ACME Corporation

Artificial Intelligence Usage Policy

Version 2.0
Effective Date: January 1, 2025
Last Revised: October 25, 2025

Executive Summary

This Artificial Intelligence Usage Policy establishes guidelines and requirements for the responsible development, deployment, and use of AI technologies at ACME Corporation. Our commitment is to leverage AI in ways that enhance business value, respect individual rights, ensure transparency, and maintain the highest ethical standards. All employees, contractors, and partners working with AI systems must adhere to this policy.

1. Purpose and Scope

The purpose of this policy is to:

- Establish clear guidelines for ethical and responsible AI use
- Ensure compliance with applicable laws, regulations, and industry standards
- Protect the rights and privacy of individuals whose data may be processed by AI systems
- Mitigate risks associated with AI deployment including bias, discrimination, and security vulnerabilities
- Promote transparency and accountability in AI decision-making processes
- Foster innovation while maintaining appropriate governance and oversight

This policy applies to all AI systems, machine learning models, automated decision-making tools, and generative AI applications used or developed by ACME Corporation, regardless of whether they are developed in-house, purchased from vendors, or accessed via third-party services.

2. Definitions

Term	Definition

Artificial Intelligence (AI)	Systems that can perform tasks that typically require human intelligence, including learning, reason
Machine Learning (ML)	A subset of AI where systems learn from data and improve performance without explicit programm
Generative AI	AI systems capable of creating new content including text, images, code, or other media based on
Large Language Model (LLM)	AI models trained on vast amounts of text data to understand and generate human-like text.
Automated Decision System	Any AI system that makes or significantly influences decisions affecting individuals without human
AI Training Data	Data used to train, validate, or test AI models and systems.
Bias	Systematic errors in AI outputs that create unfair outcomes for certain groups or individuals.

3. AI Governance Structure

ACME Corporation has established a multi-tiered governance structure to oversee AI initiatives:

3.1 AI Ethics Committee

The AI Ethics Committee, composed of executives, legal counsel, data scientists, and ethics experts, is responsible for reviewing high-risk AI applications, establishing ethical guidelines, and ensuring compliance with this policy. The committee meets quarterly and reviews all AI systems classified as high-risk before deployment.

3.2 Chief AI Officer (CAIO)

The CAIO oversees all AI initiatives, ensures policy compliance, manages AI-related risks, and serves as the primary point of contact for AI governance matters. The CAIO reports directly to the CEO and the AI Ethics Committee.

3.3 AI Review Boards

Department-level AI Review Boards evaluate AI proposals, conduct impact assessments, and monitor ongoing AI deployments within their respective areas.

4. Acceptable Use Guidelines

4.1 Permitted Uses

AI systems may be used for:

- Enhancing productivity and efficiency in business operations
- Automating repetitive tasks that do not require human judgment
- Data analysis and generating insights to support decision-making
- Improving customer experience through personalization and support
- Research and development of new products and services
- Code generation and software development assistance
- Content creation and editing with appropriate human oversight

4.2 Prohibited Uses

AI systems must NOT be used for:

- Making final employment decisions (hiring, firing, promotions) without human review

- Determining creditworthiness or financial eligibility without human oversight
- Creating deepfakes or synthetic media intended to deceive
- Surveillance or monitoring that violates privacy rights or regulations
- Developing weapons systems or tools intended to cause harm
- Discriminating against protected classes or vulnerable populations
- Circumventing security controls or accessing unauthorized information
- Processing personal data without proper legal basis and consent

5. AI Risk Classification

All AI systems must be classified according to their potential risk level:

Risk Level	Description	Examples	Requirements
Minimal Risk	Low impact on individuals and operations	Spam filters, recommendation engines	Standard testing, documentation
Limited Risk	Moderate impact requiring transparency	Chatbots, virtual assistants, predictive analytics	User notification, human oversight option
High Risk	Significant impact on rights or safety	Hiring tools, credit scoring, medical diagnostics, facial recognition	Mandatory human review, bias testing, impact assessment
Unacceptable Risk	Poses clear threat to safety or rights	Social scoring, real-time biometric surveillance, subliminal manipulation	PROHIBITED

6. Data and Privacy Requirements

6.1 Data Collection and Use

AI training and operation must comply with all applicable data protection laws including GDPR, CCPA, and other relevant regulations. Personal data used for AI must:

- Have a clear legal basis for processing
- Be collected transparently with appropriate notice
- Be limited to what is necessary and relevant
- Be accurate and kept up to date
- Be retained only as long as necessary
- Be protected with appropriate security measures

6.2 Data Minimization

AI systems should be designed to minimize data collection and processing. Preference should be given to techniques such as federated learning, differential privacy, and synthetic data generation when appropriate.

