# Guidelines for Fair and Responsible AI Usage

## Chapter 1: General

### 1.1 Introduction

This document outlines the foundational principles, policies, and frameworks for the responsible use of artificial intelligence (AI) within the organization. The rapid integration of AI into various functions necessitates a proactive and principled approach to ensure its benefits are harnessed while potential risks are comprehensively managed.1 This policy extends the organization's core values to the domain of AI, establishing a commitment to fairness, transparency, and accountability as fundamental pillars of technological adoption.3 This document is designed to guide all employees and stakeholders in the ethical and safe deployment of AI systems, whether internally developed, procured from third parties, or based on open-source models.5

Effective AI governance is not a one-time compliance exercise but a continuous process that encompasses the entire lifecycle of an AI system, from its design and development to its deployment and ongoing operation.1 This framework provides a structured approach to mitigate risks such as inherent biases, privacy infringements, and security vulnerabilities that can arise from the human element in AI creation and maintenance.2 The policy's balanced perspective reflects the organization’s dual commitment to being an "innovation-first" entity that also prioritizes "customer safety" above all else.5 By establishing clear guardrails and a systematic review process, the organization can foster innovation while safeguarding against unnecessary risks, protecting its reputation, and building trust with customers and the public.5

### 1.2 Purpose

The primary purpose of this document is to provide a comprehensive framework that clarifies how employees can and cannot use AI at work. By outlining specific guidelines and sanctioned processes, the policy aims to achieve several key objectives. First, it serves to reduce risk by providing employees with clear guardrails for acceptable use, minimizing the likelihood of unintentional policy violations or unsafe AI adoption.5 Clear and actionable definitions of AI are essential for accurately identifying AI in real-world applications and applying appropriate governance measures. Without them, definitions can be misinterpreted, leading to misaligned and inconsistent oversight [Image 1]. This also helps in addressing the risks associated with "shadow AI," which are AI use cases that are not managed by the AI governance framework [Image 1]. Second, it fosters a culture of responsible innovation by establishing a clear, sanctioned process through which new AI use cases can be proposed, reviewed, and approved.5 This encourages the exploration of new technologies while ensuring that all adoption aligns with the organization's risk tolerance. Third, the policy is an essential tool for ensuring regulatory compliance and mitigating financial, legal, and reputational risks.1 It provides a consistent and auditable system for managing AI-related risks, safeguarding the organization from potential liabilities and maintaining its standing as a trustworthy entity.

### 1.3 Subject

The scope of this policy is comprehensive, covering all AI systems and models utilized by the organization, regardless of their origin.5 This includes, but is not limited to, internal instances of AI created by fine-tuning open-source models, foundation models like ChatGPT, Gemini, and Claude, and any other AI tools, services, or platforms adopted for internal or external use.5 The policy applies equally to AI systems used for internal business processes, such as synthesizing meeting notes or analyzing data, as it does to customer-facing applications or models that inform critical business decisions, such as hiring or lending.5 This broad application ensures a consistent standard of governance and risk management across the entire technological landscape of the organization.

### 1.4 Revision and Termination

This policy is a dynamic, or "living," document that will undergo regular review to reflect the rapid pace of technological innovation, emerging risks, and evolving legal and regulatory landscapes.2 Revisions will be triggered by significant events, including but not limited to, the introduction of new AI models, changes in the terms of use for third-party vendors, or the enactment of new regional or industry-specific regulations, such as the EU AI Act.1 The designated AI governance committee will be responsible for periodically revisiting the risk management plan, updating risk categories, and incorporating lessons learned to address new challenges.6

In addition, a formal process for the termination of a policy section or the discontinuation of an approved AI system will be established. This process will be initiated if an AI system's risk profile changes, its performance deviates significantly from established benchmarks, or it is found to be non-compliant with updated legal or ethical standards.2 A clear termination clause ensures that the organization can react swiftly and decisively to mitigate new or evolving risks.

### 1.5 Scope of Application

This policy applies to every individual who interacts with, develops, or deploys AI systems on behalf of the organization. This includes all full-time employees, contractors, and consultants.5 The policy's reach extends to all departments and business units that utilize AI. Crucially, it also governs the use of third-party AI systems and vendors. The organization acknowledges that a vendor's compliance risk is, in effect, its own.8 Therefore, this policy mandates that all third-party AI systems must be vetted and managed according to the same rigorous standards as internally developed systems. This comprehensive scope ensures a unified and consistent approach to AI governance across the entire enterprise.

