

[Organization Name] AI Acceptable Use Policy

Version: 1.0 **Owner:** [Chief Information Security Officer] **Effective Date:** [Date]

Review Cadence: Annual or upon material change

1. Purpose and Objective

The purpose of this policy is to establish guidelines for how employees, contractors, and authorized personnel at [Organization Name] interact with artificial intelligence (AI) technologies during their employment. This framework ensures the protection of corporate and client data, maintains compliance with regulatory and contractual commitments, and promotes responsible AI adoption in alignment with frameworks such as the [NIST AI RMF / EU AI Act / ISO 42001].

2. Terminology

- **AI Applications:** Any software utilizing machine learning, generative, or agentic capabilities. Examples include ChatGPT, Microsoft Copilot, Claude, Gemini, Perplexity, GitHub Copilot, Cursor, and native AI integrations in existing SaaS products.
- **Generative AI:** Artificial intelligence models designed to produce text, source code, imagery, audio, video, or synthetic data.
- **Agentic AI:** Autonomous or semi-autonomous AI systems capable of executing multi-step workflows and interacting on behalf of the user.
- **Unauthorized (Shadow) AI:** Any AI tool or service being utilized within [Organization Name] that does not appear on the officially sanctioned software list.
- **Sensitive Information:** Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry (PCI) data, proprietary trade secrets, source code, cryptographic materials, authentication credentials, unreleased financial figures, client data protected under Non-Disclosure Agreements (NDAs), and any records marked as Confidential or Restricted.

3. Scope

This policy framework covers the following:

- Every employee, intern, contractor, and third-party representative working on behalf of [Organization Name].
- All AI applications, generative AI services, agentic AI frameworks, and AI functionalities embedded within SaaS platforms.
- All corporate-issued hardware as well as personal devices utilized for business operations (BYOD).
- All information classification tiers (Public, Internal, Confidential, Restricted).

4. Approved AI Solutions

The following AI solutions are officially approved for business purposes:

[Insert approved enterprise tools — e.g., Microsoft 365 Copilot, Claude for Business, ChatGPT Enterprise, Gemini for Workspace, GitHub Copilot Business]

Any application absent from this list is considered unauthorized and strictly forbidden for internal use. This prohibition extends to the use of personal accounts on otherwise approved platforms (e.g., utilizing a personal ChatGPT Plus subscription for work tasks).

Exceptions must be documented and formally approved in writing by the [AI Review Board].

5. Data Classification and Permitted AI Use

DATA CLASSIFICATION	DESCRIPTION	PERMITTED AI USE
Public	Data explicitly approved for public release Examples: Marketing copy, press releases, published website content, public product documentation	Any approved tools Examples: Publicly available/free tiers of AI tools may be used for general research, provided no login linking corporate credentials is required
Internal	Data not meant for public release but carrying low security risk Examples: Standard operating procedures, non-sensitive internal memos, meeting agendas	Enterprise tools only Approved AI platforms governed by a zero-retention data agreement
Confidential	Sensitive organizational data	Restricted enterprise &

	requiring protection. Examples: Unreleased financial forecasts, strategic plans, legal contracts, partner data under NDA, network architecture	anonymization Permitted ONLY on approved Enterprise platforms. Users MUST abstract, redact, or anonymize identifiable entities (names, precise figures, internal project codes) before submitting the prompt.
Restricted	Highly sensitive, regulated, or proprietary data Examples: PII, Protected Health Information (PHI), credit card data (PCI), proprietary source code, passwords/keys.	Strictly prohibited No input allowed into any AI tool (enterprise or public). Processing is only permitted on localized, on-premise, air-gapped AI environments explicitly authorized by the CISO

6. Prohibited Activities

The following activities are strictly forbidden across all platforms and data categories, without exception:

- Inputting Restricted data (e.g., PHI, PCI, security secrets, proprietary source code) into any AI tool without prior written authorization.
- Relying solely on AI-generated outputs to make decisions impacting individuals (such as employment, lending, medical, legal, or regulatory matters) without documented, verifiable human oversight.
- Publishing or distributing content that presents AI-generated material as human-authored, particularly where disclosure is legally or ethically required.
- Using AI to generate source code or materials specifically designed to circumvent security mechanisms, access controls, or compliance protocols.
- Employing personal AI accounts for business duties, or authenticating into sanctioned AI platforms using personal credentials.
- Transmitting client data protected by NDA into AI platforms that are not secured under an enterprise master service agreement.
- Leveraging AI technologies to spoof or impersonate any person or entity.
- Permitting third-party AI vendors to train their models on [Organization Name]'s proprietary data, unless explicitly authorized by contract.

