

[Your Company Name] Standard AI Acceptable Use & Governance Policy

[Your Company Name] Standard AI Acceptable Use & Governance Policy

Date: [Insert Date] | Intended Audience: [Your Company Name]

This agreement-style policy is designed for immediate adoption by [Your Company Name]. Replace bracketed fields and attach to your Employee Handbook and Vendor Handbook.

[Member Company] Information

[Member Company Legal Name]: _____

[Member Address]: _____

[Primary Contact/Title]: _____

[Effective Date]: _____ [Version]: v1.0

1) Purpose & Scope

This policy establishes enforceable rules for responsible, secure, and compliant use of Artificial Intelligence (“AI”) by employees, contractors, and vendors of [Member Company]. It applies to all AI systems, tools, platforms, models, and services—whether developed internally, licensed, or integrated from third parties—that are used, deployed, or accessed by [Member Company] Information Resource. The policy ensures that AI is used ethically, lawfully, securely, and in alignment with organizational values and compliance obligations.¹

2) Definitions (operational)

- **AI System:** Software or technologies that perform tasks normally requiring human intelligence, including but not limited to natural language processing, machine learning, computer vision, and automation. This includes systems that generate outputs (content/recommendations/actions) from prompts or data (e.g., Microsoft 365 Copilot, Azure OpenAI, Amazon Bedrock).
- **Generative AI:** AI that can create content such as text, images, audio, or code (e.g., ChatGPT, DALL·E).
- **Client Data:** Information owned by or processed for a client under an MSA/SOW, including personal information and confidential business data.
- **Personal Information / Sensitive PI:** As defined by CPRA/CCPA and applicable privacy laws.
- **Approved AI Platform:** Company-vetted tools configured by Security/IT (enterprise tenants only).
- **Consequential Decision:** An automated decision with legal or similarly significant effects on a person or business.
- **Authorized Use:** Activities that are approved by management and aligned with this policy.

¹ [ISMS POL 13 AI Acceptable Use Policy.docx](#)

3) Governing Standards & Laws (reference mapping)

- Privacy: CPRA/CCPA (service-provider/contractor obligations), GLBA (financial), HIPAA (health), state data breach laws.
- Security & Assurance: SOC 2 / ISO 27001; NIST CSF; MSPAlliance MSP/Verify or Cyber Verify (as applicable).
- AI Governance: NIST AI RMF 1.0 & NIST Generative AI Profile; Microsoft Responsible AI Standard (v2) as external benchmark.
- Sector Overlays (if applicable): CJIS (public safety), PCI DSS (payment), other customer-mandated frameworks.
- Additional References: NIST AI Risk Management Framework (AI RMF), ISO/IEC 42001:2023 Artificial Intelligence Management Systems, OECD AI Principles, Company Code of Ethics and Data Security Policy.²

4) Principles

- Client-first; least-privilege; security-by-design and privacy-by-default.
- Human-in-the-loop for consequential actions; documented approvals for exceptions.
- Transparency and auditability (log access, prompts where permitted, and output provenance for material client work).
- No model training on client data by default when using enterprise AI services.
- Our approach to AI is guided by six core principles: fairness, reliability and safety, privacy and security, inclusiveness, transparency, and accountability.³

5) Approved vs Prohibited AI Use

5.1 Approved (with training + logging):

- Draft internal docs, ticket summaries, and code comments using approved enterprise AI (no client secrets).
- Summarize public information or client-designated materials explicitly permitted in the SOW/DPA.
- Automate repetitive tasks (knowledge retrieval, report skeletons) with human review before external release.
- Use responsibly and ethically; avoid using AI for deception, manipulation, discrimination, harassment, or generating false or misleading content.
- Respect intellectual property—do not use AI to create, replicate, or manipulate copyrighted content without proper authorization. AI-generated content must be reviewed for potential IP risks before external use.⁴
- Ensure human oversight—AI-generated decisions that affect employment, customer experience, or business operations must be reviewed by a human prior to execution. AI should augment, not replace, critical human judgment in sensitive areas.

² [ISMS POL 13 AI Acceptable Use Policy.docx](#)

³ [ISMS POL 13 AI Acceptable Use Policy.docx](#)

⁴ [ISMS POL 13 AI Acceptable Use Policy.docx](#)

- Ensure data privacy and security—review access and data classification prior to enabling AI resources; do not input confidential, proprietary, or personally identifiable information (PII) into public AI tools unless approved and secured. Comply with applicable data protection regulations.⁵
- When using Microsoft 365 Copilot, sign in with your work account and apply sensitivity labels as appropriate to protect company data.⁶
- Monitor and audit AI systems for biased outputs or discriminatory outcomes. Always double-check AI-generated results for accuracy and be aware of potential biases. Report any unintended consequences or harms to [Member Company].⁷
- Maintain transparency and documentation—ensure transparency in customer communications, public-facing content, or decision-making; document purpose, data sources, training sets, and outputs of internally developed AI models; clearly label AI-generated content when required.⁸
- Monitor usage of AI and limit use to authorized tools and use cases. Only use approved AI vendors, platforms, and models vetted by [Member Company]. Unauthorized use of AI tools (e.g., unsanctioned plugins or APIs) is prohibited.⁹

5.2 Prohibited:

- Pasting client PI/PHI/PCI/CJI, secrets/keys/credentials/firmware, device logs with identifiers, or unreleased code into non-approved AI tools.
- Using personal/consumer AI accounts for any company work.
- Relying on AI outputs as final legal, financial, HR, or operational decisions without authorized human sign-off.
- Deepfakes or impersonation; surveillance without a legal basis or consent.
- Automating high-risk decisions without appropriate governance.
- Bypassing security controls or cybersecurity defenses.
- Generating harmful or offensive content, including hate speech, harassment, and discrimination.
- Content promoting child sexual exploitation or abuse, grooming, non-consensual intimate content, sexual solicitation, human trafficking, sexually explicit content, content related to suicide and self-injury, violent content and conduct (including graphic violence, terrorism, and violent extremism), deception, disinformation, inauthentic activity, active malware or exploit, and scenarios likely to generate undesired content due to limitations.¹⁰

6) Data Handling & Prompt Hygiene

- Default to synthetic or redacted data in prompts; minimize data exposure (minimum necessary).
- Use approved repositories for prompts/outputs related to material client work; apply retention tags.
- Honor client data residency; avoid cross-region transfers without explicit approval.
- Do not input confidential, proprietary, or personally identifiable information (PII) into public AI tools unless approved and secured.

⁵ [ISMS POL 13 AI Acceptable Use Policy.docx](#)

⁶ [ISMS POL 13 AI Acceptable Use Policy.docx](#)

⁷ [ISMS POL 13 AI Acceptable Use Policy.docx](#)

⁸ [ISMS POL 13 AI Acceptable Use Policy.docx](#)

⁹ [ISMS POL 13 AI Acceptable Use Policy.docx](#)

¹⁰ [ISMS POL 13 AI Acceptable Use Policy.docx](#)

7) Governance and Review

- AI use must be registered and approved by the [Member Company] IT Security Committee.
- AI applications must undergo regular risk assessments, bias evaluations, and compliance audits.
- Changes to AI use cases, tools, or data sets must be documented and re-approved.

8) Reporting Violations

- Violations of this policy should be reported to [Member Company] IT Security Committee or Ethics Hotline.
- Violations may result in disciplinary action, including termination of access or employment, and potential legal action.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	mm/dd/yyyy	mm/dd/yyyy		Initial Creation

© 2025 Technology Assurance Group (TAG) / Jaida. This template is provided “as-is” and should be reviewed by each Member’s counsel before adoption.