AI Acceptable Use Policy

Enterprise Governance & Compliance Program

Organization Name: [Your Organization Name]

Document Owner: AI Governance Program Office

Version: 1.0

Effective Date: [Insert Date]

Review Cycle: Annual

Document ID: AUP-001

Confidentiality: Internal Use Only

Table of Contents

[Purpose 3](#_Toc194150491)

[Scope 3](#_Toc194150492)

[1. Permissible Uses of AI 3](#_Toc194150493)

[2. Prohibited Uses of AI 3](#_Toc194150494)

[3. Data Protection and Privacy 4](#_Toc194150495)

[4. Roles and Responsibilities (RACI Model) 4](#_Toc194150496)

[5. Human Oversight and Accountability 4](#_Toc194150497)

[6. Security and Risk Mitigation 5](#_Toc194150498)

[7. Training and Awareness 5](#_Toc194150499)

[8. Enforcement and Sanctions 5](#_Toc194150500)

[9. Policy Review and Maintenance 5](#_Toc194150501)

[10. Incident Reporting and Response 6](#_Toc194150502)

[11. Shadow AI and Unapproved Tools 6](#_Toc194150503)

[Definitions 8](#_Toc194150504)

[References 9](#_Toc194150505)

[Appendix A – Executive Briefing Summary 10](#_Toc194150506)

[Appendix B – User Attestation Form 10](#_Toc194150507)

[Appendix C – Training Checklist 10](#_Toc194150508)

[Document Control 10](#_Toc194150509)

# Purpose

This Acceptable Use Policy (AUP) outlines the permissible and prohibited uses of Artificial Intelligence (AI) technologies within the organization. It serves to promote responsible, ethical, secure, and legally compliant use of AI tools and systems while minimizing risks to data privacy, cybersecurity, intellectual property, and organizational integrity.

# Scope

This policy applies to all employees, contractors, vendors, consultants, interns, and third-party users who access or interact with AI systems owned, deployed, developed, or sanctioned by the organization. It encompasses both internally developed AI solutions and third-party AI applications, including generative AI models, machine learning systems, SaaS AI services, open-source libraries, and APIs.

# 1. Permissible Uses of AI

**Authorized users may employ AI technologies for the following purposes, provided all uses adhere to this policy, applicable laws, and ethical standards:**

- Enhancing productivity through AI-assisted tools for drafting, summarizing, coding, data analysis, or visualization.

- Supporting internal decision-making through supervised models with human oversight.

- Automating routine workflows where risk assessments confirm acceptable impacts.

- Conducting R&D or prototyping with pre-approved AI datasets and tools.

- Leveraging vetted generative AI tools to create content that is reviewed before public or customer-facing use.

- Supporting inclusive, fair, and equitable services by identifying and reducing bias using explainable AI (XAI) techniques.

# 2. Prohibited Uses of AI

**The following activities are strictly prohibited:**

- Inputting confidential, proprietary, regulated, or personally identifiable information (PII) into unapproved or public AI systems.

- Using AI to generate harmful, misleading, offensive, or manipulative content, including deepfakes.

- Employing AI systems in discriminatory practices that adversely affect individuals based on protected attributes (e.g., race, gender, disability).

- Relying on AI for fully autonomous decisions that impact employment, legal status, finance, health, or access to essential services.

- Circumventing established approval workflows, security controls, or governance processes using AI automation.

- Training or fine-tuning models using unauthorized data, or violating copyright, data protection, or export control regulations.

# 3. Data Protection and Privacy

All use of AI must be conducted in compliance with organizational data governance policies and regulatory frameworks, including but not limited to GDPR, HIPAA, CCPA, and ISO/IEC 27001:

- Apply data minimization, pseudonymization, and anonymization where applicable.

- Do not submit sensitive data to external or third-party AI services unless explicitly approved and under a data processing agreement (DPA).

- Ensure all datasets used in training or fine-tuning AI models are lawfully sourced and include appropriate consent mechanisms.

- Document data lineage, dataset composition, and any preprocessing techniques used.

# 4. Roles and Responsibilities (RACI Model)

- Responsible: End users of AI, Data Scientists, AI Developers, Product Teams

- Accountable: Chief AI Officer (CAIO), Chief Information Security Officer (CISO)

- Consulted: Legal Counsel, Data Privacy Officer (DPO), Ethics Committee, Risk Management

- Informed: All relevant staff interacting with AI systems and outputs

Departments are expected to maintain an internal AI Use Inventory and report new AI projects to the Governance Committee.

# 5. Human Oversight and Accountability

- AI decisions that affect individuals must include human-in-the-loop validation and approval.

- Document and log key decisions made with AI assistance.

- Require traceability for AI model logic, explainability of outcomes, and justification for usage.

- Designated personnel must regularly audit AI model performance and impact.

# 6. Security and Risk Mitigation

- AI tools must be vetted through the organization’s security review process.

- Prevent known AI-specific threats, including adversarial inputs, model inversion, prompt injection, and data poisoning.

- Use secure coding and MLOps practices, including version control, model registry, container security, and access control.

- Conduct periodic threat modeling and penetration testing for AI-integrated systems.

