SAMPLE POLICY - Artificial Intelligence (AI) Governance, Responsible Use, and Employment Decision-Making

Effective Date: _____

Approved By: _____

Policy Owner: _____

How to Use This Policy

This is a master template. Not every section applies to every organization. Use it in three steps:

Step 1 — Find your stage. Each stage includes everything below it, plus its own additions.

Stage	This is you if…
1 — Open Use	You let people use AI tools as they see fit. No approved list. Tools are standalone and used by hand.
2 — Approved Tools	You've decided which tools are allowed and which aren't. Use is still mostly standalone.
3 — Connected & Embedded	AI is built into systems you already use (Copilot, Gemini, AI in your HRIS / ATS / CRM). It can reach company data and is often on by default.
4 — Agentic	AI doesn't just draft — it takes actions for you across systems (sends, schedules, updates records).

Step 2 — Keep the sections for your stage. Each section is tagged with the stage that triggers it. Keep everything tagged *All stages*, plus everything tagged for your stage and below. Delete the rest.

Section	Applies to
1 Purpose, 2 Scope, 3 Definitions, 4 Guiding Principles, 5 Acceptable Use, 6 Prohibited Uses	All stages
7 AI Tool Classification	Stage 2 and up
8 Data Privacy & Security (8.1–8.4)	All stages; 8.4 expands at Stage 3
9 AI Governance	Light at all stages; named ownership at Stage 3
10 Employment & HR Use, 11 Recruiting & Screening	All stages that hire
11.4 Applicant Notice	Stage 3 (or wherever AI touches screening)
12 Embedded & Connected AI	Stage 3 and up
13 Agentic AI Controls	Stage 4
14–21 + Addendum	All stages

Step 3 — Fill in the brackets and delete the drafting notes. Bracketed text like `[Company Name]` is for you to complete. Indented notes marked *Drafting note* are guidance — delete them before you publish.

---

1. Purpose

Applies to: All stages

[Company Name] recognizes that Artificial Intelligence ("AI"), including Generative AI ("GenAI"), machine learning systems, predictive analytics, automated decision-making tools, and related technologies, can improve productivity, innovation, customer service, business operations, and workforce management.

The purpose of this Policy is to establish standards for the responsible, ethical, secure, transparent, and legally compliant use of AI technologies. This Policy is intended to:

- Promote innovation while protecting employees, applicants, customers, and business partners.
- Ensure compliance with applicable federal, state, local, and international laws governing privacy, employment, discrimination, consumer protection, and intellectual property.
- Protect confidential, proprietary, and personal information.
- Prevent discriminatory or unfair outcomes resulting from AI systems.
- Establish governance, accountability, oversight, and risk management practices for AI use.
- Ensure that AI supports, rather than replaces, appropriate human judgment.

2. Scope

Applies to: All stages

This Policy applies to:

- All employees, officers, directors, temporary workers, contractors, consultants, interns, and third parties acting on behalf of the Company.
- All AI technologies used, developed, purchased, licensed, implemented, or accessed by the Company, **including AI features embedded in software the Company already uses, whether or not those features were separately adopted.**
- All business functions, including recruiting, hiring, HR, operations, finance, sales, marketing, customer service, information technology, legal, and compliance.

This Policy applies to both:

- Company-approved AI systems; and
- Publicly available third-party AI tools, including but not limited to ChatGPT, Gemini, Claude, Copilot, Midjourney, DALL-E, Perplexity, and similar technologies.

3. Definitions

Applies to: All stages (Embedded AI applies at Stage 3+; Agentic AI applies at Stage 4)

Artificial Intelligence (AI). Any machine-based system that can generate predictions, recommendations, decisions, content, classifications, rankings, or outputs that influence physical or virtual environments.

Generative AI (GenAI). AI systems capable of generating text, images, audio, video, code, analyses, summaries, or other content.

Automated Employment Decision Tool (AEDT). Any AI-enabled or algorithmic system that substantially assists or replaces discretionary decision-making in employment-related decisions, including recruitment, screening, hiring, promotion, discipline, compensation, performance evaluation, retention, or termination.

