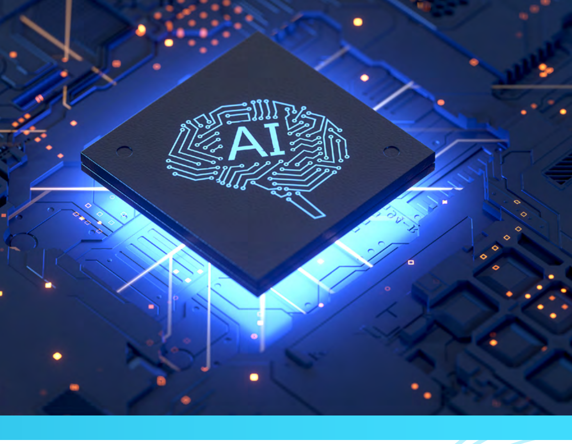
Artificial Intelligence Use Policy Template

This template is provided as an example and does not constitute legal advice. To ensure the template meets your needs, please consult your legal and compliance teams. This document should be customized to fit your specific needs, context, and organizational requirements.



1.0 Purpose

The purpose of this policy is to establish guidelines and best practices for the responsible, ethical, and secure use of artificial intelligence (AI) technologies within our organization. This policy applies to all forms of AI technologies including but not limited to Generative AI, Agentic AI, Predictive AI, Conversational AI, and Cognitive AI.

2.0 Scope

This policy applies to every individual involved in the use, development, or management of AI technologies on behalf of the organization. This includes employees, contractors, partners, and vendors. It also covers all organizational data and systems that interact with or are impacted by AI technologies.

3.0 Risks

There are significant risks associated with the use of AI tools, particularly those available on the web.

- AI tools available on the web are not private. Any data you submit to an AI tool may be used for training with the AI model and could become available to other users.
- AI's training data may include copyrighted materials and violate the rights of others.
- AI tools may provide biased results based on their training and data.
- AI tools are not accurate. Information may be outdated, misleading, or fabricated.

4.0 Acceptable Use

Only use AI platforms that have been approved by the organization, and solely for tasks and data that have been specifically authorized.

- Your use of AI must align with our values, ethics, and quality standards.
- Do not share your username or passwords to an AI platform with anyone else.
- Do not use AI content that is misleading, harmful, offensive, or discriminatory.
- You must verify the accuracy of any results from AI.
- Unless we provide otherwise, do not input any sensitive or protected data into AI systems, such as:
  - Personally identifiable information (PII).
  - Personal health information (PHI and ePHI).
  - Our intellectual property or trade secrets.
  - Strategic information, including AI requests that inadvertently give away our plans and strategy (for example, asking ChatGPT to summarize notes from a board meeting during which directors discussed financial updates and other strategies that are confidential).
  - Financial data.

5.0 Approval and Governance

- Our IT team and Executive Leadership must evaluate and approve any use of AI.
- Our evaluation process must include a review of the tool's security features, terms of service, privacy policy and confirmation that such tools meet the AI Risks and Trustworthiness Framework offered by the National Institute of Standards and Technology.
- The IT Team shall maintain a list of authorized AI platforms, integrations, and use cases aligned with our data classification policies.
- An AI Governance Committee shall be established responsible for overseeing the strategy, implementation, and compliance of AI technologies.
- The Committee will review and approve high-risk AI projects, maintain documentation, and ensure ongoing alignment with organizational values and regulatory requirements.
- The Committee will engage stakeholders in the ethical development and deployment of AI and periodically review this policy to address emerging risks and advancements.

6.0 Training

- All employees, contractors, and relevant third parties must complete mandatory training on responsible AI use, data privacy, and security before accessing or deploying AI technologies.
- Training will be updated regularly to reflect new risks, technologies, and regulatory requirements.
- Additional specialized training will be provided for those directly involved in developing, deploying, or managing AI systems.

7.0 Incident Response Guidelines

- Any suspected or confirmed AI-related incident (e.g., data breach, misuse, bias, or system failure) must be reported immediately to the IT team and the AI Governance Committee.
- The organization will investigate all AI incidents promptly, assess the impact, and take corrective actions as necessary.
- Incident response procedures will include containment, eradication, recovery, and post-incident review to prevent recurrence.
- All incidents will be documented, and lessons learned will be incorporated into future policy updates and training.

8.0 Compliance with Laws and Regulations

All users of AI must comply with applicable laws, regulations, and ethical guidelines governing intellectual property, privacy, data protection, and other relevant areas. We prohibit unauthorized use of copyrighted material or creation of content that infringes on the intellectual property of others.

9.0 Non-Compliance

Non-Compliance with this policy may result in disciplinary action, up to and including termination of employment or contract. Violation of laws may also result in civil and criminal prosecution.

10.0 Policy Review

We will review and update this policy periodically to address emerging risks, technological advancements, and regulatory changes.