Description: Bluekyte AI is an AI process automation and AI-powered solutions company.

Author: Piyush

Designation: AI Engineer

Date: 25th March 2025

1. Introduction

This risk assessment report evaluates potential risks associated with Bluekyte AI's operations, IT infrastructure, and data security. The assessment follows a structured approach to identifying, analyzing, and mitigating security risks.

2. Risk Assessment Methodology

- Identify potential risks and vulnerabilities.
- Analyze the likelihood and impact of each risk.
- Implement security measures to mitigate risks.
- Regularly review and update the risk assessment process.

3. Identified Risks

Risk Category	Description	Likelihood	Impact	Mitigation Measures
Data Breach	Unauthorized access to sensitive data	Low	High	Implement strong encryption, access control, and monitoring

Insider Threats	Employees or contractors misusing data	Low	High	Enforce strict access policies and conduct regular audits
Phishing Attacks	Employees targeted by phishing emails	Low	Medium	Conduct security awareness training and email filtering
System Downtime	Server outages affecting operations	Low	Medium	Implement failover solutions and regular system maintenance
Third-Party Risks	Security vulnerabilities in vendor services	Low	Medium	Perform regular vendor security assessments

4. Risk Findings Summary

After a thorough evaluation, no significant risks were found that could severely impact Bluekyte AI's operations. Existing security controls and mitigation strategies are sufficient to address potential threats.

5. Conclusion and Recommendations

- Continue monitoring and reviewing security policies to ensure robustness.
- Maintain regular security awareness training for employees.
- Conduct periodic security audits and risk assessments.
- Strengthen partnerships with secure and compliant vendors.

Approval:

Piyush

AI Engineer, Bluekyte AI

Date: 25th March 2025