High-Risk AI System. Any AI system that may significantly affect individuals' rights, opportunities, employment, privacy, safety, or access to services.

Embedded AI. *(Stage 3+)* Artificial intelligence features built into software, platforms, or services the Company already licenses or uses — for example, AI assistants within productivity suites, customer relationship management systems, applicant tracking systems, or human resource information systems. Embedded AI is frequently enabled by default and may operate without a separate decision to adopt it. For purposes of this Policy, embedded AI is subject to the same governance, data-handling, and oversight requirements as standalone AI tools, including configuration review and vendor verification.

Agentic AI. *(Stage 4)* Artificial intelligence systems that can take autonomous actions to pursue a goal — such as sending communications, scheduling, creating or modifying records, executing transactions, or triggering workflows across one or more systems — rather than only generating output for a person to review. Because agentic AI may act without a person reviewing each step, its use requires additional controls, including pre-authorization of permitted actions, activity logging, defined scope limits, and the ability to suspend or stop the system.

4. Guiding Principles

Applies to: All stages

The Company's use of AI shall be guided by the following principles:

4.1 Human-Centered Design. AI shall augment human capabilities and decision-making rather than replace human judgment in matters involving significant business, employment, legal, ethical, or safety consequences.

4.2 Fairness and Non-Discrimination. AI systems shall be designed, selected, tested, monitored, and used in a manner that promotes equal opportunity and avoids unlawful discrimination.

4.3 Transparency. The Company will provide appropriate transparency regarding the use of AI and maintain documentation regarding AI systems and their intended uses. Transparency obligations to applicants, employees, and consumers attach to AI used in decisions about people; they do not require disclosure of routine internal use of AI for drafting, research, or productivity.

4.4 Accountability. Humans remain accountable for decisions assisted by AI systems. Employees may not shift responsibility for decisions to an AI tool.

4.5 Privacy and Data Protection. The Company will protect personal, confidential, and proprietary information throughout the AI lifecycle.

4.6 Security. AI systems must be deployed and managed using appropriate cybersecurity safeguards.

4.7 Reliability and Accuracy. AI outputs must be validated before use in business operations or decision-making.

5. Acceptable Use of AI

Applies to: All stages

Employees may use approved AI tools for legitimate business purposes including:

- Drafting communications
- Research assistance
- Brainstorming
- Summarization
- Translation
- Data analysis
- Coding assistance
- Process automation
- Training and educational purposes
- Customer service support
- Administrative tasks

All AI-generated outputs must be reviewed and verified by a qualified human before being relied upon or distributed.

> *Drafting note (Stage 1): If you do not maintain an approved-tool list, replace "approved AI tools" above with a short "smart use" standard — e.g., "any reputable AI tool, provided employees follow the data boundary rules in Section 8." The data rules carry the weight when there is no tool gate.*

6. Prohibited Uses

Applies to: All stages

Employees may not use AI systems to:

- Violate any law or regulation.
- Create discriminatory, harassing, retaliatory, or offensive content.
- Generate false or misleading information intentionally.
- Circumvent Company policies.
- Make unauthorized commitments on behalf of the Company.
- Create deepfakes, deceptive content, or fraudulent communications.
- Engage in unlawful surveillance.
- Process sensitive data without authorization.
- Upload confidential or proprietary Company information into unauthorized AI systems.
- Upload personal information into public AI tools unless specifically approved and legally permissible.

7. AI Tool Classification

Applies to: Stage 2 and up

The Company maintains a current list of AI tools, organized into the categories below. The list is maintained by [Policy Owner / IT / AI Governance Committee] and is available to all employees at [location].

- **Approved** — Tools the Company has reviewed and permits for the uses described. Employees may use these for legitimate business purposes consistent with this Policy.

- **Approved with conditions** — Tools permitted only for specific uses, data types, roles, or settings. The conditions are stated next to the tool.
- **Requires approval** — Tools the Company has not yet reviewed. Employees must request approval before using them for Company work.
- **Prohibited** — Tools the Company does not permit for any Company purpose. Employees may not use these for Company work or with Company data.