### 1.6 Key Definitions

To ensure a shared understanding across the organization, it is important to clarify key terminology related to AI systems [Image 2].

* **Model:** An AI model is a mathematical or logical representation that uses machine learning to process input data and generate outputs. These can include functions that predict the likelihood of an outcome or a large language model (LLM) that generates text based on a prompt.
* **System:** An AI system is a broader concept that includes the AI model itself, as well as the software components, infrastructure, and workflows that enable it to be deployed in real-world applications. A single system can contain multiple AI models and a large number of software features.

## Chapter 2: Risks and Points to Note Concerning AI Use

### 2.1 Primary Risks of AI

The deployment of AI systems, while offering significant opportunities, introduces a complex array of risks that must be systematically identified and mitigated. These risks are not isolated but are often interconnected, with a vulnerability in one area leading to a cascade of negative consequences in another. For effective governance, these risks are categorized into three primary areas: Technical, Societal, and Operational & Security.

#### Technical Risks

* **System Failures and Unpredictable Behaviors:** AI systems can be susceptible to bugs, data inconsistencies, or unforeseen interactions with their environment, which can lead to system failures.9 In high-stakes applications like medical diagnosis or autonomous vehicles, such failures can have severe consequences.9 Due to the complexity of many AI models, their decision-making processes can be opaque, leading to unpredictable behaviors when they encounter novel scenarios outside of their training data.9
* **Adversarial Attacks and Model Poisoning:** AI models, particularly those based on machine learning, are vulnerable to malicious manipulation. Adversarial attacks involve making subtle modifications to input data to deceive the AI system and lead to incorrect outputs or decisions.9 A more insidious threat is model poisoning, where attackers inject malicious data or subtly modify existing data to compromise the integrity of the AI system during its training phase.10 This can lead to biased outcomes or unauthorized access to the system.
* **Scalability and Robustness Issues:** An AI model that performs well in a controlled, limited environment may fail to maintain its performance when scaled up to real-world applications with diverse and unpredictable inputs.9 Ensuring the robustness of AI systems across a wide range of scenarios remains a significant challenge.
* **Supply Chain Attacks:** AI systems often rely on a network of external software libraries, frameworks, and APIs. If any of these dependencies are compromised or maliciously altered, it can introduce vulnerabilities into the entire AI system, enabling unauthorized access or control by attackers.10

#### Societal Risks

* **Bias and Discrimination:** A significant risk is that AI models can learn and perpetuate biases present in their training data, leading to unfair and discriminatory outcomes.9 This can manifest in critical areas such as hiring, lending, or criminal justice, where biased decisions can exacerbate social inequalities.9 The policy must emphasize the need for thorough bias audits and mitigation techniques throughout the AI lifecycle.11
* **Concentration of Power:** AI’s ability to process vast amounts of data and automate complex tasks could lead to an unprecedented accumulation of economic and political power within a few organizations.9 This concentration could threaten fair competition and democratic processes.9
* **Misinformation and Manipulation:** Generative AI can be used to create highly realistic fake content, including deepfakes, to spread misinformation at scale, manipulate public opinion, and undermine trust in institutions.9 This risk is compounded by AI-enabled social engineering attacks that can deceive individuals.10
* **Impact on Human Labor:** The increasing automation of tasks by AI has the potential to displace human labor, leading to job loss and socioeconomic inequalities.10 The ethical considerations of this impact and the need for upskilling and retraining must be a part of the long-term strategic plan.

#### Operational & Security Risks

* **Data Breaches and Privacy Infringement:** AI systems, which require and process large volumes of data, are attractive targets for cybercriminals.10 Breaches can result in unauthorized access to sensitive information, including personal data, financial records, or research data, leading to identity theft and misuse.10
* **Malicious Use of AI:** AI technology can be harnessed for nefarious purposes, such as developing sophisticated phishing attacks, creating autonomous weapons, or automating social engineering techniques, which pose significant risks to individuals and society.10
* **Lack of Transparency:** Many advanced AI systems, especially deep learning models, operate as "black boxes," making their decision-making processes difficult to understand or audit.9 This lack of explainability poses a critical challenge to accountability.9 When a system makes a negative decision, it can be unclear who should be held responsible—the developers, the users, or the AI itself. This ambiguity creates a significant risk for legal and ethical frameworks where accountability is a requirement.

