Corporate AI Policy Template

Introduction

Artificial Intelligence Policy Template

This policy template provides a framework for establishing safe and compliant artificial intelligence (AI) use within your organisation. It addresses governance, risk management, user guidelines and compliance considerations. Adapt it to suit your organisation's specific needs, risk profile and industry requirements.

This template was provided by Lanboss AI as a starting framework for corporate institutions. For comprehensive policy development support, including implementation guides, stakeholder communication templates and staff training materials, contact Lanboss AI at info@lanboss.ai or visit www.lanboss.ai.

Implementation Guidance

To effectively implement this policy, consider the following steps:

1. **Form an AI Working Group** with representatives from users, Security, IT and leadership
2. **Customise this template** to reflect your organisation's specific needs and values
3. **Conduct stakeholder consultations** to gather feedback before finalisation
4. **Develop a communications plan** to ensure all users understand the policy
5. **Create supporting materials** such as user guides and kitchen posters
6. **Establish regular review cycles** to keep the policy current with technological changes, because these are happening rapidly

1. Introduction

1.1 Purpose

This policy establishes guidelines for the responsible acquisition, development, deployment and use of AI systems within [ORGANISATION NAME].

1.2 Scope

This policy applies to:

- All employees, contractors and third parties using AI tools on behalf of the organisation
- All AI systems whether developed internally, purchased from vendors or accessed as services
- Both public AI platforms (e.g., ChatGPT, Claude) and private AI implementations
- Data used to train, test or operate AI systems

2. Roles and Responsibilities

2.1 AI Governance Committee

- Oversees AI policy implementation and compliance
- Reviews and approves AI use cases
- Maintains AI inventory and risk register
- Reports to senior leadership on AI activities
- Members include: [LIST RELEVANT POSITIONS]

2.2 Managers

- Ensure team members understand and follow this policy
- Review AI use within their department
- Request approvals for new AI implementations
- Report incidents and non-compliance

2.3 All Staff

- Complete required AI literacy training
- Follow approval processes before using new AI tools
- Report concerns or potential misuse
- Adhere to data handling protocols when using AI

2.4 IT/Security Teams

- Implement technical safeguards for AI systems
- Monitor AI system access and usage
- Conduct security assessments of AI implementations
- Support incident response for AI-related issues

3. AI System Classification

All AI systems must be classified according to risk level:

3.1 Low Risk

- Systems with minimal privacy, security or operational impact
- Examples: basic document summarisation, simple data analysis
- Requirements: departmental approval, basic documentation

3.2 Medium Risk

- Systems affecting operational efficiency or using non-sensitive data
- Examples: customer service chatbots, operational forecasting
- Requirements: AI Governance Committee approval, vendor assessment, training

3.3 High Risk

- Systems using sensitive data or affecting critical decisions
- Examples: HR screening tools, credit decisioning, sensitive data processing
- Requirements: executive approval, impact assessment, monitoring, regular review

4. Acceptable Use Guidelines

4.1 Approved AI Platforms

- [LIST APPROVED PUBLIC AI PLATFORMS, e.g., Microsoft Copilot, Claude]
- [LIST APPROVED PRIVATE AI IMPLEMENTATIONS]
- Unapproved AI platforms must not be used without explicit permission

4.2 Data Protection Requirements

- No sensitive personal data may be shared with public AI platforms
- No proprietary business information may be shared with public AI platforms
- Use private AI implementations for sensitive work
- All AI outputs must be verified before operational use

4.3 Prohibited Uses

- Generating content that violates code of conduct (discriminatory, offensive)
- Bypassing security controls or authentication systems
- Making critical decisions without human oversight
- Automating processes without appropriate testing and approval

5. Acquisition and Development Process

5.1 New AI System Requests

- Complete AI Use Case Form [LINK TO FORM]
- Document intended benefits and potential risks
- Identify data sources and output usage
- Submit to AI Governance Committee for review

5.2 Vendor Assessment Criteria

- Data security and privacy practices
- Algorithm transparency and explainability
- Service level agreements and support
- Training data diversity and bias mitigation
- Compliance with relevant regulations

5.3 Development Standards

- Documented design and training methodology
- Regular testing for accuracy and bias
- Clear documentation of limitations
- Human oversight mechanisms
- Security by design principles