A tool's absence from the list does not mean it is approved. Any AI tool not listed as Approved or Approved-with-conditions is treated as Requires approval.

7.1 Requesting a New Tool. An employee who wants to use an AI tool that is not approved should submit a request through [process], including the tool, the intended use, and the types of data involved. [Owner] will review the tool for security, privacy, contractual, and compliance fit before approving it.

7.2 Unapproved Use (Shadow AI). Using AI tools that are not approved — or entering Company data into them — creates risk the Company cannot see or manage. An employee who has already used an unapproved tool for Company work should report it through [channel] so the use can be assessed. The Company's priority is identifying and managing risk, not penalizing good-faith disclosure.

> *Drafting note: The shadow-AI language above favors disclosure over punishment, which surfaces hidden use instead of driving it underground. A more control-oriented organization may replace the final sentence with a statement that unapproved use is a policy violation. Choose one.*

8. Data Privacy and Information Security

Applies to: All stages (8.4 expands at Stage 3)

8.1 Confidential Information. Employees shall not enter the following into public or unapproved AI systems:

- Trade secrets
- Proprietary business information
- Customer information
- Employee records
- Financial information
- Strategic plans
- Non-public legal information
- Passwords, credentials, or access keys

8.2 Personal Information. Personal information may only be processed through AI systems when:

- Authorized by the Company;
- Necessary for a legitimate business purpose;
- Appropriate security controls exist; and
- Processing complies with applicable privacy laws.

8.3 Data Minimization. Only the minimum amount of data necessary to achieve a business purpose shall be processed.

8.4 Security and Configuration. Security controls for AI use shall be appropriate to how a tool accesses and handles Company data.

For standalone tools, the data boundaries and minimization requirements in Sections 8.1–8.3 are the primary safeguard.

(Stage 3+) For embedded and connected AI — features built into platforms the Company already uses — the Company shall, before enabling or continuing to use the feature, verify:

- What Company data the feature can access, and whether that access respects existing user permissions, so the feature does not surface information to users who should not see it;
- Whether Company data is retained by, or used to train, the vendor's models, and whether that can be disabled;
- The data-residency, tenant, and administrative settings that govern the feature; and
- That the feature is configured to the most restrictive settings consistent with its business purpose.

Existing enterprise security controls — access management, multi-factor authentication, encryption, logging, and data loss prevention — continue to apply to AI use. They need not be duplicated for AI where they already cover the underlying systems.

9. AI Governance

Applies to: All stages (named ownership and risk assessments apply at Stage 3)

9.1 Ownership and Oversight. The Company assigns responsibility for AI governance as follows:

- [Policy Owner] owns this Policy and its periodic review.
- *(Stage 3+)* [AI Governance Committee / named roles] is responsible for reviewing AI initiatives, conducting risk assessments, approving high-risk AI implementations, monitoring regulatory developments, and maintaining AI standards and controls.
- [IT / Security] is responsible for configuration, access, and security of AI systems.
- [HR / Legal] is responsible for employment, privacy, and non-discrimination compliance.

> *Drafting note: At Stage 1, a single named owner is enough. Name real roles rather than leaving "the Company may establish" language — unowned responsibilities are the most common failure point.*

9.2 AI Inventory. *(Stage 2+)* The Company shall maintain an inventory of approved AI systems and their intended uses. *(Stage 3+)* The inventory shall also identify AI features embedded in existing systems, including any that score, rank, screen, or otherwise evaluate applicants or employees (see Sections 11.2 and 12).

9.3 Risk Assessments. *(Stage 3+)* Before deployment, high-risk AI systems shall undergo documented assessments evaluating:

- Privacy risks
- Security risks
- Bias risks
- Employment risks
- Consumer protection risks
- Legal compliance

10. Employment and Human Resources Use of AI

Applies to: All stages that hire

10.1 General Rule. The Company may use AI-assisted tools to support HR processes only when appropriate safeguards, oversight, and compliance measures are in place. AI may assist HR professionals but may not replace meaningful human review and decision-making.