### 2.2 Points to Note Concerning AI Use

In addition to the primary risks, the following points must be given careful consideration for every AI use case.

* **Privacy and Data Protection:** All AI systems must operate within the strict boundaries of data protection protocols and legal requirements.1 Robust data security and privacy standards must be implemented to mitigate risks from data breaches and unauthorized access, particularly for sensitive consumer data.1 The organization must ensure that all AI systems comply with regional AI regulations and data protection laws, such as GDPR and CCPA.1
* **Intellectual Property and Plagiarism:** Employees must be aware that generative AI models can produce content that infringes upon intellectual property rights, leading to issues of plagiarism and unauthorized use of copyrighted materials.10 This policy strictly prohibits the use of third-party content without the necessary permissions and requires a clear process for confirming that AI outputs do not violate intellectual property laws.14
* **Regulatory Compliance:** The organization must maintain a proactive stance toward regulatory compliance by staying updated on relevant regional AI regulations and industry-specific guidelines.1 This includes ensuring that third-party vendors' practices also align with these evolving requirements.7 Regular updates to internal policies and practices are essential to ensure ongoing adherence to all applicable laws and standards, thereby enhancing trust and efficiency.1

## Chapter 3: Risk Judgment/Inventory

### 3.1 Use of AI

AI use cases are classified based on the potential risks they present to the organization, its employees, and its customers. The policy delineates three categories of use: approved, restricted, and prohibited. Acceptable AI uses are those that are low-risk and do not involve sensitive company or personal data, such as summarizing meeting notes or drafting internal communications.5 These uses are generally sanctioned and do not require a formal review.

A second category includes AI uses that may be acceptable but require further review. This applies to use cases that could influence material decisions for employees or customers (e.g., hiring, credit), are externally-facing, or involve any use of company confidential or personal data.5 This formal review process, which is detailed in the Screening Policy section, ensures that potential risks are thoroughly assessed and mitigated before the AI system is deployed.

### 3.2 Prohibited AI

Certain AI applications are strictly prohibited within the organization due to their potential to cause significant harm, compromise ethical standards, or violate legal requirements. These uses are not eligible for review and are forbidden under all circumstances.5

Prohibited AI uses include, but are not limited to:

* Using subliminal, manipulative, or deceptive techniques that could influence a person’s behavior.14
* Exploiting vulnerabilities related to age, disability, or socio-economic circumstances.14
* Generating or promoting disinformation, misinformation, or false online engagement.14
* Making automated decisions in domains that significantly affect an individual’s rights or well-being, such as law enforcement, credit, employment, or housing, without a human-in-the-loop oversight mechanism.14
* Providing tailored legal, medical, or financial advice.14
* Categorizing individuals based on their biometric data to deduce sensitive attributes like race, political opinions, or religious beliefs.14
* Using content from third parties without the necessary permissions or legal right.14
* Collecting or processing personal data without complying with legal requirements.14

### 3.3 Risk Judgment

The process for judging the risk of an AI system is based on a structured methodology to ensure consistency and thoroughness. The core of this process is the NIST AI Risk Management Framework, which consists of four key steps 6:

* **Govern:** Establish the governance structure, such as an AI Governance Committee, with clear oversight roles for managing AI accountability.6
* **Map:** Understand the specific context of the AI use case, including its purpose, the data it uses, and who relies on its outputs.6 This involves identifying all potential risks associated with the system.
* **Measure:** Evaluate the potential impact and likelihood of each identified risk. A risk matrix is used to classify severity (e.g., insignificant, major, catastrophic) and likelihood (e.g., improbable, likely) to arrive at a quantified risk rating.6
* **Manage:** Implement safeguards and mitigation strategies to address the identified risks. This may include enhancing data security protocols, embedding bias-detection algorithms, or setting up fallback systems to minimize disruptions.6

The following table serves as a guide for measuring the risk of an AI system:

| Likelihood ↓ / Severity → | Insignificant | Minor | Moderate | Major | Catastrophic |
| --- | --- | --- | --- | --- | --- |
| Low | Low Risk | Low Risk | Medium Risk | High Risk | Extreme Risk |
| Medium | Low Risk | Medium Risk | Medium Risk | High Risk | Extreme Risk |
| High | Medium Risk | High Risk | High Risk | Extreme Risk | Extreme Risk |

### 3.4 Screening Policy

All AI use cases that fall into the "requires review" category must be submitted for formal screening.5 The screening process is designed to ensure that new AI adoptions are aligned with the organization's risk appetite and ethical principles. Employees must submit a formal intake form that details the proposed use case, its purpose, the data involved, and a preliminary risk assessment.

