IT Security Policy

Artificial Intelligence (AI) Usage Guidelines

1. Purpose

This policy establishes guidelines for the secure and compliant use of Artificial Intelligence (AI) platforms, tools, and services within the organization. It aims to protect company data, ensure regulatory compliance, and promote responsible AI usage across all departments.

2. Scope

This policy applies to all employees, contractors, consultants, and third-party personnel who access or use AI tools and services in connection with company business operations.

3. Approval for Usage

- Any use of AI platforms, tools, or services must receive prior approval from the IT team.
- Employees must submit an AI Tool Request Form detailing the intended use case, data involved, and business justification.
- The IT team will evaluate requests based on security, compliance, and business requirements.

4. Company Email Usage

- Employees are required to use company-provided email accounts for all AI-related activities.
- Personal email addresses must not be used for any AI-related work, including account registration, communication, or data sharing.
- This ensures proper audit trails and compliance with data governance requirements.

5. Use of Free-Tier Accounts

- For research, testing, or experimental purposes, employees must utilize free-tier accounts of AI services whenever possible.
- Free-tier limitations should be documented when requesting approval for paid services.
- Testing environments should be isolated from production data.

6. Paid AI Services

- Paid credits or tokens for AI services may only be used for business-critical tasks or other important projects.

- Prior approval from the IT team is required for the use of paid AI services, and this approval must be documented in advance.
- Employees must seek IT team approval before making any purchases related to AI services that involve payment.
- Monthly usage reports must be submitted to the IT and Finance departments.

7. Data Privacy and Security

- Employees must ensure that no sensitive or confidential company data is uploaded to any AI platform without proper encryption or anonymization.
- All AI tools must comply with the company's data privacy policies and applicable regulations, such as GDPR, HIPAA, or other industry-specific standards.
- Data classification must be performed before any data is processed by AI tools.
- Personal Identifiable Information (PII) must never be shared with external AI services without explicit authorization.

8. Restricted AI Use Cases

- Employees are prohibited from using AI tools for any illegal, unethical, or unauthorized purposes, including but not limited to fraud, discrimination, or harassment.
- AI tools should not be used for activities that may harm the reputation of the company, its stakeholders, or the public.
- Generation of misleading content, deepfakes, or impersonation is strictly prohibited.
- Using AI to circumvent security controls or access unauthorized systems is forbidden.

9. AI Model Training and Customization

- Any AI model training or fine-tuning should be done under the supervision of the IT or data science teams to ensure that data is appropriately prepared and processed.
- Employees should avoid uploading proprietary or private datasets to AI platforms unless explicitly approved by the IT team.
- All custom models must be documented and version-controlled.
- Training data must be reviewed for bias and accuracy before use.

10. Audit and Monitoring

- The IT team will periodically audit AI tool usage to ensure compliance with internal policies.
- Employees must cooperate with any audits or monitoring efforts related to AI usage.
- Audit logs will be retained for a minimum of 12 months.
- Non-compliance may result in disciplinary action.

11. Reporting Security Vulnerabilities

- If any employee discovers a potential security vulnerability or flaw in any AI tool, they must report it immediately to the IT security team for evaluation and remediation.
- Reports should include: description of the vulnerability, steps to reproduce, potential impact, and any evidence.
- The IT security team will acknowledge receipt within 24 hours and provide updates on remediation progress.

12. Integration with Company Systems

- Any AI tool integrated into company systems (e.g., CRM, ERP, HR software) must undergo a thorough security review by the IT team before integration.
- Employees must refrain from integrating personal or non-approved AI tools into company systems.
- API connections must use secure authentication methods and encrypted channels.
- Integration documentation must be maintained and updated regularly.

13. Account and Credential Management

- Employees must use company-provided accounts and credentials for accessing AI platforms. Sharing of login credentials or accounts is prohibited.
- If an employee leaves the company, their AI accounts and access must be promptly disabled.
- Multi-factor authentication (MFA) must be enabled on all AI platform accounts where available.
- Passwords must comply with the company's password policy requirements.

14. Training and Awareness

- Employees should complete any required training related to AI tool usage and security before using AI services.
- Regular refresher courses or updates on AI best practices and security should be taken to ensure ongoing compliance with company policies.
- Training completion records will be maintained by HR and reviewed during performance assessments.

15. Reporting Misuse

- Any employee who observes or suspects the misuse of AI tools (e.g., violating usage policies, engaging in unethical practices) should report the incident to the appropriate authority in the company (e.g., IT team, HR).
- Reports can be made anonymously through the company's ethics hotline.
- Retaliation against reporters is strictly prohibited.

16. Access Control

- Access to AI tools should be restricted based on the role of the employee. Employees will only have access to AI tools that are necessary for their job functions.
- Access rights will be reviewed quarterly and adjusted as needed.
- Privileged access requires additional approval and enhanced monitoring.

17. Compliance with Industry Standards

- Employees must ensure that any AI tools used comply with relevant industry standards, certifications, and regulations that the company adheres to.
- AI tools and services used for business operations must be regularly evaluated to ensure they meet the company's compliance requirements.
- Applicable frameworks include: SOC 2, ISO 27001, NIST Cybersecurity Framework, and industry-specific regulations.

18. Policy Violations

Violations of this policy may result in disciplinary action, up to and including termination of employment. Serious violations may be referred to law enforcement authorities. Examples of violations include:

- Unauthorized use of AI tools
- Uploading sensitive data without authorization
- Sharing credentials with unauthorized individuals
- Failure to report security incidents or misuse

19. Policy Review

This policy will be reviewed annually or as needed to address emerging AI technologies, evolving security threats, and changes in regulatory requirements. Updates will be communicated to all employees and require acknowledgment.

Acknowledgment

I have read, understood, and agree to comply with this IT Security Policy for AI Usage.

_____

Employee Name (Print)

_____

Employee Signature

_____

Date