AI Policy

(Artificial Intelligence Guidelines)

SAMPLE DOCUMENT

This is a watermarked sample showing actual policy output quality.

Your tailored policy will reflect your specific company context and AI usage.

Scan for more information

Organisation:	Acme Corporation Ltd.
Industry:	Technology / IT
Document Version:	1.0 (Sample)
Generated:	January 2026
Frameworks:	EU AI Act, ISO 42001, GDPR
AI Tools:	ChatGPT, Gemini, Claude
Automated Decisions:	Yes
Sensitive Data:	No

AI Policy (Artificial Intelligence Guidelines)

IMPORTANT NOTICE

Automatically generated - not legal advice

This document was automatically generated by AI and does not constitute legal advice. It serves exclusively as guidance. For binding legal advice, please consult a lawyer or legal expert.

Company: Acme Corporation Ltd.
Generated Language: English
Industry: technology
Creation date: 18.01.2026 15:44:59

AI Policy for Technology Company: EU AI Act, ISO/IEC 42001, and GDPR Compliance

1. Introduction and Legal Framework

This AI Policy establishes the principles, procedures, and controls governing the use of artificial intelligence (AI) systems within the company. The policy ensures compliance with the EU AI Act (Regulation EU 2024/1689), ISO/IEC 42001:2023 AI Management System Standard, the General Data Protection Regulation (GDPR), and relevant technology industry regulations.

The company is committed to responsible, ethical, and transparent use of AI technologies, including ChatGPT, Google Gemini, and Claude AI, to deliver personalized experiences for customers and employees. This policy applies to all AI-related activities, systems, and processes within the organization.

2. Scope and Definitions

This policy applies to all employees, contractors, and third parties involved in the development, deployment, management, or use of AI systems within the company.

For the purposes of this policy, the following definitions apply:

AI System: Any software or hardware system that uses machine learning, natural language processing, or other forms of artificial intelligence to perform tasks that would otherwise require human intelligence.

Automated Decision-Making: Any process where an AI system makes decisions without direct human intervention, including but not limited to personalized recommendations and behavioral analysis.

Personal Data: Any information relating to an identified or identifiable natural person, as defined by GDPR.

High-Risk AI System: An AI system classified as high-risk under the EU AI Act due to its potential impact on individuals' rights, safety, or legal status.

3. EU AI Act Compliance and Risk Classification

The company classifies its AI systems in accordance with the EU AI Act. The use of ChatGPT, Google Gemini, and Claude AI for automated decision-making constitutes a high-risk AI application due to its influence on individuals' experiences and potential impact on their rights.

The following compliance actions are required:

[ ] Conduct and document a comprehensive risk assessment for each AI system in use.

[ ] Register all high-risk AI systems in the EU AI Act database as required.

[ ] Implement mandatory risk mitigation measures, including human oversight and technical safeguards.

[ ] Ensure conformity assessment procedures are completed before deployment.

[ ] Maintain up-to-date technical documentation and logs for all high-risk AI systems.

[ ] Establish mechanisms for user feedback and redress.

4. ISO 42001 AI Management System

The company implements an AI Management System (AIMS) in accordance with ISO/IEC 42001:2023 to ensure systematic governance, risk management, and continual improvement of AI activities.

The following actions are required:

[ ] Define and document the AI policy, objectives, and scope.

[ ] Assign roles and responsibilities for AI governance.

[ ] Establish processes for risk assessment, monitoring, and review of AI systems.

[ ] Integrate AI management with existing information security and quality management systems.

[ ] Conduct regular internal audits of the AIMS.

[ ] Review and update the AIMS at least annually.

5. Governance Structure and Responsibilities

The company establishes a clear governance structure for AI oversight and compliance.

[ ] Appoint an AI Compliance Officer responsible for regulatory adherence and policy enforcement.

[ ] Define responsibilities for AI system owners, developers, and users.

[ ] Establish an AI Ethics Committee to review high-risk AI deployments.

[ ] Ensure management oversight of AI risk management and compliance activities.

[ ] Maintain records of governance decisions and actions.

6. Specific Regulations for AI Tools Used

Tool	Use Case	Risk Level	Key Compliance Actions
ChatGPT	Personalized recommendations for customers/employees	High	[ ] Conduct risk assessment [ ] Register as high-risk [ ] Implement human oversight [ ] Maintain logs
Google Gemini	Behavioral analysis and experience personalization	High	[ ] Conduct risk assessment [ ] Register as high-risk [ ] Implement human oversight [ ] Maintain logs
Claude AI	Automated decision support for user interactions	High	[ ] Conduct risk assessment [ ] Register as high-risk [ ] Implement human oversight [ ] Maintain logs

7. Data Protection and GDPR Compliance

The company ensures that all AI activities comply with GDPR and data protection requirements, even though no sensitive or personal data is processed by the AI systems as currently configured.