# 7. Training and Awareness

- All users must complete mandatory AI training covering ethical use, security, privacy, and organizational policies.

- Specialized training is required for developers, engineers, and data professionals handling sensitive models or data.

- AI literacy programs must be updated to include emerging risks and regulatory changes.

# 8. Enforcement and Sanctions

- Violations of this AUP will trigger investigations led by the Ethics, Compliance, and Security teams.

- Consequences may include revocation of system access, disciplinary action, contract termination, or legal proceedings.

- Whistleblowers reporting improper AI use are protected from retaliation.

# 9. Policy Review and Maintenance

- The AI Governance Committee will review this policy at least annually or upon significant changes in law, technology, or organizational priorities.

- Updates shall be communicated to all stakeholders and may trigger required retraining.

- Revisions will be informed by internal audits, regulatory developments, and stakeholder feedback.

# 10. Incident Reporting and Response

All users must promptly report suspected or actual violations of this policy or any misuse of AI technologies.

**Reporting Procedures:**

- Report incidents through the internal AI Incident Reporting Portal or directly to the Information Security Team.

- Use secure channels to submit concerns involving sensitive or confidential information.

- Reports may be submitted anonymously where legally permissible.

**Incident Types Include:**

- Unintended harmful output from AI (e.g., bias, hallucinations)

- Data privacy or security breaches linked to AI use

- Model drift or performance degradation

- Unauthorized AI tool use or access

- Shadow AI deployment

**Response Procedures:**

- Incidents are triaged by the AI Security and Governance teams.

- Investigations follow the organization’s established cyber incident response plan.

- Root cause analysis and policy updates may follow major incidents.

**Framework Alignment:**

- Aligns with NIST AI RMF “Manage” function and CSA AI Governance guidelines.

# 11. Shadow AI and Unapproved Tools

To ensure visibility, safety, and governance over all AI tools in use, the following policies apply:

**Restrictions:**

- Users must not deploy or use unvetted AI models, services, or scripts without prior review and approval by the AI Governance Committee.

- This includes open-source models, external APIs, and browser extensions with embedded AI.

**Detection and Monitoring:**

- The organization employs automated monitoring to detect unauthorized AI activity.

- Asset inventories and system scans will be used to identify potential shadow AI tools.

**Remediation:**

- Unapproved tools may be immediately disabled or blocked.

- Violations will trigger review and possible disciplinary action.

**Registration Process:**

- A centralized AI Usage Declaration Form must be submitted for all new AI tools or services.

- Review includes data privacy, security, IP, and ethics assessment.

**Framework Alignment:**

- Informed by Cloud Security Alliance and CSA AI Organizational Responsibility Working Group guidance.

# Definitions

This section provides key definitions to support consistent understanding of AI-related terminology used in this policy.

- **Artificial Intelligence (AI):** The simulation of human intelligence in machines programmed to think and learn.

- **Generative AI**: A class of AI models that can generate new content such as text, images, or code based on learned data.

- **Shadow AI:** The use of AI tools, systems, or models without formal approval or governance oversight.

- **Human-in-the-loop (HITL):** A design requirement where human oversight is mandatory in AI-driven decision-making processes.

- **Personal Identifiable Information (PII):** Information that can be used to identify an individual, such as name, SSN, email, or biometric records.

- **Data Minimization:** A principle requiring only the necessary amount of personal data be collected and processed.

# References

This policy aligns with the following industry standards and frameworks:

- NIST AI Risk Management Framework (AI RMF 1.0): <https://www.nist.gov/itl/ai-risk-management-framework>

- ISO/IEC 42001 – AI Management System Standard: <https://www.iso.org/standard/81228.html>

- EU Artificial Intelligence Act (2024 Draft): <https://artificialintelligenceact.eu/>

- Cloud Security Alliance (CSA) AI Governance Guidance: <https://cloudsecurityalliance.org>

- GAO AI Accountability Framework: <https://www.gao.gov/products/gao-21-519sp>

- U.S. Executive Order on Safe, Secure, and Trustworthy AI (2023): <https://www.whitehouse.gov/briefing-room/presidential-actions/>

# Appendix A – Executive Briefing Summary

- This policy supports enterprise alignment with NIST AI RMF, EU AI Act, and ISO/IEC 42001.

- Acceptable use principles are embedded in the organization’s broader Responsible AI strategy.

- The policy is part of a layered governance model including access controls, risk assessments, and audit trails.

# Appendix B – User Attestation Form

- I acknowledge that I have read, understood, and agree to abide by the AI Acceptable Use Policy.

- I understand the consequences of violating this policy.

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Appendix C – Training Checklist

- [ ] Completed AI Acceptable Use Policy training

- [ ] Completed AI security and threat awareness training

- [ ] Completed responsible use and ethics course

- [ ] Acknowledged AI-AUP via attestation form

- [ ] Reviewed most recent policy updates

# Document Control

Version: 1.0

Effective Date: [Insert Date]

Owner: AI Governance Program Office

Approved By: [Executive Sponsor or Oversight Committee]

Next Review Date: [Insert Date + 1 year]