10.2 Human Oversight Requirement. No applicant or employee shall be subject to a significant employment decision based solely on an AI-generated recommendation or automated decision. A qualified human reviewer must evaluate relevant information before making:

- Hiring decisions
- Promotion decisions
- Termination decisions
- Discipline decisions
- Compensation decisions
- Performance decisions

11. Recruiting and Applicant Screening Requirements

Applies to: All stages that hire (11.4 applies at Stage 3 or wherever AI touches screening)

11.1 Non-Discrimination. AI systems used in recruiting, screening, ranking, interviewing, testing, or hiring must not discriminate on the basis of any legally protected characteristic, including but not limited to: race, color, religion, sex, pregnancy, sexual orientation, gender identity, national origin, age, disability, veteran status, genetic information, or any other protected classification under applicable law.

11.2 Verification and Prohibition of Automatic Rejection. No applicant shall be screened out, rejected, ranked out of consideration, or subjected to any adverse employment decision solely through AI-based decision-making, without meaningful human review.

(Stage 3+) Because screening, ranking, and filtering features may be built into applicant tracking, recruiting, or HRIS platforms — and may operate by default — the Company shall not assume that human review is occurring. Before using any such system, and periodically afterward, the Company shall:

- Ask the vendor, in writing, whether the system scores, ranks, filters, automatically advances, or automatically rejects applicants, and on what basis;
- Identify which of the Company's existing recruiting and HR systems include these features and whether they are active;
- Disable or constrain automatic advancement or rejection where present, or insert a documented human review step before any adverse decision; and
- Retain the vendor's responses and the Company's configuration decisions as part of its AI records.

11.3 Bias Testing and Audits. Where AI is used in employment-related decision-making, the Company shall conduct periodic assessments, audits, or validation studies designed to identify and mitigate disparate impact or discriminatory outcomes. Such reviews may include selection rate analyses, adverse impact analyses, validation studies, bias assessments, and fairness testing.

11.4 Applicant Notice. *(Stage 3+, or wherever AI touches screening)* Where AI is used to screen, rank, assess, or otherwise evaluate applicants, the Company will notify applicants at the application stage that AI is used in the hiring process, including:

- That AI is used, and at what stage;

- The general categories of information the AI evaluates;
- How to request a reasonable accommodation or an alternative evaluation process; and
- Any additional disclosures required by applicable state or local law.

The placement and timing of this notice — for example, in the job posting, in the application portal, or in a separate notice — shall follow the requirements of the jurisdictions in which the Company recruits.

Notice obligations under this Section apply to AI used in decisions about people. They do not apply to internal use of AI for content generation, drafting, research, or similar productivity purposes that do not make or materially inform decisions about applicants or employees.

11.5 Accommodation and Alternative Review. Applicants who require accommodations due to disability or other legally protected reasons shall be provided an alternative evaluation process when required by law.

11.6 Recordkeeping. The Company shall maintain records relating to AI-assisted employment processes as required by applicable law.

12. Embedded and Connected AI

Applies to: Stage 3 and up

This Section governs AI features built into systems the Company already uses, which may be enabled by default and may reach Company data.

12.1 Default-On Features. When a vendor enables or introduces an AI feature in a system the Company already uses, the feature shall be evaluated before it is relied upon for Company work. [Owner] decides whether to keep the feature enabled, restrict it, or disable it, and records that decision in the AI inventory.

12.2 Vendor Verification. Before relying on an embedded AI feature, the Company shall confirm with the vendor what the feature does — specifically whether it generates, scores, ranks, filters, recommends, or acts — and what Company data it uses. For features that evaluate applicants or employees, follow the verification steps in Section 11.2.

12.3 Access and Oversharing. Embedded AI shall be configured so that it respects existing user permissions and does not surface information to users who would not otherwise have appropriate access to it (see Section 8.4).