[ ] Conduct Data Protection Impact Assessments (DPIA) for all AI systems.

[ ] Apply privacy by design and by default principles in AI system development.

[ ] Ensure data minimization and purpose limitation for all data processed by AI systems.

[ ] Implement technical and organizational measures to safeguard data integrity and confidentiality.

[ ] Maintain records of processing activities related to AI systems.

[ ] Review data protection measures annually or upon significant changes.

8. Risk Management and Security Measures

The company adopts a risk-based approach to AI system security and reliability.

[ ] Identify and assess risks associated with each AI system.

[ ] Implement appropriate technical and organizational controls to mitigate identified risks.

[ ] Ensure robust access controls and authentication for AI system management.

[ ] Monitor AI system performance and security continuously.

[ ] Establish incident detection and response procedures for AI-related risks.

[ ] Review risk management measures at least annually.

9. Transparency and Documentation Requirements

The company is committed to transparency in AI system operation and decision-making.

[ ] Provide clear information to users about the use and purpose of AI systems.

[ ] Maintain comprehensive technical documentation for each AI system, including algorithms, data sources, and decision logic.

[ ] Log all significant AI system activities and decisions.

[ ] Make documentation available to regulators upon request.

[ ] Inform users of their rights regarding AI-driven decisions.

[ ] Update documentation promptly following any system changes.

10. Training and Knowledge Transfer

The company ensures that all relevant personnel are trained in AI compliance, ethics, and risk management.

[ ] Develop and deliver mandatory AI compliance training for employees and contractors.

[ ] Provide specialized training for AI developers and system owners.

[ ] Maintain training records and review training content annually.

[ ] Facilitate knowledge transfer on regulatory updates and best practices.

[ ] Evaluate training effectiveness through regular assessments.

11. Monitoring, Audit and Continuous Improvement

The company establishes ongoing monitoring and audit processes to ensure AI compliance and performance.

[ ] Monitor AI system outputs and impacts continuously.

[ ] Conduct regular internal audits of AI systems and compliance controls.

[ ] Review audit findings and implement corrective actions.

[ ] Solicit feedback from users and stakeholders on AI system performance.

[ ] Update AI systems and controls based on audit results and technological advancements.

[ ] Document all monitoring and improvement activities.

12. Incident Response and Reporting Obligations

The company maintains procedures for prompt response to AI-related incidents and regulatory reporting.

[ ] Establish an AI incident response plan, including roles and escalation procedures.

[ ] Detect, document, and investigate all AI-related incidents.

[ ] Notify affected parties and regulators of incidents as required by law.

[ ] Implement corrective actions to prevent recurrence.

[ ] Review and update incident response procedures annually.

[ ] Maintain an incident log for all AI-related events.

13. Stakeholder Management

The company engages with internal and external stakeholders to ensure responsible AI use.

[ ] Identify and map all stakeholders affected by AI systems.

[ ] Communicate AI policy, risks, and user rights to stakeholders.

[ ] Establish channels for stakeholder feedback and concerns.

[ ] Incorporate stakeholder input into AI system design and governance.

[ ] Review stakeholder engagement processes annually.

14. Implementation Plan and Timeline

Action Item	Responsible Role	Deadline	Status
Appoint AI Compliance Officer	Management	18.02.2026	[ ] Pending
Conduct risk assessments for all AI tools	AI Compliance Officer	18.03.2026	[ ] Pending
Register high-risk AI systems	AI Compliance Officer	18.03.2026	[ ] Pending
Develop and deliver AI compliance training	HR / Training Manager	18.04.2026	[ ] Pending
Implement technical and organizational controls	IT Security Lead	18.04.2026	[ ] Pending
Complete conformity assessment procedures	AI Compliance Officer	18.04.2026	[ ] Pending
Establish AI Ethics Committee	Management	18.03.2026	[ ] Pending
Conduct Data Protection Impact Assessments (DPIA)	Data Protection Officer	18.03.2026	[ ] Pending
Integrate AIMS with existing management systems	Quality Manager	18.07.2026	[ ] Pending
Conduct internal audit of AI Management System	Internal Auditor	18.01.2027	[ ] Pending

Document Hash (SHA-256): c0578c29a87facdb14396620e7f614aaddf52ace807e11d0ea4f95d6fc3fb5a0
Timestamp: 18.01.2026 15:44:59 UTC

This document was automatically generated.