The intake form is then reviewed by a cross-functional committee of experts. This committee typically includes business leaders who provide context on the business problem, as well as AI risk specialists who evaluate the technical and ethical risks.5 This collaborative process ensures that the evaluation is comprehensive, balancing business needs with a thorough understanding of potential risks and compliance requirements. The committee's review culminates in an official decision to approve, reject, or request modifications to the proposed use case.5

### 3.5 AI Checklist

To assist employees and the screening committee in their review, a detailed AI checklist will be used to evaluate each proposed system. The checklist is built around the core dimensions of responsible AI and includes questions that must be answered to assess the system's safety and alignment with organizational standards.15 The checklist covers the following areas:

* **Fairness and Bias:** Has the training data been audited for bias? Have bias mitigation techniques been applied? Is the system's performance evaluated across diverse groups to ensure equitable outcomes? 11
* **Transparency and Explainability:** Is the model interpretable? Is there clear documentation on the system's design and data sources? Can the outputs and decisions be explained to both technical and non-technical stakeholders? 11
* **Privacy and Security:** What data is used, and is it adequately protected? Are robust cybersecurity protocols in place to prevent data breaches? Are legal and privacy requirements met? 11
* **Validity and Reliability:** Has the system undergone rigorous testing and validation? Is there a process for continuous monitoring of its performance to ensure accuracy and consistency? 11
* **Accountability:** Are the roles and responsibilities of stakeholders (e.g., developers, owners, users) clearly defined? Are there mechanisms to monitor and audit the system for compliance? 11

### 3.6 AI Inventory (AI List)

The establishment of a centralized AI inventory is crucial for effective enterprise-level risk management. This inventory is not merely a list; it is a dynamic database that provides a single source of truth for all AI systems utilized within the organization.5 This centralized tracking enables strategic decision-making by providing a clear overview of the organization's total AI risk exposure and adoption patterns [Image 9].

The inventory will track the following core attributes for each AI system:

| Attribute | Description | Justification |
| --- | --- | --- |
| **Purpose and Scope of the Use Case** | A brief description of the problem the AI is solving and its boundaries. | Essential for understanding the business value and context, and for aligning with the organization's strategic goals. |
| **Type of AI Employed in the Use Case** | The specific type of AI technology used (e.g., predictive, generative, computer vision). | Important for assessing technical risk and for ensuring the right skills are available for management and oversight. |
| **Data Used in the Use Case** | The type and sensitivity level of the data used for training, processing, or inference. | Critical for evaluating privacy and security risks and for ensuring compliance with data protection laws. |
| **AI Risks and Mitigations Associated with the Use Case** | A summary of the identified risks (e.g., bias, security, performance drift) and the controls in place to mitigate them. | Allows for a quick assessment of the system’s risk profile and the effectiveness of its governance measures. |
| **Status and Governance of the AI Use Case** | The current status (e.g., in review, approved, deployed, decommissioned) and the governance policies applied. | Provides visibility into the approval workflow and ensures that systems are not deployed without proper authorization and oversight. |
| **Third Party AI Model Information** | The name of the third-party provider, model name, and contractual obligations. | Necessary for managing third-party risks and ensuring that the vendor’s practices align with the organization's standards. |

By maintaining a comprehensive and up-to-date AI inventory, the organization can aggregate risk data across all its AI systems. This allows for a holistic, macro-level view of the entire AI portfolio, which is the foundation for effective enterprise-level risk management. Without this granular data, it would be impossible to accurately assess the total risk exposure or to make informed strategic decisions about resource allocation and risk tolerance.8

## Chapter 4: AI Lifecycle Management

### 4.1 All-inclusive Image of AI Lifecycle

AI governance is an end-to-end process that requires continuous oversight across the entire AI lifecycle. This lifecycle is best understood as a series of interconnected stages: Planning, Stage Prior to Contract and Release, and During-the-term Management [Image 3]. This framework ensures that ethical considerations, risk assessments, and governance protocols are embedded from the very beginning of a project and continue throughout its entire operational life. It is not a linear process but rather a feedback loop where insights from later stages inform and improve earlier ones, ensuring the framework remains dynamic and adaptable.16