6. Training and Awareness

6.1 Required Training

- AI Literacy Fundamentals (all staff)
- AI Security Awareness (all staff using AI tools)
- Advanced AI Training (developers, analysts)
- AI Ethics and Governance (leadership, AI Committee)

6.2 Training Frequency

- Initial training upon employment
- Annual refresher courses
- Additional training when new systems are implemented
- Remedial training after policy violations

7. Monitoring and Compliance

7.1 Usage Monitoring

- Technical controls to track AI system usage
- Regular audits of AI interactions
- Cost monitoring and optimisation
- Performance and output quality assessment

7.2 Incident Response

- AI-specific incident reporting procedure
- Investigation process for AI misuse or failures
- Remediation steps for identified issues
- Lessons learned process for continuous improvement

7.3 Policy Violations

- Graduated response based on severity and intent
- Education and additional training for minor violations
- Disciplinary action for serious or repeated violations

8. Regulatory Compliance

8.1 EU AI Act Compliance

- Documentation of high-risk AI systems
- Risk management system maintenance
- Human oversight mechanisms
- Technical documentation and record-keeping

8.2 Data Protection Compliance

- Privacy impact assessments for AI systems
- Data minimisation principles in AI applications
- Transparency regarding AI use affecting data subjects

- Exercise of data subject rights for AI-processed data

8.3 Industry-Specific Requirements

- [ADD INDUSTRY-SPECIFIC COMPLIANCE REQUIREMENTS]

9. Policy Review and Updates

This policy will be reviewed annually or when significant changes occur in AI technology, organisational structure or regulatory requirements.

10. Approval and Implementation

Policy Owner: [POSITION] Approved by: [APPROVER] Effective Date: [DATE] Next Review Date: [DATE]

Appendices

Developed by Lanboss AI

These appendices provide practical templates and supporting materials for implementing your organisation's AI policy. Adapt them to suit your specific needs while ensuring compliance with regulatory requirements and maintaining a risk-balanced approach to AI adoption.

Appendix A: AI Use Case Request Form

AI Use Case Request

Requestor Information:

- Name:
- Department:
- Role:
- Date of Request:

AI System/Tool Information:

- Name of AI System/Tool:
- Provider/Vendor (if applicable):
- Type:
  - ▫ Public AI Platform (e.g., ChatGPT, Claude)
  - ▫ Private AI Implementation
  - ▫ Custom-developed Solution
  - ▫ Vendor Product with AI Features

Use Case Description:

- Purpose of AI system (describe the business need):
- Primary functions and capabilities:
- Anticipated users/departments:
- Expected benefits:
- Success metrics:

Data Considerations:

- Types of data the AI system will access:
  - ▫ Public domain information
  - ▫ Internal non-sensitive data
  - ▫ Confidential business information
  - ▫ Personal data (staff)
  - ▫ Personal data (customers/clients)
  - ▫ Special category personal data (health, biometric, etc.)
- Data storage location:
- Data retention period:

- Data security measures:

Risk Assessment (Preliminary):

- Potential privacy impacts:
- Potential security concerns:
- Potential operational risks:
- Potential ethical considerations:
- Proposed risk mitigation measures:

Implementation Requirements:

- Integration needs:
- Training requirements:
- Timeline for implementation:
- Resources required:
- Budget considerations:

Alternative Solutions:

- Non-AI alternatives considered:
- Reasons for selecting AI approach:

Approvals:

- Department Manager:
- IT Security Review:
- Data Protection Review:
- AI Governance Committee Decision:
  - ▫ Approved
  - ▫ Approved with conditions
  - ▫ Declined
  - ▫ More information needed
- Conditions/Comments:

Appendix B: AI Risk Assessment Template

AI Risk Assessment

System Information:

- System Name:
- Risk Classification: ▫ Low Risk ▫ Medium Risk ▫ High Risk
- Date of Assessment:
- Assessment Conducted By:

1. Data Risk Analysis

Risk Factor	Risk	Details	Mitigation Measures
Sensitive Data Exposure			
Data Accuracy			
Data Bias			
Data Security			
Data Governance			

2. Technical Risk Analysis

Risk Factor	Risk Level	Details	Mitigation Measures
System Reliability			
Output Accuracy			
Security Vulnerabilities			
Integration Risks			
Scalability Issues			

3. Operational Risk Analysis

Risk Factor	Risk Level	Details	Mitigation Measures
Business Continuity			
Cost Management			
Dependency Risks			
Process Disruption			
Staff Adaptation			

