Security Policy

Security Policy Document

Company Name: Bluekyte AI

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

Author: Abhishek

Designation: DevOps Engineer

Date: 25th March 2025

---

1. Introduction

Bluekyte AI is committed to maintaining the highest standards of security to protect its assets, customer data, and intellectual property. This document outlines the security policies and procedures applicable to all employees, contractors, and third parties interacting with Bluekyte AI systems and data.

2. Information Security Governance

- The core technical team is responsible for defining, implementing, and enforcing security policies.
- Regular security audits and assessments will be conducted to ensure compliance.
- Employees will undergo security awareness training.

3. Access Control Policy

- Access to company systems and data will be based on the principle of least privilege (PoLP).
- Multi-factor authentication (MFA) will be enforced for all critical systems.
- Access logs will be maintained and reviewed periodically.

- Employees must report lost/stolen credentials immediately.

4. Data Protection Policy

- Sensitive data must be encrypted at rest and in transit.
- End-to-end encryption (E2EE) will be enforced for communication channels.
- Data access will be restricted based on user roles.
- Data retention and disposal policies will be strictly followed.

5. Network Security Policy

- Firewalls and intrusion detection/prevention systems (IDS/IPS) will be implemented.
- Regular security patches and updates will be applied to all systems.
- Secure VPNs must be used for remote access.

6. Endpoint Security Policy

- Company devices must have up-to-date antivirus and endpoint detection solutions.
- Personal devices accessing company data must comply with security policies.
- Automatic device locking and encryption will be enforced.

7. Incident Response Policy

- A formal incident response plan (IRP) will be maintained.
- Security incidents must be reported to the security team immediately.
- Post-incident analysis will be conducted to prevent future occurrences.

8. Vendor and Third-Party Security Policy

- Vendors and partners must comply with Bluekyte AI's security policies.
- Regular security assessments will be conducted on third-party services.

- Data shared with third parties must be encrypted and access controlled.

9. Security Awareness and Training

- All employees must complete security awareness training annually.
- Phishing simulation exercises will be conducted regularly.
- Security best practices will be communicated to all staff.

10. Compliance and Legal Considerations

- Bluekyte AI is bound to comply with relevant laws and regulations (e.g., GDPR, DPDPA) and complies with HIPAA and CCPA via existing partners.
- Regular audits will be conducted to ensure compliance.
- Employees must adhere to all security and privacy policies.

11. Policy Review and Updates

- This security policy will be reviewed and updated annually.
- Employees will be notified of significant changes to security policies.

Approval:

Abhishek

Devops Engineeer, Bluekyte AI

Date: 25th March 2025