7. Mandatory Human Verification

Manual human verification is mandatory prior to utilizing AI-generated outputs in these specific scenarios:

- Outbound communications directed at clients, partners, regulatory bodies, or media outlets.
- The drafting of legal agreements, contracts, and compliance filings.
- Determinations regarding security and privacy (e.g., access provisioning, data dissemination, granting policy exceptions).
- Human resources and employment actions (e.g., recruitment, performance evaluations, terminations).
- Fiscal and financial authorizations exceeding \$[Threshold Amount].
- Source code being merged or committed into live production environments.

Reviewing personnel are required to record and document the completion of their review within the appropriate system of record.

8. Shadow AI Discovery

[Organization Name] maintains the authority to identify, audit, and eliminate unapproved AI applications from organization networks and managed hardware. The [Security Team] will routinely conduct discovery sweeps for unauthorized AI usage leveraging [Approved Discovery Solutions].

9. Monitoring and Technical Safeguards

To ensure compliance, [Organization Name] may implement the following technical safeguards:

- Active, real-time inspection of prompts submitted to sanctioned AI platforms (utilizing Block, Warn, and Audit configurations).
- Cross-platform data redaction across integrations such as Microsoft Teams, Slack, Gmail, Google Workspace, Zendesk, and Salesforce.
- Endpoint telemetry and monitoring to detect unsanctioned applications, locally hosted LLMs, and unauthorized personal AI activity on company hardware.
- Retention of system audit logs for a minimum duration of [Retention Period].
- Centralized governance managed via [Designated AI Governance Platform].

Staff members are hereby notified that interactions with AI tools may be logged, monitored, and reviewed in accordance with applicable legislation and [Organization Name]'s official privacy

policies.

10. Incident Notification Procedures

Personnel are required to notify [security@organization.com] of the following events within [24 hours / 1 business day]:

- The accidental or unintentional submission of restricted information to any AI platform.
- The generation of AI outputs that appear to expose another entity's proprietary or confidential information.
- Any suspected instances of prompt injection, jailbreaking, or malicious model manipulation.
- The creation or distribution of AI-generated content that resulted in, or had the potential to result in, harm or reputational damage.
- The observation of unauthorized (shadow) AI usage by a colleague or external vendor.

Reports made in good faith are protected under whistleblower guidelines; conversely, failing to report known incidents constitutes a policy violation.

11. Education and Awareness

AI acceptable use training is mandatory for all staff during onboarding and on an [cadence] basis thereafter. Specialized, role-centric training modules will be provided to engineering, legal, cybersecurity, and client-facing departments.

12. Disciplinary Actions

Failure to comply with these guidelines may lead to the following outcomes, based on the severity of the infraction: mandated remedial training, revocation of AI access privileges, formal disciplinary proceedings up to and including employment termination, and potential civil or criminal litigation. Egregious offenses (such as the deliberate exfiltration of data or repeated mishandling of restricted information) may result in immediate dismissal.

13. Governance Roles

- **AI Review Board:** Evaluates and approves tools, grants policy exceptions, and oversees high-risk AI deployments.

- **Security Team:** Implements technical enforcement controls, manages incident response, and conducts unauthorized AI discovery.
- **Legal Department:** Maps regulatory requirements and reviews vendor AI service agreements.
- **Privacy Officer:** Executes Data Protection Impact Assessments (DPIAs) for proposed AI workflows.
- **People / HR Team:** Administers training programs and manages the disciplinary escalation process.
- **Employees:** Maintain strict compliance, fulfill reporting duties, and complete required educational modules.

14. Policy Maintenance

This governance document will undergo review annually, or immediately following any material changes (e.g., the introduction of a major new AI system, shifts in regulatory landscapes, or significant security incidents). All material updates require formal ratification by the [AI Review Board].

15. Employee Acknowledgment

All personnel must formally acknowledge receipt and understanding of this policy during onboarding, and annually thereafter. Records of this acknowledgment will be maintained within the [HR Management System].