**[Company Name] Artificial Intelligence (AI) Usage Policy**

**Effective Date:** [Date]

**Last Updated:** [Date]

**Version Number:** [Version]

**Policy Owner:** [Responsible Department/Individual]

**Approval Authority:** [Approval Entity]

**Policy Contact Information:** [Contact Details]

Table of Contents

[Purpose](#_4rcsek60wq0c)

[Scope](#_m9g9vkx8ilio)

[Definitions](#_549nw98hk8u7)

[Policy Statement](#_r3zptoto8xab)

[Guiding Principles](#_mpvuzvyeu5vb)

[Ethical Use](#_aqu3vse3wytf)

[Data Privacy and Protection](#_scwfndbds7hw)

[Transparency and Accountability](#_39urj7pnh7zx)

[Legal Compliance](#_ppybeji9y22e)

[Risk Management](#_1s51f4qp806g)

[Training and Awareness](#_7qf1mkfhg693)

[Review and Oversight](#_fr888xngyu4k)

[Stakeholder Assurance](#_vczwlbbjefn3)

[Innovation Encouragement](#_8o19p1y2mtc)

[Third-Party Vendors and Outsourcing](#_6g9sjxieovw6)

[Personal Devices](#_t1hiukp1jxdw)

[Reporting and Violations](#_dzm97ra5ptj0)

[Revision and Updates](#_jvi9hh645to2)

[Related Documents](#_mvn9sr86z6a9)

[Revision History](#_rpo24g2g52nb)

#### Purpose

 This policy establishes guidelines and practices for the ethical, responsible, and secure use of Artificial Intelligence (AI) within [Company Name]. It ensures the proper utilization, transparency, and protection of AI technologies, supporting innovation while complying with international standards and safeguarding sensitive data.

#### Scope

 This policy applies to all [Company Name] employees, contractors, third-party vendors, and partners who utilize or interact with AI technologies on behalf of the company.

#### Definitions

* AI (Artificial Intelligence): Technologies that enable machines to simulate human intelligence.
* Confidentiality: Ensuring sensitive data is protected from unauthorized access.
* Integrity: Maintaining the accuracy and completeness of data.
* Availability: Ensuring that data and systems are accessible when needed.
* Least Privilege: Granting the minimum level of access necessary.
* Need to Know: Limiting access to information strictly to those who require it for their role.

#### Policy Statement

##### Guiding Principles

* Confidentiality: Protect sensitive data and ensure it is inaccessible to unauthorized entities.
* Integrity: Preserve the accuracy and completeness of data and AI processes.
* Availability: Ensure data and AI systems are available when required.
* Privacy: Respect individual data rights and adhere to privacy regulations, including GDPR.
* Least Privilege: Grant access only to those who absolutely need it.
* Need to Know: Limit data access and processing to only necessary entities.

##### Ethical Use

* Fairness: Avoid biases in AI models and ensure fairness in outcomes.
* Transparency: AI implementations should be transparent about their purpose, data sources, and decision-making processes.
* Prevent Harm: Actively monitor and prevent harm from AI systems, including misleading or harmful information dissemination.

##### Data Privacy and Protection

* Anonymization and Encryption: Data utilized by AI should be anonymized when possible and encrypted both in transit and at rest.
* Regular Audits: Regularly audit and evaluate data sources to ensure adherence to privacy laws and ethical standards.
* Data Retention Policy: Ensure a data retention policy that deletes data no longer needed, ensuring compliance with GDPR and other international data protection laws.

##### Transparency and Accountability

* Stakeholder Communication: Clearly communicate the usage and outcomes of AI systems to stakeholders.
* Audit Trails: Maintain an audit trail of AI decisions and the data that influenced them.
* Regular Reviews: Regularly review and assess AI models and algorithms for accuracy, fairness, and other ethical concerns.

##### Legal Compliance

* Stay Updated: Stay updated with local, national, and international laws concerning AI, data privacy, and related areas.
* Compliance Standards: Ensure AI technologies comply with standards like ISO/IEC 27001, NIST, PCI DSS, HIPAA, GDPR, SOC 2, OWASP, CMMC, COBIT, and others as applicable.
* Legal Review: Engage legal counsel to periodically review AI endeavors for potential legal implications.

##### Risk Management

* Risk Identification: Identify potential risks associated with AI projects, including reputational, legal, and technical risks.
* Mitigation Strategies: Develop mitigation strategies for identified risks and regularly review and update these strategies.

##### Training and Awareness

* Regular Training: Organize regular training sessions for employees and stakeholders to ensure they understand this policy and the ethical considerations of AI.
* Updated Materials: Continually update training materials to reflect technological advancements and regulatory changes.

##### Review and Oversight

* Regular Audits: Conduct regular audits of AI systems to ensure adherence to this policy and associated regulations.
* Policy Review: Review this policy at least annually to ensure it remains current and comprehensive.

##### Stakeholder Assurance

* Ethical Commitment: Actively communicate our commitment to ethical AI usage to all stakeholders, including employees, customers, partners, and investors.
* Feedback and Concerns: Address concerns and feedback regarding our AI systems promptly and transparently.

##### Innovation Encouragement

* Guided Innovation: Encourage teams to innovate within the guidelines of this policy, promoting the development of beneficial and responsible AI technologies.
* Recognition: Recognize and reward innovations that align with this policy’s principles.

##### Third-Party Vendors and Outsourcing

* Vendor Compliance: Ensure all third-party vendors adhere to this AI policy.
* Regular Reviews: Regularly review and audit third-party AI systems for compliance, data protection, and ethical standards.

##### Personal Devices

* Security Compliance: Authorized employees using personal devices to access or interact with AI systems must ensure they comply with IT's security protocols and monitoring.
* Up-to-date Security: Personal devices must have up-to-date security software and be encrypted to protect company data.

#### Reporting and Violations

* Encouraged Reporting: Employees and stakeholders are encouraged to report any violations of this policy or any concerns related to AI usage.
* Disciplinary Actions: Violations of this policy can result in disciplinary action, up to and including termination.

#### Revision and Updates

* Policy Updates: This policy will be revised as necessary to reflect technological advancements, regulatory changes, and feedback from stakeholders.

#### Related Documents

[List of related policies, procedures, or documents]

#### Revision History

| Date | Version | Description | Approved By |
| --- | --- | --- | --- |
| 2024-06-18 | 1.0 | Initial Release | Mark Annati |
|  |  |  |  |
|  |  |  |  |

Note: This AI usage policy is a general framework and needs customization to fit specific organizational needs. It is also essential to consult with legal counsel in the jurisdictions the company operates to ensure full compliance.