AI Governance Policy Template

A practical policy framework for governing AI tools, vendors, and data
Customizable for [Company Name] and ready for legal and security review.

Prepared by NTD Consulting

ntdconsulting.com/contact.html

How to use this template

This template is designed for companies adopting AI tools under investor, board, or regulatory scrutiny. Customize bracketed placeholders, remove instructional text, and route the final version through legal, security, and HR before adoption. Pair it with the AI Risk-Assessment Checklist at the end of this document.

Adoption tip

Start with a narrow scope: apply the policy to generative AI tools first, then expand to machine-learning models and embedded AI features as your program matures.

1. Purpose and Scope

1.1 Purpose

This policy establishes the principles, roles, and controls for the responsible use of artificial intelligence (AI) tools and systems at [Company Name]. Its purpose is to balance innovation with risk management, protect company and customer data, and ensure compliance with applicable laws, contracts, and ethical standards.

1.2 Scope

This policy applies to:

- All employees, contractors, interns, and directors ("Personnel").
- All AI tools used on company devices, company accounts, or with company data, including free, trial, and paid services.
- All third parties and vendors that provide AI-powered products or services to [Company Name].

1.3 Definitions

- "AI Tool": Any software or service that uses artificial intelligence, machine learning, or generative models to produce content, recommendations, predictions, code, or decisions.
- "High-Risk AI Use": Use of AI in decisions affecting customers, employees, finance, legal rights, safety, security, or regulated activities.
- "Low-Risk AI Use": Use of AI for routine productivity tasks where output is non-binding and reviewed before any external use.
- "Public AI Tool": An AI service operated by a third party where inputs may be used to train models or retained by the vendor.

2. Governance and Roles

2.1 AI Governance Committee

[Company Name] maintains an AI Governance Committee responsible for approving high-risk AI use cases, reviewing incidents, and updating this policy. Members include representatives from Security, Legal, Engineering, Product, and HR.

2.2 Individual Accountability

Every user of an AI tool is responsible for:

- Using only approved AI tools for approved purposes.
- Verifying AI-generated output before relying on it.
- Reporting suspected misuse, data exposure, or harmful output.

2.3 Vendor Accountability

Vendors providing AI tools must complete a security and risk assessment before procurement and must contractually agree to data-handling, confidentiality, audit, and incident-response requirements.

3. Acceptable Use

3.1 Permitted Uses

Personnel may use approved AI tools for:

- Drafting internal communications, documentation, and code.
- Ideation, brainstorming, and research assistance.
- Low-risk automation of repetitive tasks where output is reviewed.
- Decision support, provided the output is validated by a qualified human.

3.2 Required Precautions

Before using any AI tool, Personnel must:

- Confirm the tool is on the [Company Name] approved tool list or obtain approval.
- Not enter confidential, personal, regulated, or proprietary information into public AI tools.
- Label or disclose AI-generated content when required by policy, contract, or law.
- Maintain records of high-risk AI use as required by the AI Governance Committee.

4. Prohibited Use

The following uses are prohibited unless explicitly authorized in writing by the AI Governance Committee:
- Entering customer PII, PHI, payment card data, credentials, or source code into public AI tools.
- Using AI to generate or alter legal, financial, medical, or safety-critical documents without human review.
- Making automated employment, credit, insurance, or disciplinary decisions without human oversight.
- Creating deepfakes, impersonations, or misleading content.
- Bypassing security controls, monitoring, or compliance obligations using AI.
- Using AI tools from vendors that have not completed the vendor security assessment.

5. Data Classification and Protection

5.1 Data Handling

All data entered into AI tools must be classified according to the [Company Name] Data Classification Policy. Confidential, restricted, and regulated data may only be used in enterprise AI tools that have been contractually approved for that data type.

5.2 Retention and Deletion

[Company Name] must understand and document where AI vendor data is stored, how long it is retained, and how it can be deleted. Contract terms must be reviewed by Legal before any confidential data is processed.

5.3 Model Training

Public AI tools must not be used in a manner that allows [Company Name] data to train third-party models, unless explicitly approved by the AI Governance Committee and covered by contract.

6. Human Oversight

6.1 Review Requirements

All high-risk AI output must be reviewed and approved by a qualified person before it is used to make decisions or communicated externally. Low-risk output should be spot-checked for accuracy, bias, and appropriateness.

6.2 Escalation

Any AI output that appears incorrect, biased, harmful, or that exposes the company to legal or reputational risk must be escalated to the AI Governance Committee and the responsible manager.

7. Vendor Management

7.1 Approved Vendor List

The AI Governance Committee maintains an approved vendor list for AI tools. Tools not on the list require a risk assessment and written approval before use.

7.2 Minimum Contract Terms

AI vendor contracts must address:

- Data ownership, confidentiality, and permitted use.
- Prohibition on using company data for model training without consent.
- Subprocessor disclosure and notification.
- Security controls, audit rights, and penetration testing.
- Incident notification and breach liability.
- Data deletion and return obligations at contract termination.

8. Incident Reporting

Suspected or confirmed AI-related incidents -- including data leakage, unauthorized AI use, biased output, security compromise, or misuse -- must be reported to [security@company.com] and [legal@company.com] within 24 hours of discovery. The AI Governance Committee will assess the incident, contain impact, and determine required notifications.

9. Training and Enforcement

9.1 Training

All Personnel must complete AI governance training at onboarding and annually thereafter. Role-specific training is required for Engineering, Product, Legal, HR, Finance, and customer-facing teams.

9.2 Exceptions

Exceptions to this policy may be granted by the AI Governance Committee on a case-by-case basis, documented in writing, and reviewed at least annually.

9.3 Enforcement

Violation of this policy may result in disciplinary action, up to and including termination, and may trigger contractual, legal, or regulatory consequences.

10. Policy Maintenance

This policy is owned by [Security/Legal/AI Governance Committee]. It will be reviewed at least annually and updated when there are material changes to AI use, vendor landscape, legal requirements, or business risk.

AI Risk-Assessment Checklist

Complete this checklist before onboarding a new AI tool or approving a new high-risk use case.

[ ] Is the AI tool on the approved vendor list?

[ ] What business problem does the tool solve?

[ ] Will the tool process confidential, personal, regulated, or proprietary data?

[ ] Will the output affect customers, employees, finance, legal rights, safety, or security?

[ ] Is a qualified human required to review the output before action?

[ ] Does the vendor contract prohibit using company data for model training without consent?

[ ] Does the vendor disclose subprocessors and provide breach notification?

[ ] Can company data be deleted or returned upon contract termination?

[ ] Has the vendor completed a security assessment?

[ ] Have Legal and Security reviewed and approved the use case?

[ ] Has the AI Governance Committee granted written approval?

Approval record

Use case / tool: _____

Approved by: _____ Date: _____

Review date: _____