|  |
| --- |
| **AI Acceptable Use Policy**  Template — Customize for Your Organization |

|  |  |
| --- | --- |
| **Organization:** | [Organization Legal Name] |
| **Version / Date:** | 1.0 | Effective: [Date] |
| **Policy Owner:** | [Name, Title] |
| **Review Cycle:** | Annually, or upon material regulatory change |

**1. Purpose**

This policy establishes guidelines for the responsible, secure, and compliant use of artificial intelligence (AI) tools by all personnel of [Organization Name]. It ensures AI adoption proceeds in alignment with our legal obligations, client commitments, risk appetite, and organizational values.

**2. Scope**

This policy applies to:

* All employees, contractors, vendors, and authorized third parties
* All AI tools — chatbots, writing assistants, code generators, image tools, and AI features embedded in existing software
* Both company-owned and personal devices used for any work-related purpose

**3. Key Definitions**

|  |  |
| --- | --- |
| **Term** | **Meaning** |
| **AI Tool** | Any software using machine learning, generative AI, or large language models (e.g., chatbots, writing assistants, code generators, image tools). |
| **Approved AI Tool** | A tool reviewed and authorized by [Policy Owner / IT / Compliance] for specific data tiers and use cases. |
| **Sensitive Data** | Any data classified Tier 2–4 per the organization's Data Tier Map. Includes client, financial, personnel, and regulated data. |
| **PHI / PII** | Protected Health Information (HIPAA) or Personally Identifiable Information. Requires highest level of protection. |

**4. Acceptable Use**

**Employees MAY use approved AI tools for the following:**

* Drafting and editing internal documents, policies, and communications
* Summarizing meeting notes that contain no client names or identifying information
* Generating ideas, outlines, or first drafts using publicly available or anonymized information
* Writing, reviewing, or explaining code that does not involve regulated or confidential data
* Responding to general inquiries using publicly available information
* Creating training materials, presentations, or educational content

**5. Prohibited Use**

**Employees MAY NOT:**

* Enter PHI, PII, or regulated data into any AI tool without a specific approved workflow and signed BAA or DPA
* Share confidential client information — names, account details, financials, contracts — with any general-purpose AI tool
* Use unapproved AI tools for any work-related purpose, including on personal devices
* Present AI-generated content as original human work without disclosure where required (filings, legal docs, client deliverables)
* Use AI to make final autonomous decisions on employment, lending, healthcare, or other high-stakes matters without human review

**6. Data Handling Requirements**

Before entering any data into an AI tool, you must:

* Classify the data using the Data Tier Map (see attached worksheet)
* Confirm the tool is on the Approved AI Tools List for that data tier
* Remove or anonymize identifiers if using a general-purpose AI tool with Tier 2 data
* Never upload documents containing Tier 3 or Tier 4 data to a general AI tool

**7. Approved AI Tools**

The current approved tools list is maintained by [Policy Owner] at [link/location]. All new tools must be submitted through the AI Vendor Assessment process before use. See the AI Vendor Assessment Checklist.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool Name** | **Approved Use Cases** | **Max Data Tier** | **Notes / Restrictions** |
| [Tool Name] | [Use case description] | Tier 1–2 | [Restrictions] |
| [Tool Name] | [Use case description] | Tier 1–2 | [Restrictions] |
| [Tool Name] | [Use case description] | Tier 1–2 | [Restrictions] |

**8. Incident Reporting**

If you believe sensitive data has been accidentally shared with an AI tool or you observe a violation:

* Stop using the tool immediately
* Document what data was shared, with which tool, and when
* Report to [Policy Owner / Security Team] within [24 hours]
* Do not attempt to delete logs or conceal the incident

**9. Consequences of Non-Compliance**

Violations may result in disciplinary action up to and including termination, and potential legal liability. Incidents involving regulated data may trigger mandatory breach notification obligations under applicable law.

**10. Acknowledgment**

By using AI tools for any work purpose, I confirm I have read, understood, and agree to comply with this policy.

|  |  |
| --- | --- |
| **Employee Name:** | **Signature:** |
| **Date:** | **Department:** |

|  |
| --- |
| **✏ CUSTOMIZATION TIPS**  1. Fill in all fields in brackets [ ] with your organization's specifics.  2. Have legal or compliance review before distributing — especially the prohibited use and incident response sections.  3. Distribute to all staff annually and retain signed acknowledgments for audit purposes. |