AI Acceptable Use Policy

Governing the safe and responsible use of AI tools

This policy template defines how your organisation's employees and contractors should use artificial intelligence tools, including generative AI services, AI-powered development tools, and internal AI systems. It addresses data protection, prohibited uses, approval workflows, and accountability requirements.

Prepared by: Nuvencia — Information Security Advisory

Author: Jaouhar Mosbahi, CISSP, CCSP, ISO 27001 LI/LA

Version: 1.0 — February 2026

Classification: Template — Customise for your organisation

This template is provided by Nuvencia for guidance purposes. Organisations should customise it to reflect their specific context, risk appetite, and regulatory requirements.

© 2026 Nuvencia. All rights reserved.

1. Purpose and Scope

This policy governs the use of artificial intelligence (AI) tools and services by all employees, contractors, and third parties acting on behalf of [Organisation Name]. It applies to all AI tools including but not limited to: generative AI chatbots (e.g., ChatGPT, Claude, Gemini), AI-powered code assistants (e.g., GitHub Copilot), AI image and content generators, and internally developed AI systems.

2. AI Tool Classification

AI tools used within the organisation are classified into three tiers:

Tier	Description	Approval
Tier 1 — Approved	Pre-approved tools vetted by IT/Security. May be used for approved purposes without additional approval.	Pre-approved
Tier 2 — Conditional	Tools that may be used with restrictions (e.g., no client data, no PII). Requires awareness training.	Line manager
Tier 3 — Prohibited	Tools that do not meet security or privacy requirements. Must not be used for any business purpose.	Not permitted

[Guidance: Maintain and publish a registry of AI tools by tier. Review quarterly.]

3. Prohibited Uses

The following uses of AI tools are strictly prohibited:

- Inputting client data, personal data (PII), or confidential business information into external AI tools
- Using AI-generated content in client deliverables without human review and validation
- Using AI tools to make automated decisions affecting employees or customers without human oversight
- Submitting proprietary source code to external AI services without IT Security approval
- Using AI to generate misleading, deceptive, or fraudulent content
- Bypassing security controls or using AI for unauthorised system access
- Using AI outputs without verifying accuracy and factual correctness

4. Data Protection Requirements

When using approved AI tools, users must ensure no sensitive data is shared with external services. Data classification determines what can be processed by AI tools:

Classification	AI Tool Usage
Public	May be used with any approved AI tool
Internal	May be used with Tier 1 tools only, with enterprise data protection agreements in place
Confidential	Restricted to internally hosted AI tools with approved data processing agreements
Restricted / PII	Must not be processed by any external AI tool. Internal tools only with explicit CISO approval.

© 2026 Nuvencia. All rights reserved.

5. Human Oversight and Accountability

All AI-generated outputs must be reviewed by a qualified human before being used in any business context. The individual who submits or publishes AI-assisted content is accountable for its accuracy, quality, and compliance. AI tools are assistants, not decision-makers.

6. Intellectual Property

Users must be aware that content generated by AI tools may not be protected by copyright. AI-generated code must be reviewed for potential licence compliance issues. The organisation retains ownership of all work products created with AI assistance, subject to the terms of service of the AI tools used.

7. Reporting and Compliance

Any misuse of AI tools, suspected data leakage through AI services, or AI-related security incidents must be reported immediately to the IT Security team. Violations of this policy may result in disciplinary action up to and including termination of employment or contract.

8. Document Control

[Guidance: Add version history, approval signatures, and next review date here.]

© 2026 Nuvencia. All rights reserved.