

SAMPLE

AI Governance Policy Bundle

The opening of AI-Gov-Acceptable-Use-Policy.docx, one of 12 files in the kit. <https://solasai.net/products/ai-governance-bundle/>

AI Acceptable Use Policy

Rules for employee and organizational use of AI tools

Product: AI Governance Policy Bundle, version 3.0, 19 October 2026. **Classification:** Purchaser use only, customize before use. Solas AI, solasai.net.

Field	Value
Owner	[AI Governance Lead / CISO / CTO]
Approved by	[CEO / Executive Sponsor]
Effective date	[Date]
Review cycle	Annual, and on any material change in the tools used or the law
Related policies	AI Data Governance Policy, AI Vendor Selection Policy, AI Incident Response Supplement, AI Transparency Policy

1. Purpose

This policy sets the rules for using artificial intelligence tools at [Organization Name]. It exists so that staff can use AI for the work it is good at without exposing customer data, confidential information, or the organization to legal and reputational harm. It replaces informal practice with three things: a short list of approved tools, clear rules on what data may go into them, and a fast path for requesting new ones.

2. Scope

The policy applies to every employee, contractor, intern, and authorized third party who performs work for [Organization Name], on any device, whether the tool was supplied by the organization or found independently. It covers generative AI (text, code, image, audio, video), AI assistants embedded in approved software (for example AI features inside the office suite, the CRM, or the IDE), AI agents and automations that act on systems or data, and browser extensions or desktop applications that send content to an AI service. It does not cover AI features in customer-facing products built by [Organization Name], which the AI Model Management Policy governs.

3. Definitions

- **AI tool.** Any software or service that uses a machine learning model to generate, transform, classify, or decide on content or actions, including features inside other software.
- **Prompt.** Anything submitted to an AI tool: typed text, pasted documents, uploaded files, screenshots, voice, or data sent through an integration.
- **Output.** Anything an AI tool returns: text, code, images, decisions, or actions taken on another system.
- **Enterprise agreement.** A contract under which the vendor commits in writing not to train on the organization's data, to delete it on a schedule, and to provide security terms acceptable to [IT/Security]. A paid individual subscription is not an enterprise agreement.
- **AI Tool Registry.** The maintained list of tools with their tier, owner, permitted data classes, and contract reference, kept in [location] and shipped with this bundle as the AI Tool Inventory workbook.
- **Data classes.** Public, Internal, Confidential, and Restricted, as defined in the AI Data Governance Policy. Restricted includes customer personal data, health information, payment data, credentials, and anything under a non-disclosure obligation.

4. Roles and Responsibilities

Role	Responsibility
Executive Sponsor [CEO / COO]	Approves this policy, resolves escalations, owns the risk appetite for AI use
AI Governance Lead [CISO / CTO / designated manager]	Owns the policy, the AI Tool Registry, and the tool request process; reports quarterly
[IT/Security]	Evaluates tools, configures enterprise controls, monitors for unapproved tools, revokes access
[Legal / Privacy]	Reviews vendor terms, data protection obligations, and disclosure requirements
People managers	Ensure their teams know the registry, approve requests at the first stage, handle first-line violations
Every user	Checks the registry before use, follows the data rules in Section 6, verifies output, reports problems

The sample ends here. The full document runs about 1,523 words; the kit holds 12 files. Version 2.2, 19 October 2026. Buy it at <https://solasai.net/products/ai-governance-bundle/>, 14-day refund for any

reason.