### 4.2 Planning Stage

#### 4.2.1 Role of the AI Development Department

The planning stage is the foundation of any AI project. The AI development department is responsible for meticulously defining the business problem, establishing success metrics, and identifying user requirements.16 A key part of this is assessing the technical and organizational feasibility of the proposed project, including determining the type of AI model needed and the availability and quality of the required data.17 This upfront work is critical, as it aligns business leaders, data engineers, and compliance teams around a unified vision, preventing costly rework later in the process.16 The development department must also create a comprehensive risk profile for the proposed AI solution, considering both technology and business-related risks.17

#### 4.2.2 Role of the AI Screening Department

The AI screening department's role in the planning stage is to provide an early-stage review of the proposed use case. Their primary responsibility is to perform an initial risk assessment and ensure that the project aligns with the organization's documented risk appetite and all relevant legal and regulatory requirements.6 This early intervention ensures that projects with a high-risk profile or those that fall into the "prohibited" category are identified before significant resources are committed to their development.

### 4.3 Stage Prior to Contract and Release

#### 4.3.1 Role of the AI Development Department

During this phase, raw data is acquired, processed, and transformed into a format suitable for model training.16 The development team is responsible for ensuring data quality by cleaning, normalizing, and enriching it, as data integrity directly impacts the reliability of AI outcomes.1 They then build and iteratively train the model, a process that requires rigorous testing to optimize for accuracy, efficiency, and fairness.16 For high-stakes applications, a "human-in-the-loop" oversight mechanism must be implemented to ensure a human can review and override AI-generated decisions.11 The team must also prepare all necessary documentation for the AI model, including data sources and the rationale for its design.11

#### 4.3.2 Role of the AI Screening Department

The screening department conducts a final, rigorous audit of the AI system before it is deployed. This pre-release validation is a critical check-and-balance in the governance framework. The department is responsible for conducting thorough bias audits of both the training data and the algorithms and for validating the system's performance across diverse groups to ensure equitable outcomes.11 They must also verify that the system is transparent, that its decisions are interpretable, and that clear documentation is in place. This final review ensures that the system is compliant with all internal policies and external regulations, and that a process for redress is established to address any unintended consequences.11

### 4.4 During-the-term Management

#### 4.4.1 Role of the AI Development Department

Once an AI system is deployed, the AI development department's role shifts to continuous monitoring and maintenance. This involves tracking the system's performance indicators and observing for signs of "data drift," a gradual shift away from established benchmarks that can degrade performance over time.8 They are responsible for retraining models as needed, addressing any identified issues, and implementing containment protocols in the event of a malfunction or malicious attack.11 They also manage all change requests, ensuring that any modifications to the system are properly documented and communicated.

#### 4.4.2 Role of the AI Screening Department

The screening department provides ongoing oversight and audits of deployed AI systems. Their continuous monitoring role ensures that systems remain in compliance with both internal policies and external regulations.8 This is particularly important for models that can "drift" over time, leading to changes in output quality and reliability.2 The screening department also manages the change management process, ensuring that any proposed updates or modifications to an AI system are properly screened for new risks before being implemented. This separation of duties between the builder (development) and the auditor (screening) is a fundamental principle of effective governance, ensuring that a single group does not prioritize speed over safety.12

## Governance with Skills, Knowledge, and Culture

Effective AI governance is not solely a matter of technology and policy; it is fundamentally about the people, skills, and culture of the organization. A safety-oriented culture is a critical risk mitigation strategy, fostering an environment where all employees understand and prioritize responsible AI usage.12 This requires clearly defined roles and a comprehensive set of skills.