4. Compliance Risk Analysis

Risk Factor	Risk Level	Details	Mitigation Measures
EU AI Act Compliance			
Data Protection			
Industry-Specific			
Documentation			
Reporting Obligations			

5. Ethical Risk Analysis

Risk Factor	Risk Level	Details	Mitigation Measures
Bias and Fairness			
Transparency			
Human Oversight			
Accountability			
Social Impact			

6. Risk Rating Methodology

Risk Level Definitions:

- **Low**: Minimal impact if risk materialises; simple controls sufficient
- **Medium**: Moderate impact if risk materialises; additional controls needed
- **High**: Significant impact if risk materialises; comprehensive controls required

Overall Risk Assessment:

- Combined Risk Rating:
- Primary Risk Areas:
- Required Monitoring Frequency:

Approval:

- Risk Assessment Approved By:
- Date:
- Next Review Date:

Appendix C: Approved AI Systems Inventory

AI Systems Inventory

System Name	Provider	Risk Classification	Purpose	Approved Users	Approval Date	Review Date	Status

System Details Template:

System Name:
Provider/Vendor:
Version/Model:
Risk Classification: ▫ Low ▫ Medium ▫ High
System Type: ▫ Public AI ▫ Private AI ▫ Custom ▫ Vendor Product
Purpose:
Primary Functions:
Data Used:
Data Classification:
Integration Points:
Approved Users/Departments:
Approval History:
Key Restrictions:
Monitoring Requirements:
Required Training:
Cost Information:
Contract Renewal Date:
Technical Contact:
Business Owner:
Documentation Location:
Status: ▫ Active ▫ Suspended ▫ Retired ▫ Pending
Approval

Appendix D: AI Incident Response Procedure

AI Incident Response Procedure

1. Purpose

This procedure outlines the steps to identify, report, contain, investigate and remediate incidents involving AI systems. It provides a structured approach for responding to issues such as data breaches, system malfunctions, biased outputs or unauthorised use.

2. Incident Classification

Severity Level	Description	Example	Response Time	Escalation Path
Critical	Significant harm to individuals, major operational disruption, serious regulatory breach	AI system making unauthorised financial decisions, exposing sensitive personal data	Immediate (within 1 hour)	CISO, DPO, CEO
High	Potential harm to individuals, notable operational impact, possible regulatory issue	Biased outputs affecting decisions, system providing dangerous recommendations	Within 4 hours	IT Director, Department Head
Medium	Limited impact, moderate disruption, potential reputation concerns	System outage affecting productivity, minor data exposure	Within 24 hours	AI Governance Committee
Low	Minimal impact, isolated incident, no sensitive data involved	Occasional inaccurate outputs, performance issues	Within 72 hours	System Owner

3. Incident Response Team Roles

- **Incident Coordinator**: Manages overall response, coordinates team activities
- **Technical Investigator**: Analyses technical aspects of the incident
- **Data Protection Officer**: Assesses data protection implications
- **Legal/Compliance Representative**: Evaluates regulatory obligations
- **Business Unit Representative**: Provides context on business impact
- **Communications Lead**: Manages internal/external communications if needed

4. Incident Response Process

4.1 Identification and Reporting

- Any staff member identifying an AI-related incident must report it via:
  - Email: [AI-INCIDENT@ORGANISATION.COM]
  - Phone: [EMERGENCY CONTACT NUMBER]
  - Incident Reporting Form: [LINK TO FORM]
- The report should include:
  - Description of the incident
  - AI system involved
  - Time and date observed
  - Affected data or processes
  - Initial assessment of impact
  - Any immediate actions taken

4.2 Initial Assessment and Classification

- The AI Governance Committee representative evaluates the report
- Determines severity level and activates appropriate team members
- Creates an incident record with unique identifier
- Notifies relevant stakeholders based on severity

4.3 Containment and Mitigation

- Technical team implements immediate containment measures:
  - Isolating the affected system if necessary
  - Suspending problematic features
  - Applying emergency controls
  - Preserving evidence (system logs, outputs)
- Business continuity measures activated if needed

4.4 Investigation

- Technical analysis of:
  - Root cause determination
  - Extent of the incident
  - Data affected
  - System vulnerabilities
  - Control failures
- Documentation of findings in incident record

4.5 Resolution and Recovery

- Develop and implement remediation plan
- Test fixes before full restoration

- Update AI system inventory with incident details
- Restore normal operations with enhanced monitoring