12.4 Configuration. Embedded AI shall be configured to the most restrictive settings consistent with its business purpose, including settings that govern data retention and model training (see Section 8.4).

13. Agentic AI Controls

Applies to: Stage 4

This Section applies to AI systems that take autonomous actions rather than only generating output for review.

13.1 Pre-Authorization. Before an agentic AI system is permitted to take any action with business, legal, financial, or employment consequences, [Owner] shall define and approve the specific actions the system may take and the limits on those actions.

13.2 Action Logging. Agentic AI systems shall maintain a log of the actions they take, sufficient to reconstruct what the system did, when, and on whose authorization.

13.3 Scope Limits and Stop Control. Agentic AI systems shall operate within defined scope limits, and the Company shall maintain the ability to suspend or stop the system. Consequential or irreversible actions shall require human confirmation before execution.

13.4 Continued Accountability. The use of agentic AI does not change Section 4.4. A human remains accountable for the actions an agentic system takes on the Company's behalf, even where no person reviewed the individual action.

14. Third-Party AI Vendors

Applies to: All stages (verification deepens at Stage 3)

Prior to implementing a third-party AI solution, the Company shall evaluate:

- Security practices
- Privacy practices
- Compliance controls
- Bias mitigation processes
- Audit capabilities
- Contractual protections
- Regulatory compliance representations

Vendors may be required to provide documentation demonstrating compliance with applicable AI, privacy, employment, and anti-discrimination laws. *(Stage 3+)* For AI embedded in systems the Company already uses, the vendor-verification steps in Sections 11.2 and 12.2 apply.

15. Intellectual Property

Applies to: All stages

Employees remain responsible for ensuring AI-generated content does not infringe copyrights, misappropriate trade secrets, violate trademarks, or violate contractual obligations. AI-generated content must be reviewed before publication or external distribution.

16. Training

Applies to: All stages (manager/HR training deepens at Stage 3)

Employees using AI systems shall receive training regarding responsible AI use, privacy requirements, security requirements, bias and discrimination risks, human oversight obligations, employment law compliance, and Company-approved AI tools. Managers and HR personnel shall receive additional training regarding AI-assisted employment decisions.

17. Monitoring, Auditing, and Compliance

Applies to: All stages

The Company reserves the right to monitor AI use on Company systems and audit AI-generated outputs.

18. Reporting Concerns

Applies to: All stages

Employees must promptly report suspected policy violations, AI-generated discrimination, privacy concerns, security incidents, unauthorized AI use, and inaccurate or harmful AI outputs. Reports may be made through established reporting channels without fear of retaliation.

19. Violations

Applies to: All stages

Violations of this Policy may result in disciplinary action up to and including revocation of AI access privileges, corrective action, termination of employment, and legal action where appropriate.

20. Policy Review

Applies to: All stages

This Policy shall be reviewed at least annually and updated as necessary to reflect technological developments, changes in applicable laws, regulatory guidance, and industry best practices.

21. Disclaimer

Applies to: All stages

Nothing in this Policy is intended to interfere with or restrict employee rights protected under applicable labor laws, including rights protected by the National Labor Relations Act or similar state laws.

Employment AI Compliance Addendum

Applies to: All stages that hire

The Company specifically intends that any AI-assisted recruiting, hiring, promotion, compensation, discipline, performance management, or termination practices comply with:

- Title VII of the Civil Rights Act
- ADA
- ADEA
- EEOC guidance regarding AI
- State AI employment laws and regulations
- State privacy laws
- Biometric privacy laws where applicable
- Consumer privacy laws governing automated decision-making

No AI system may be implemented in employment-related decision-making unless the Company has documented:

- Human oversight procedures;
- Bias testing procedures;
- Applicant notification procedures where required;
- Privacy and security controls; and
- A process for addressing applicant or employee concerns regarding AI-assisted decisions.

This Policy is a sample template provided for informational purposes and does not constitute legal advice. Organizations should consult qualified legal counsel before adopting or relying on any AI governance policy.