The five key roles involved in AI governance are Executives, Builders, Custodians, Use Case Owners, and Business Users [Image 4]. Each role has a unique set of responsibilities and requires a combination of three main skill types to manage AI-specific risks effectively [Image 4]:

* **Technical Skills:** Knowledge of AI implementation, security protocols, and benchmarking is essential for builders and custodians.4
* **Cross-Functional Skills:** This includes expertise in AI governance, legal compliance, and risk management, which are crucial for executives and custodians.6
* **Behavioral Skills:** A familiarity with business ethics and responsible decision-making is necessary for all roles, especially use case owners and business users.4

The following table provides a high-level overview of the roles and their responsibilities across the AI lifecycle:

| Role | Responsibility during AI Lifecycle |
| --- | --- |
| **Executives** | Sets the overall tone and culture for responsible AI. Invests in training and resources. Responsible for high-level governance and risk appetite. |
| **Builders** | Develops and integrates AI models. Responsible for technical implementation, security, and continuous monitoring. |
| **Custodians** | Oversees AI governance framework. Responsible for risk assessments, policy enforcement, and auditing. Acts as the guardian of ethical AI principles. |
| **Use Case Owners** | Identifies business problems and proposes AI solutions. Responsible for submitting use cases for review and ensuring they align with business objectives. |
| **Business Users** | Interacts with and uses AI tools to perform their work. Responsible for adhering to the policy and reporting any misuse or concerns. |

This collaborative, cross-functional approach ensures that accountability is not a vague concept but is tied to specific functions and people. It minimizes the risk of a single department prioritizing speed and innovation over safety and compliance, thereby strengthening the entire governance framework.12 In addition, the Board of Directors and senior leadership—including the CEO, CIO, and CDO—should establish dedicated committees to address AI-specific challenges and ensure clear responsibility for AI governance [Image 4]. Operational risk departments should also update their capabilities to enable effective AI governance.

## Uplift Practices for Managing Third-Party AI Risks

The use of third-party AI systems introduces a new class of risks that must be managed proactively, as a vendor's failure in governance or security can directly impact the organization.7 To mitigate these risks, the organization must go beyond checkbox diligence and integrate AI-oriented controls into its vendor risk management framework.7

Key practices for managing third-party AI risks include:

* **Revisiting Vendor Contracts:** Update agreements to require vendors to disclose their use of AI in service delivery. Include provisions for transparency, notification of changes, and clear data-handling practices.7
* **AI-Specific Due Diligence:** Perform enhanced due diligence by asking targeted questions about the vendor’s AI model design, data sources used for training, risk controls, explainability, and monitoring processes.7 This is crucial as there can be information asymmetry, where vendors have more information about their models than the organization using them [Image 3].
* **Enhancing Risk-Tiering Frameworks:** Modify risk scoring to account for AI use cases. Prioritize due diligence based on the type of AI deployed, the sensitivity of the data used, and the potential business impact of an AI failure or misuse.7
* **Continuous Monitoring:** Establish a process for ongoing monitoring of third-party systems, not just a one-time vetting process.7 This includes staying ahead of emerging regulations and ensuring the vendor’s practices align with the latest regional and sector-specific requirements.7

This approach transforms the management of third-party risk from a reactive exercise into a strategic function that enables responsible AI adoption while mitigating risk exposure.7 Additionally, the organization must be wary of over-reliance on a single third-party provider, as this can increase risk exposure [Image 3].

## Govern AI Infrastructure

The governance of AI systems is intrinsically linked to the security of the underlying infrastructure that supports them. Secure AI infrastructure is a prerequisite for fair and responsible AI usage, as it safeguards the entire AI data pipeline from initial data acquisition to final deployment.4

Key practices for governing AI infrastructure include:

* **Securing the AI Data Pipeline:** Implement robust security measures to protect data at every stage, from collection and storage to processing and use. This is crucial to prevent data breaches and unauthorized access to sensitive information.4
* **Protecting Model Artifacts:** Safeguard the trained AI models from theft or tampering. Measures should include strict access controls and encryption to ensure the integrity of the models.4
* **Hardening Deployment Infrastructure:** Secure the environments where AI models are deployed and run. This involves implementing rigorous access management and protecting against malicious attacks that could disrupt operations or compromise the system.4
* **Continuous Monitoring and Response:** Implement automated monitoring tools to continuously track system performance and detect anomalies in real-time.18 This proactive approach allows for swift responses to security threats, operational failures, or performance degradation, ensuring that the system remains reliable and secure.4

By applying a Zero Trust model across all AI environments, the organization can ensure that security is not an afterthought but is woven into the very fabric of the AI infrastructure.4

## Conclusions and Recommendations

The creation of a comprehensive AI usage policy is a strategic imperative for any organization seeking to harness the power of artificial intelligence while proactively managing its inherent risks. This document provides a foundational framework for achieving this objective by consolidating best practices, outlining clear responsibilities, and establishing a continuous governance model.

The analysis indicates that effective AI governance is a collaborative, end-to-end process that requires a clear separation of duties. The distinction between the "AI Development Department" and the "AI Screening Department" is a critical system of checks and balances, ensuring that the drive for innovation is tempered by a commitment to safety, compliance, and ethical standards. This dual-role structure prevents a single group from prioritizing speed over safety, which is a significant organizational risk.

The AI inventory, a seemingly simple record-keeping tool, is identified as the central foundation for enterprise-level risk management. By tracking key attributes of every AI system, the organization can aggregate risk data to gain a holistic view of its entire AI portfolio. This enables senior leadership to make informed strategic decisions about resource allocation and risk tolerance, moving beyond a tactical, use-case-by-use-case approach to a truly strategic one.

This document serves as the first draft for the organization's AI usage guidelines. It is recommended that the governance committee review this report and customize the policy based on the organization's specific risk appetite. The policy should be operationalized through training, clear communication, and the implementation of the recommended tools and processes, ensuring that the principles outlined in this document are not just words on a page but are embedded into the daily operations and culture of the organization.

#### Works cited

1. AI Governance: Best Practices and Importance | Informatica, accessed August 25, 2025, <https://www.informatica.com/resources/articles/ai-governance-explained.html>
2. What is AI Governance? - IBM, accessed August 25, 2025, <https://www.ibm.com/think/topics/ai-governance>
3. onlinedegrees.sandiego.edu, accessed August 25, 2025, <https://onlinedegrees.sandiego.edu/ai-governance/#:~:text=There%20are%20four%20core%20principles,they%20work%20easier%20to%20understand.>
4. What Is AI Governance? - Palo Alto Networks, accessed August 25, 2025, <https://www.paloaltonetworks.com/cyberpedia/ai-governance>
5. AI Usage Policy: Defining Employee Acceptable AI Use, accessed August 25, 2025, <https://fairnow.ai/ai-acceptable-use-policy-template/>
6. How to Perform an AI Risk Assessment? Steps & Best Practices - Qualysec, accessed August 25, 2025, <https://qualysec.com/ai-risk-assessment/>
7. Responsible AI and third-party risk management: what you need to know - PwC, accessed August 25, 2025, <https://www.pwc.com/us/en/tech-effect/ai-analytics/responsible-ai-tprm.html>
8. How to Manage Third-Party AI Risk: 10 Tips for Financial Institutions - Ncontracts, accessed August 25, 2025, <https://www.ncontracts.com/nsight-blog/how-to-manage-third-party-ai-risk>
9. AI Risk Management Framework - Palo Alto Networks, accessed August 25, 2025, <https://www.paloaltonetworks.com/cyberpedia/ai-risk-management-framework>
10. Challenges of AI | Office of the Provost | Washington State University, accessed August 25, 2025, <https://provost.wsu.edu/challenges-of-ai/>
11. 7 actions that enforce responsible AI practices - Huron Consulting, accessed August 25, 2025, <https://www.huronconsultinggroup.com/insights/seven-actions-enforce-ai-practices>
12. AI Risks that Could Lead to Catastrophe | CAIS - Center for AI Safety, accessed August 25, 2025, <https://safe.ai/ai-risk>
13. Safeguard Cloud Endpoints for Effective AI Security - Microsoft, accessed August 25, 2025, <https://www.microsoft.com/en-sg/microsoft-365/business-insights-ideas/resources/importance-secure-cloud-endpoints-ai-onboarding>
14. Usage policies - OpenAI, accessed August 25, 2025, <https://openai.com/policies/usage-policies/>
15. Building AI Responsibly - AWS, accessed August 25, 2025, <https://aws.amazon.com/ai/responsible-ai/>
16. Optimizing Your AI Lifecycle: Designing, Deploying, and Governing AI | Tredence, accessed August 25, 2025, <https://www.tredence.com/blog/ai-lifecycle>
17. Generative AI lifecycle - AWS Documentation, accessed August 25, 2025, <https://docs.aws.amazon.com/wellarchitected/latest/generative-ai-lens/generative-ai-lifecycle.html>
18. Meet Davis, our powerful AI-engine - Dynatrace, accessed August 25, 2025, <https://www.dynatrace.com/platform/artificial-intelligence/>