

AI Usage Policy Template

Philippine business starter template

Organization	[Company / Organization Name]
Policy owner	[Department / Responsible Person]
Effective / review date	[Date] / [Review Date]

How to use this template. Replace bracketed placeholders, identify approved AI tools, define restricted information, align the policy with your privacy, security, HR and contractual requirements, and obtain appropriate legal/compliance review where needed.

1. Purpose

This policy governs the use of generative AI and other artificial intelligence tools for company work. Employees may use AI only in ways that protect company information, personal data, intellectual property, clients and the security of company systems.

2. Scope

This policy applies to employees, contractors and other authorized users who access AI tools for company work, whether through company-provided or personally accessed services.

3. Approved AI Tools

Employees may use only AI tools approved by the company for work involving company information. Personal or unapproved accounts must not be used for restricted information.

Approved tools: [List tools / enterprise accounts / approved use cases].

4. Information That Must Not Be Uploaded

- Passwords, API keys, authentication codes or other credentials.
- Confidential business information unless specifically approved.
- Personal or sensitive personal information unless processing is approved and legally permitted.
- Client information protected by contract or professional duty.
- Source code, trade secrets or unpublished intellectual property unless authorized.
- Security vulnerabilities or internal system details unless the use case is specifically approved.

5. Human Review

AI output must be reviewed by a qualified employee before it is used in decisions, customer communications, legal documents, financial work, public content or other material outputs.

6. Accuracy and Hallucinations

Employees must verify factual claims, citations, calculations and legal or technical conclusions generated by AI. AI output must not be treated as automatically accurate.

7. Copyright and Intellectual Property

Employees must avoid requesting or using AI output that knowingly infringes third-party rights. Company ownership and approval rules continue to apply to work produced with AI assistance.

8. Personal Data

Any use of personal data with AI must follow the Data Privacy Act of 2012, applicable National Privacy Commission issuances, company privacy policies, contracts and approved processing purposes.

Do not input personal or sensitive personal information unless the processing is authorized, necessary, proportionate and permitted by company policy.

9. Security

Employees must not use AI to bypass security controls, expose credentials, generate malicious code for unauthorized purposes or disclose vulnerabilities without authorization.

10. Disclosure and Recordkeeping

Teams may require disclosure of material AI assistance for specified work products and should retain records where needed for audit, quality control, legal obligations or compliance.

11. High-Risk and Restricted Uses

Uses involving employment decisions, health, financial eligibility, legal determinations, biometric data, surveillance, customer profiling or other high-impact decisions require prior approval from [Responsible Person / Committee].

12. Violations

Misuse of AI tools may result in removal of access, corrective action or disciplinary measures consistent with company policy and applicable law.

13. Exceptions and Approval

Requests for exceptions should be submitted to [Approver / Department] with the purpose, data involved, tool, expected output, controls and retention requirements.

Implementation Checklist

- Name the approved AI tools and enterprise accounts.
- Define confidential-data classifications and prohibited inputs.
- Identify who approves exceptions and high-risk use cases.
- Add industry-specific privacy, security or regulatory requirements.
- Define record-retention and deletion rules.
- Define when AI use must be disclosed.
- Align the policy with employment, disciplinary, privacy and information-security policies.
- Train personnel and document policy acknowledgement.

Important Note

This is a general starter template, not legal advice. It should be adapted to the organization's actual systems, contracts, industry obligations and risk profile.