4.6 Notification and Reporting

- Determine notification requirements:
  - Internal stakeholders
  - Affected individuals
  - Regulatory authorities (if applicable)
  - Third parties (vendors, partners)
- Prepare appropriate communications

4.7 Post-Incident Review

- Conduct lessons learned session
- Document:
  - Incident timeline
  - Root causes
  - Effectiveness of response
  - Gaps in controls
  - Recommendations for improvement
- Update risk register and controls

5. Documentation Requirements

All incidents must be documented using the AI Incident Record template, including:

- Incident details and classification
- Response actions and timeline
- Root cause analysis
- Affected data/systems
- Business impact assessment
- Remediation measures
- Regulatory notifications (if applicable)
- Preventative recommendations

6. Continuous Improvement

The AI Governance Committee will:

- Review all incidents quarterly
- Update the incident response procedure annually
- Incorporate lessons learned into AI training
- Enhance monitoring based on incident patterns
- Adjust risk assessments for similar systems

Appendix E: Glossary of AI Terms

AI Terminology Guide

This glossary provides definitions of common AI terms used throughout the policy and implementation documents. It serves as a reference to ensure consistent understanding across the organisation.

Artificial Intelligence (AI): Computer systems that can perform tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making and language translation. In practical business terms, AI refers to software that can analyse data, learn patterns and make predictions or recommendations.

Algorithm: A set of rules or instructions followed by a computer program to solve problems or perform tasks. Algorithms are the foundation of AI systems, determining how they process data and generate outputs.

Bias: Systematic errors in AI outputs that can result in unfair treatment of certain groups or individuals. Bias can be introduced through training data, algorithm design or implementation practices.

Deep Learning: A subset of machine learning that uses neural networks with multiple layers to analyse various factors of data. Deep learning excels at processing unstructured data like images, text and audio.

EU AI Act: European Union regulation establishing legal framework for development, deployment and use of AI systems within the EU. It categorises AI systems by risk level and imposes graduated requirements, with mandatory compliance by August 2026.

Fine-tuning: The process of taking a pre-trained AI model and further training it on a smaller, specific dataset to adapt it for particular tasks or domains. Fine-tuning helps customise models for organisation-specific terminology and workflows.

Foundation Model: Large AI models trained on vast datasets that serve as a base for multiple applications. These models require adaptation (through fine-tuning or RAG) for specific organisational use cases.

Generative AI: AI systems that can create new content such as text, images, audio or video based on patterns learned from training data. Examples include large language models like GPT-4 and Claude.

Human-in-the-Loop (HITL): An approach that combines AI automation with human oversight and intervention. HITL ensures appropriate human review of AI outputs, particularly for high-stakes decisions.

Large Language Model (LLM): AI models trained on vast amounts of text data that can understand and generate human-like text. These models power many generative AI applications and can be used through public platforms or private implementations.

Machine Learning: A subset of AI where systems learn patterns from data without being explicitly programmed. Machine learning models improve through exposure to more data and feedback.

Natural Language Processing (NLP): AI technology that enables computers to understand, interpret and generate human language. NLP powers applications like chatbots, text summarisation and sentiment analysis.

Private AI: AI models deployed within an organisation's own infrastructure, providing greater control over data, security and costs compared to public AI platforms. Private AI may involve fine-tuned models or retrieval-augmented generation with proprietary data.

Public AI Platform: Commercial AI services accessed via APIs or web interfaces, such as ChatGPT or Claude. These platforms offer convenience but may present data security, cost control and customisation challenges.

Retrieval-Augmented Generation (RAG): A technique that enhances AI outputs by retrieving relevant information from a knowledge base before generating a response. RAG improves accuracy and allows AI to access organisation-specific information.

Supervised Learning: A machine learning approach where the model is trained on labelled examples, learning to map inputs to correct outputs. Supervised learning is common in classification and prediction tasks.

Training Data: The dataset used to teach an AI model patterns and relationships. The quality, diversity and representativeness of training data significantly impact model performance and fairness.

Unsupervised Learning: A machine learning approach where the model identifies patterns in unlabelled data without specific guidance. Unsupervised learning is useful for clustering, anomaly detection and dimensionality reduction.

Vector Database: A specialised database that stores data as mathematical vectors, enabling semantic search and similarity matching. Vector databases are often used in retrieval-augmented generation systems to find relevant information.