6.3 Third-Party AI Services

When using external AI services (e.g., ChatGPT, Claude, other LLMs), employees must:

- Never input confidential, proprietary, or personal information
- Review and accept the service's terms of use and privacy policy
- Verify that the service provider has adequate security measures
- Obtain approval from IT Security for enterprise-wide AI tool adoption
- Understand that inputs may be used to train third-party models

7. Fairness and Bias Mitigation

7.1 Bias Prevention

All AI systems must be evaluated for potential bias before deployment. Development teams must:

- Use diverse and representative training datasets
- Test for disparate impact across protected characteristics
- Document any identified biases and mitigation strategies
- Implement ongoing monitoring for bias in production systems
- Establish feedback mechanisms for reporting bias concerns

7.2 Fairness Metrics

High-risk AI systems must be evaluated using appropriate fairness metrics such as demographic parity, equal opportunity, or equalized odds, depending on the use case. Metrics must be documented and reviewed regularly.

8. Transparency and Explainability

8.1 User Notification

Users must be informed when they are interacting with an AI system. For automated decision-making that significantly affects individuals, clear explanations of the decision process must be provided.

8.2 Documentation Requirements

All AI systems must maintain documentation including:

- Purpose and intended use of the system
- Description of the AI model and its capabilities
- Training data sources and characteristics
- Performance metrics and evaluation results
- Known limitations and failure modes
- Risk assessment and mitigation strategies
- Monitoring and maintenance procedures

9. Security Requirements

AI systems must adhere to ACME Corporation's information security standards and implement appropriate safeguards:

- Secure development lifecycle practices for AI models
- Protection against adversarial attacks and model poisoning
- Access controls and authentication for AI system interfaces
- Encryption of sensitive data used in AI processing
- Regular security assessments and penetration testing
- Incident response procedures for AI-related security events
- Secure model storage and version control

10. Human Oversight and Control

High-risk AI systems must include meaningful human oversight. This means:

- Humans must be able to understand AI system outputs and limitations
- Humans must have the ability to override AI decisions when necessary
- Clear escalation procedures must exist for challenging AI outputs
- Regular human review of AI system performance and outcomes
- Training programs for employees working with AI systems

11. Intellectual Property Considerations

11.1 AI-Generated Content

Content generated by AI systems should be reviewed and edited by humans before external use. AI-generated content must not infringe on copyrights, trademarks, or other intellectual property rights. When AI is used to create content, appropriate attribution and disclosure should be provided where required.

11.2 Training Data Rights

Organizations must have appropriate rights and licenses for all data used to train AI models. Publicly available data does not automatically grant permission for AI training purposes.

12. Monitoring and Auditing

AI systems must be continuously monitored for:

- Performance degradation or model drift
- Emergence of bias or fairness issues
- Security vulnerabilities or attacks
- Compliance with applicable regulations
- User feedback and complaints
- Unintended consequences or harmful outputs

High-risk AI systems must undergo annual audits by internal or external auditors to verify compliance with this policy and applicable regulations.

13. Training and Awareness

All employees working with AI systems must complete mandatory AI ethics and responsible use training. Developers, data scientists, and product managers must complete advanced training on bias mitigation, fairness, and AI security. Training must be refreshed annually.

14. Incident Response and Reporting

Any incidents involving AI systems must be reported immediately to the CAIO and IT Security. Incidents include:

- Discriminatory outcomes or bias discovered in production
- Security breaches or adversarial attacks
- Data privacy violations
- System malfunctions causing harm or significant business impact
- Unauthorized use of AI systems
- Regulatory inquiries or complaints

The AI Ethics Committee will investigate significant incidents and implement corrective actions as needed.

15. Compliance and Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment. In addition, violations may expose individuals and the company to civil or criminal liability. All employees have a responsibility to report suspected policy violations to their manager, the CAIO, or through the company's ethics hotline.

16. Policy Review and Updates

This policy will be reviewed and updated at least annually, or more frequently as needed to address emerging technologies, regulatory changes, or lessons learned from AI deployments. The AI Ethics Committee is responsible for policy updates, which must be approved by the Executive Leadership Team.

Policy Approved by:

Jennifer Martinez	**David Kim**	**Sarah Johnson**
Chief Executive Officer	**Chief AI Officer**	**Chief Compliance Officer**
Date: January 1, 2025	Date: January 1, 2025	Date: January 1, 2025

Appendix A: AI System Approval Workflow

Step	Action	Responsible Party	Timeline
1	Submit AI proposal with use case description	Project Sponsor	1 day
2	Initial risk classification	Department AI Review Board	3-5 days
3	Detailed impact assessment (high-risk only)	AI Team + Legal	2-3 weeks
4	Security and privacy review	IT Security + Privacy Officer	1-2 weeks
5	Ethics Committee review (high-risk only)	AI Ethics Committee	1-2 weeks
6	Final approval and deployment authorization	CAIO	1 week
7	Post-deployment monitoring setup	AI Operations Team	Ongoing

Appendix B: Key Contacts

Chief AI Officer (CAIO)

David Kim

Email: david.kim@acmecorp.com

Phone: (555) 123-4570

AI Ethics Committee

Email: ai-ethics@acmecorp.com

IT Security

Email: security@acmecorp.com

Phone: (555) 123-4571

Legal Department

Email: legal@acmecorp.com

Phone: (555) 123-4568

Ethics Hotline

Phone: 1-800-ETHICS-1 (1-800-384-4271)

Available 24/7, anonymous reporting available