1 PURPOSE 1

Company: eBay Inc.
Author(s): Mohammad Tahaei, Lauren Wilcox
File name: Responsible-AI-Policy.pdf

Summary

eBay's Responsible AI Policy outlines principles for the ethical and accountable use of AI, emphasizing risk management, inclusivity, and compliance with regulatory frameworks throughout the AI lifecycle.

1. AI Usage Boundaries

• Applies to all AI systems used by eBay and its subsidiaries.
• Covers both internal and customer-facing applications.

2. Ethical & Legal Considerations

• Compliance with applicable regulatory frameworks.
• Human oversight throughout AI system lifecycle.

3. Human vs AI Roles

• Human oversight is required in the development and deployment of AI systems.
• Documentation of key decisions is encouraged.

4. Oversight & Accountability

• Accountability is shared among all eBay personnel.
• The Responsible AI Committee oversees adherence to the policy.

5. Data Governance

• Privacy by Design principles guide AI system development.
• Focus on data minimization and quality.

6. Risk Management

• Risk-based approach to AI system development and deployment.
• Regular assessments to identify and rectify safety issues.

7. Transparency & Explainability

• Users are provided transparency about AI usage.
• Disclosure of AI type and usage context is prioritized.

8. Training & Awareness

• Employees are required to comply with the Responsible AI Policy.
• Training on responsible AI practices is implied.

9. Enforcement

• Compliance is mandatory for all eBay employees.
• Internal governance structures will ensure adherence.

10. Other Considerations

• Policy will be updated to reflect new laws and technologies.
• Inclusivity and fairness are prioritized in AI design.

Regulatory Citations

• EU AI Act
• EU AI Act, i

1.1. Supplier is not permitted to Process Protected Data for training , retraining or improving

Company: Cisco
Author(s): Unknown
File name: Supplier-AI-Policy.pdf

Summary

The Supplier Artificial Intelligence Policy outlines the governance framework for the use of AI and machine learning technologies by suppliers, emphasizing the need for express permission from Cisco for processing protected data and the establishment of a robust AI/ML governance program that adheres to industry standards.

1. AI Usage Boundaries

• Suppliers must obtain express written permission from Cisco to process protected data for AI/ML.
• Permission is limited to one year unless otherwise agreed.

2. Ethical & Legal Considerations

• Suppliers must comply with applicable laws and regulations.
• AI/ML governance programs must meet or exceed industry standards.

3. Human vs AI Roles

• Not specified in this policy.

4. Oversight & Accountability

• Cisco reserves the right to audit the supplier's AI/ML governance program before and after granting permission.

5. Data Governance

• Protected data includes administrative data, customer data, financing data, and personal data.
• Suppliers must manage and protect all forms of protected data.

6. Risk Management

• Suppliers must perform assessments and diligence as required by Cisco.

7. Transparency & Explainability

• Not specified in this policy.

8. Training & Awareness

• Not specified in this policy.

9. Enforcement

• Cisco can audit compliance with the AI/ML governance program.

10. Other Considerations

• Not specified in this policy.

Regulatory Citations

• Not specified in this policy.

---

3 Scope 03

Company: Unknown
Author(s): Unknown
File name: en-epo-ai-policy.pdf

1. AI Usage Boundaries

• Not specified in this policy

2. Ethical & Legal Considerations

• Not specified in this policy

3. Human vs AI Roles

• Not specified in this policy

4. Oversight & Accountability

• Not specified in this policy

5. Data Governance

• Not specified in this policy

6. Risk Management

• Not specified in this policy

7. Transparency & Explainability

• Not specified in this policy

8. Training & Awareness

• Not specified in this policy

9. Enforcement

• Not specified in this policy

10. Other Considerations

• Not specified in this policy

Regulatory Citations

• EU AI Act

---

artificial intelligence (“AI”) by individuals or entities that are members , contributors, contractors, and others who deal in

Company: National Association of Residential Property Managers (NARPM)
Author(s): Unknown
File name: narpm-ai-policy-march-2024.pdf

Summary

The Artificial Intelligence Usage Policy by NARPM establishes guidelines for the ethical and responsible use of AI technologies by its members and associates, emphasizing compliance with legal standards, data privacy, and accountability.

1. AI Usage Boundaries

• AI tools must be pre-approved by NARPM before use.
• Users must not expose confidential or proprietary information to AI.

2. Ethical & Legal Considerations

• Compliance with intellectual property, data protection, and anti-discrimination laws is mandatory.
• Users must consider the ethical implications of AI usage.

3. Human vs AI Roles

• Humans must verify the accuracy of AI-generated content before use.
• AI should not replace human judgment in critical decision-making.

4. Oversight & Accountability

• Users must be transparent about AI usage and seek approval from NARPM.
• Violations of the policy may result in disciplinary action.

5. Data Governance

• Users must protect confidential and proprietary information.
• Compliance with data privacy laws is required.

6. Risk Management

• Users should be vigilant against cybersecurity threats related to AI.
• AI-generated content must be screened for biases and inaccuracies.

7. Transparency & Explainability

• Users must clearly communicate how AI systems are utilized.
• NARPM may modify AI usage parameters based on organizational needs.

8. Training & Awareness

• Users must acknowledge understanding and commitment to the AI Usage Policy.
• Regular review of the policy is encouraged to stay updated.

9. Enforcement

• Breach of the policy may lead to disciplinary action, including termination.

10. Other Considerations

• Development of in-house AI technology requires NARPM clearance.

Regulatory Citations

• Not specified in this policy

DATA – ARTIFICIAL INTELLIGENCE POLICY | © Copyright 2024 , Nasdaq, Inc. All Rights Reserved

Company: Copyright 2024 , Nasdaq, Inc. All Rights Reserved
Author(s): Unknown
File name: Data_AI_Policy.pdf

Summary

The Nasdaq Artificial Intelligence Policy outlines the responsibilities and expectations for users regarding the use of Nasdaq Information in conjunction with AI technologies. It emphasizes compliance with licensing agreements, operational controls, and ethical considerations to ensure the integrity and security of the data while leveraging AI for enhanced productivity and creativity.

1. AI Usage Boundaries

• Use of Nasdaq Information must adhere to the terms of the license governing access.
• Prohibited to grant access to Nasdaq Information in open-source AI models without written agreement.

2. Ethical & Legal Considerations

• AI technologies must be used responsibly to avoid ethical and operational challenges.
• Compliance with applicable laws is mandatory when using AI models.

3. Human vs AI Roles

• Humans must ensure proper licensing and compliance when using AI tools.

• AI tools must operate under strict controls to prevent unauthorized access to Nasdaq Information.

4. Oversight & Accountability

• Users are responsible for monitoring access to Nasdaq Information.
• Audit trails must be maintained and provided to Nasdaq as required.

5. Data Governance

• Adequate controls must be implemented to adhere to licensing terms.
• Unauthorized use of Nasdaq Information must be reported to Nasdaq.

6. Risk Management

• Operational controls must prevent unauthorized redistribution of Nasdaq Information.
• Failure to control access may result in financial liabilities.

7. Transparency & Explainability

• Technical entitlement systems must be in place for audit and compliance.
• Users must provide accurate historical audit trail information.

8. Training & Awareness

• Users must be aware of their obligations under the licensing agreements.
• Training on compliance and operational controls is implied.

9. Enforcement

• Non-compliance with the policy may lead to termination of license rights.
• Users must purge or delete Nasdaq Information from AI models upon termination of agreements.

10. Other Considerations

• Distribution of derivative works is prohibited without appropriate licensing.
• Third-party AI tools must also comply with Nasdaq's licensing terms.

Regulatory Citations

• EU AI Act), Article 5: Prohibited AI Practices
• Regulation EU 2024/1689 (EU AI Act), Article 5: Prohibited AI Practices

---

Definitions.....04

Company: SourceCode
Author(s): Kristen Stippich & Kevin Dulaney
File name: Generative-Artificial-Intelligence-Policy.pdf

Summary

This policy outlines guidelines for the responsible use of Generative Artificial Intelligence (GAI) at SourceCode, emphasizing ethical principles, legal compliance, and accountability in its deployment and

utilization.

1. AI Usage Boundaries

• Applies to all employees, contractors, and third parties interacting with GAI systems.
• GAI systems must be deployed in alignment with ethical principles and company values.

2. Ethical & Legal Considerations

• GAI systems must respect user privacy rights and comply with applicable data protection regulations.
• Measures should be taken to mitigate bias and ensure fairness in outputs.

3. Human vs AI Roles

• Users must be informed when interacting with AI-generated content.
• Individuals responsible for GAI systems are accountable for their actions and decisions.

4. Oversight & Accountability

• The AI Taskforce is responsible for reviewing and approving GAI projects.
• Regular audits and evaluations of GAI systems will be conducted.

5. Data Governance

• GAI systems must adhere to data protection policies, including GDPR and CCPA.
• Personal data used for training must be anonymized or pseudonymized.

6. Risk Management

• Non-approved GAI systems are considered insecure until a Data Privacy Impact Assessment is completed.
• Security measures must be implemented to safeguard GAI systems.

7. Transparency & Explainability

• Users must be informed that content is AI-generated.
• Mechanisms for reporting concerns related to GAI content should be established.

8. Training & Awareness

• Employees must receive training on ethical AI principles and bias mitigation techniques.
• Awareness campaigns should educate stakeholders on responsible GAI use.

9. Enforcement

• Violations may result in disciplinary action, including termination.
• Suspected breaches should be reported to Company Management or the AI Taskforce.

10. Other Considerations

• All GAI projects must undergo an ethics review before deployment.
• Compliance with the policy is mandatory for all involved parties.

Regulatory Citations

• CCPA
• CCPA, and other relevant laws

• GDPR

DEPARTMENT: Ethics and Compliance POLICY DESCRIPTION: Responsible AI PAGE: 7 of 8 REPLACES POLICY DATED: EFFECTIVE DATE: October 1, 2024 REFERENCE NUMBER: EC.031 APPROVED BY: Ethics and Compliance Policy Committee information) in any form, and however stored, transmitted or generated, including, without limitation all archives, derivatives, modifications or manipulations of the foregoing information. Director of Responsible AI means the Colleague(s) identified by the RAI Governance Council from time to time who is responsible for the management and oversight of the Responsible AI Program. Machine Learning means an application of Artificial Intelligence that is characterized by providing systems the ability to automatically learn and improve based on Training Materials or experience, without being explicitly programmed. Malicious Software means any type of code, software, application, or program that is designed to: (1) cause unauthorized access to, theft of, or intrusion upon; or (2) otherwise disrupt, lock, or damage computer equipment, software, networks, infrastructure, or data (commonly referred to as malware, virus, worm, time bomb, ransomware, Trojan horse, or spyware); or (3) software that allows an individual, network, system, or User to bypass normal authentication or authorization functions or other security controls to a product, service, system, network, or other infrastructure or system that would allow the individual, network, system, or User to remain undetected or unaudited. Output(s) means any outcome, output, or other result, action, or decision obtained from or otherwise performed by or with the assistance of, an AI Technology and/or AI Solution. Responsible AI means the area of AI governance that applies across all AI Technology Activities and establishes guidelines to address safety and security, trustworthiness, transparency, fairness, and ethics. Responsible AI (RAI) Governance Council means the Sponsors, Steering Committee, and Advisory

Committee as confirmed from time-to-time within the Company who provide sponsorship of the Responsible AI Program and focus on impacts to the enterprise, funding, timeline, and major risks arising from AI Technology Activities. Responsible AI Framework means the Responsible AI governance framework that documents how Company addresses Responsible AI. Responsible AI Program means Company's program that oversees and administers Responsible AI and is designed to harmonize ethical considerations, technical advancements, regulatory adherence, and innovation through AI Solutions. Training Materials means the information (e.g., personal information, personally identifiable information, facts, and other non-copyrightable information), raw data (e.g., metadata, sensor data), content (e.g., licensed or unlicensed, public domain), and other input that is used to train or otherwise develop an AI Technology and/or AI Solution. Users means Colleagues, developers, subcontractors, and other professionals using, developing, or deploying AI Solutions. 4/2024

Company: Ethics and Compliance POLICY DESCRIPTION: Responsible AI PAGE: 1 of 8 REPLACES POLICY DATED: EFFECTIVE DATE: October 1, 2024 REFERENCE NUMBER: EC.031 APPROVED BY: Ethics and Compliance Policy Committee SCOPE: All HCA Healthcare ("Company") affiliated facilities worldwide including, but not limited to, hospitals, ambulatory surgery centers, home health centers, home health agencies, hospice agencies, physician practices, outpatient imaging centers, urgent care centers, Parallon, joint ventures and all Corporate Departments, Groups, Divisions, and Markets (collectively, "Affiliated Employers" and individually, "Affiliated Employer"). PURPOSE: To ensure the responsible development, deployment, and use of Artificial Intelligence ("AI") across the Company following the pillars of the Responsible AI Framework as outlined in the Company's Code of Conduct ("Code"). Responsible AI includes respecting individuals' privacy, promoting transparency, fairness, bias minimization, accountability, and operation in a safe and secure manner that strives to protect individuals from physical, emotional, environmental, and/or digital harm. POLICY: This policy applies to: employees', contractors', service providers', and/or vendors' (collectively, "Colleagues") use, engagement, development, or interaction with Company-owned, externally purchased, or publicly available AI Solutions; the data used, stored, and processed for training AI models, and any other tools instrumental in creating Outputs; and AI Solutions in any and all forms, including, without limitation, AI Solutions that are standardized, custom-developed, stand-alone, or bundled with or embedded into any product or service. 1. Acceptable Use The use of AI Solutions is solely for tasks that contribute directly to Company business objectives and duties and in alignment with the Code, applicable policies, procedures, and law. Colleagues are only allowed to use AI Solutions and tools approved by the Company. 2. Prohibited Use The Company has identified two specific uses of AI Solutions that are prohibited as a matter of Company policy. a. Dark Patterns. AI Solutions may not be used to distort,

impair, trick, or otherwise interfere with the ability of an individual to make autonomous and informed choices or decisions, or otherwise manipulate a person through subliminal techniques, or so-called dark patterns, to make (or not make) a particular decision or take/refrain from a particular action. b. Exploiting Vulnerabilities. AI Solutions may not be used to exploit potential vulnerabilities of an individual or to distort or impair their ability to make autonomous and informed choices or decisions or otherwise manipulate or cause physical or psychological harm to themselves or others. 3. Responsible AI Governance Council The Responsible AI ("RAI") Governance Council has been established to address areas of stakeholder engagement, ethical considerations, policy development, risk management, and compliance

Author(s): Ethics and Compliance Policy Committee
File name: HCA_Healthcare_Responsible_AI.pdf

Summary

This policy outlines HCA Healthcare's commitment to responsible AI usage, emphasizing ethical considerations, compliance, and risk management through a structured governance framework that includes a Responsible AI Governance Council.

1. AI Usage Boundaries

• AI Solutions must align with Company business objectives and the Code of Conduct.
• Prohibited uses include dark patterns and exploiting individual vulnerabilities.

2. Ethical & Legal Considerations

• Respect individuals' privacy and promote fairness.
• Minimize bias and ensure accountability.

3. Human vs AI Roles

• Human oversight is required in the final review of AI Outputs.
• Colleagues must engage in independent reviews of AI Outputs.

4. Oversight & Accountability

• The Responsible AI Governance Council oversees ethical considerations and compliance.
• Colleagues must report anomalies and compliance deviations.

5. Data Governance

• Data usage must comply with legal requirements and Company policies.
• Implement controls to protect individuals' privacy and rights.

6. Risk Management

• Conduct risk assessments during AI solution development and deployment.
• Solutions are subject to periodic audits for compliance.

7. Transparency & Explainability

• Colleagues must ensure AI Outputs are clear and understandable.
• Document key assumptions and decisions in solution development.

8. Training & Awareness

• Colleagues must complete training on acceptable AI use and compliance.
• Awareness of AI Acceptable Use Guidelines is required.

9. Enforcement

• The RAI Governance Council can review and rescind solution approvals.
• Non-compliance may lead to disciplinary actions.

10. Other Considerations

• Maintain an inventory of AI solutions.
• Ensure cybersecurity measures are in place to protect data.

Regulatory Citations

• General Data Protection Regulation, IP
• Not specified in this policy

---

driving principles that will ensure our work with AI meets the highest standards of ethics, legality,

Company: Lenovo
Author(s): Unknown
File name: CP-00027_Lenovo_AI_Policy.pdf

Summary

Lenovo's AI Policy outlines the principles for the responsible development and use of AI, emphasizing ethical, legal, and safety standards while ensuring accountability and transparency throughout the AI lifecycle.

1. AI Usage Boundaries

• Prohibits AI systems that harm individuals or exploit vulnerabilities.
• Applies to all AI systems developed, acquired, or used by Lenovo.

2. Ethical & Legal Considerations

• Ensures AI systems do not discriminate based on protected characteristics.
• Requires informed consent for data collection and processing.

3. Human vs AI Roles

• Human oversight is essential in AI decision-making.
• Significant decisions should not rely solely on AI outputs.

4. Oversight & Accountability

• Establishes mechanisms for human intervention and oversight.
• AI systems must include capabilities for detecting and rectifying biases.

5. Data Governance

• AI systems must comply with data privacy principles.
• Data used for AI must be owned or licensed appropriately.

6. Risk Management

• AI systems posing significant risks will undergo additional scrutiny.
• Technical robustness and safety measures must be implemented.

7. Transparency & Explainability

• AI systems must be explainable and transparent to users.
• Users should be informed about data handling and AI interactions.

8. Training & Awareness

• Employees must be aware of the ethical implications of AI use.
• Regular reviews of AI systems for bias and fairness are required.

9. Enforcement

• Compliance with the policy will be monitored post-release.
• Violations of the policy may lead to corrective actions.

10. Other Considerations

• Environmental and social impacts of AI systems must be evaluated.
• Commitment to diversity and inclusion in AI development.

Regulatory Citations

• Not specified in this policy

Foreword i

Company: Unknown
Author(s): Unknown
File name: AFDN 25-1 Artificial Intelligence.pdf

1. AI Usage Boundaries

• Not specified in this policy

2. Ethical & Legal Considerations

• Not specified in this policy

3. Human vs AI Roles

• Not specified in this policy

4. Oversight & Accountability

• Not specified in this policy

5. Data Governance

• Not specified in this policy

6. Risk Management

• Not specified in this policy

7. Transparency & Explainability

• Not specified in this policy

8. Training & Awareness

• Not specified in this policy

9. Enforcement

• Not specified in this policy

10. Other Considerations

• Not specified in this policy

Regulatory Citations

• 15 U.S.C. 9401

Generative AI technology, including chatbots, virtual assistants, and similar applications, is increasingly prevalent

Company: State of Iowa
Author(s): Department of Management
File name: State of Iowa Generative Artificial Intelligence (AI) Policy.pdf

Summary

This policy establishes guidelines for the responsible and ethical use of generative AI technologies within the State of Iowa, outlining minimum requirements, prohibited uses, and accountability measures to mitigate risks associated with AI adoption.

1. AI Usage Boundaries

• Applicable to all business use cases including content generation, software code development, and decision making.
• Prohibits the use of freely available AI tools without prior written approval.

2. Ethical & Legal Considerations

• Prohibits use of AI for harmful, illegal, or unethical activities.
• Requires consultation with legal counsel regarding AI-generated code and intellectual property rights.

3. Human vs AI Roles

• Human fallback systems must be in place if AI solutions fail.

• Citizens must have the option to engage with a human representative instead of AI.

4. Oversight & Accountability

• Supported Entities and workforce members are accountable for decisions made using generative AI.
• Senior leadership is responsible for compliance with the policy.

5. Data Governance

• Sensitive and protected data cannot be used to train AI tools without authorization.
• AI outputs must undergo human evaluation before finalization.

6. Risk Management

• Supported Entities must identify and mitigate business and security risks related to AI use.
• Prohibits the use of AI technologies that discriminate or invade privacy.

7. Transparency & Explainability

• AI-generated code must be clearly marked to indicate AI involvement.
• Outputs generated by AI must not be used verbatim or as the sole reference.

8. Training & Awareness

• Mandatory training on ethical AI use, privacy, and security.
• Ongoing awareness efforts to keep workforce informed about AI developments.

9. Enforcement

• Violations of the policy may result in disciplinary actions.
• Waivers to the policy may be granted under specific conditions.

10. Other Considerations

• Prohibits impersonation and manipulation of information using AI.
• AI outputs cannot be protected by intellectual property rights.

Regulatory Citations

• Iowa Code Chapter 216
• Iowa Administrative Code 129-8.4(8B)

---

operators to utilize data to pr oactively enhance safet y, efficiency, equity, resil iency, and sustainability. The

Company: Intelligent Transportation Society of America (ITS America)
Author(s): Unknown
File name: ITS-America-AI-Policy-Principles-Rebrand.pdf

Summary

The AI Policy Principles developed by ITS America aim to guide the safe, transparent, and effective deployment of AI technologies in transportation, focusing on enhancing safety, efficiency, equity,

resiliency, and sustainability while building public trust in these technologies.

1. AI Usage Boundaries

• AI is an enhancement tool for existing transportation technologies, not a replacement.
• AI applications should be deployed to achieve specific and tangible outcomes.

2. Ethical & Legal Considerations

• Support for a modern national data privacy law.
• Evaluation of data privacy and security needs based on data storage and processing locations.

3. Human vs AI Roles

• Encouragement of a human-centric approach to AI deployment.
• Development of workforce training programs to prepare transportation workers for AI tools.

4. Oversight & Accountability

• Support for guidelines on assessing risks and impacts of AI systems.
• Call for a clear governance structure to promote AI accountability at the Federal agency level.

5. Data Governance

• Support for high-quality, representative data inputs for AI applications.
• Encouragement of research on AI equity and dataset biases.

6. Risk Management

• Adoption of guidelines for ongoing evaluation of AI system risks.
• Prioritization of cybersecurity measures in AI deployment.

7. Transparency & Explainability

• Development of transparency guidelines for AI applications.
• Support for standards of explainability for AI systems.

8. Training & Awareness

• Recommendation for a robust workforce development plan related to AI tools.
• Encouragement for accessible AI advancements for users.

9. Enforcement

• