XONIK

TEMPLATE

AI Governance Policy Starter Template

A starting point for an organization's own AI governance policy: purpose, roles, inventory, approval, data, oversight, change, incidents and review.

Version	1.0
Date	20 October 2026
Published by	XONIK
For	A compliance lead or CIO writing a first AI governance policy.
Use with	The AI Governance Assessment on the XONIK website and the AI Risk Register.

How to use this template

Read the model wording in each section, then write your own version in the box beneath it, replacing every [bracketed phrase]. Type into the boxes on screen, or print the pages and write by hand. Leave out any section that does not apply. Keep the policy short enough that the people who must follow it will actually read it. A short rule that people follow beats a long policy in a folder.

> **Guidance**
> Write for the people who use AI. Where the policy says a person must do something, name the role. Where it says an approval is needed, say who gives it. The guidance boxes are notes for you and are not part of the policy.

Policy details

Item	Entry
Policy name Organization name and the words AI Governance Policy	
Policy owner Role and name	
Approved by Role, body or committee	
Effective date The date the policy starts to apply	
Next review A date, or the event that triggers a review	
Applies to For example, all staff, contractors and suppliers acting for the organization	

1. Purpose and scope

This policy sets out how [Organization name] decides where artificial intelligence may be used, who is accountable for each use, and how its use is checked. It exists so that every AI system in use has an owner, has been approved for the purpose it serves, and can be reviewed, changed or switched off by a named person.

It applies to AI systems that [Organization name] builds, buys or uses, including AI features built into products bought for other purposes. It does not apply to [list anything out of scope, for example research carried out on public data with no effect on any person].

> **Guidance**
> Word the scope so that it covers AI features inside bought software. Those often turn up only when you make the inventory in section 4.

Your wording for section 1

2. Principles

[Organization name] applies these principles to every use of AI:

- Accountability. Every AI system has a named owner who answers for it.
- Human oversight. A person can review, correct or reverse an outcome that affects someone.
- Fitness for purpose. A system is used only for the purpose it was approved for, and tested for it.
- Transparency. People affected by a use of AI are told when it is used, in a way they can understand, where [rule or commitment] requires or where it would be reasonable to expect it.
- Care with data. Data is used only where there is a basis for it and permission to use it for this purpose.
- Proportion. The care taken is greater where an error could harm a person.

> **Guidance**
> Change the wording to fit your values. Keep each principle testable: a reader should be able to tell whether a given use of AI meets it.

Your wording for section 2

3. Roles and accountability

Role	What the role does under this policy	Held by (name or role)
Executive sponsor	Funds AI work beyond the pilot, takes part in the decision to go live, and receives reports on live systems.	
System owner	Answers for one AI system after launch: decides when it changes, notices when it is wrong, can pause or stop it.	
Data owner	Confirms that the data a system uses may be used for that purpose, and that it is accurate enough.	
Risk and compliance	Reviews the design of a live system against the rules that apply, and sets conditions.	
Security	Reviews access, logging and the handling of secrets.	
Users	Use a system only for its approved purpose, report errors, and do not rely on output the system is not approved for.	

Guidance
Name people or roles, not committees. When something goes wrong, nobody answers for what a committee owns. Each system's owner is named in the inventory below.

4. Inventory of AI systems

[Role] keeps a list of every AI system in use, including AI features built into products we buy. Each entry names the system, its purpose, its owner, the data it uses, the decisions it influences and the date it was last reviewed. A system that is not on the list is not approved for use.

System	Purpose	Owner	Data used	Decisions it influences	Last reviewed

Your wording for section 4 (who keeps the list)

5. Approving a new use of AI

Before an AI system is used for the first time, or for a new purpose, its owner brings a short proposal to [approving role or body]. The proposal states:

1. The purpose, and the change in how work is done.
2. The data the system will use, and the basis for using it.
3. Who will use it, and who will be affected by its output.
4. How it was tested, on what, and what the known failures are.
5. What happens when it is down or wrong, and who can be called.
6. The owner, who has agreed, and who can change or stop the system.
7. The approvals still needed, and the conditions set.

[Approving role or body] may approve, approve with conditions, or decline. The decision, the conditions and the date are recorded in the inventory.

> **Guidance**
> Proportion matters. Allow a light route for low-risk uses, such as drafting text that a person always reviews, and a fuller route where an error could harm a person or breach a rule. Say what decides which route applies.

Your wording for section 5

6. Data

AI systems may use only data that [Organization name] has a basis to use for that purpose. Personal data, confidential client information and [other categories] may not be entered into a system that has not been approved for them. Data sent to an outside supplier is governed by the contract with that supplier, which must say [what the contract must cover, for example whether the data is used to train models, where it is kept and how it is deleted].

> **Guidance**
> Don't leave this to individual judgment. Say which tools staff may use with which kinds of data.

Your wording for section 6

7. Human oversight

Where an AI system affects a person, a human can review the outcome and reverse it. The route for asking for a review is [route], and a review is completed within [period]. Where a person reviews output before it is used, the owner records how that review works and checks that it actually happens.

Your wording for section 7

8. Testing, monitoring and quality

Before a system goes live it is tested on real examples that were not used to build it. After launch, the owner samples output against the right answer on a schedule of [frequency], records what is found and acts on it. Anything reported as wrong by a user or a customer is recorded and its cause is found.

Your wording for section 8

9. Change

A change to a model, a prompt, a data source or a supplier behind a live system is a change to the system. The owner reviews it against the approval conditions before it reaches users, and records it. [Role] is told when a supplier announces a change to a model or a service on which a live system depends.

Your wording for section 9

10. Incidents and errors

A serious error, harm to a person, a breach of a rule or a loss of data caused by an AI system is reported to [role] immediately and in any case within [period]. [Role] decides who else must be told, including [regulators, customers or others, as required], and leads the response. After an incident the system is reviewed, and the review is recorded. The route is rehearsed [frequency].

Your wording for section 10

11. Suppliers

Before buying an AI system or a service that includes one, [role] checks the supplier's answers on data handling, security, transparency, support and continuity, and records them. The contract states [terms that matter to you]. The cost and effort of leaving are considered before signing.

Your wording for section 11

12. Training

Everyone who uses AI at work is told what this policy asks of them, [when, for example on joining and when the policy changes]. System owners and approvers receive further guidance on [topics].

Your wording for section 12

13. Exceptions, enforcement and review

An exception to this policy needs the written agreement of [role], states its reason and its end date, and is recorded. A breach of this policy is dealt with under [disciplinary or contract process]. This policy is reviewed at least [frequency], and when [events, for example a change in the law, a serious incident or a major new use of AI].

Your wording for section 13

Version history

Version	Date	Change	Approved by

Limits of this template

XONIK wrote this template as a working aid. It is general guidance, not legal advice, and it certifies nothing. Adapt it to your organization, and have someone qualified to advise on the rules that apply to you review it before you adopt it.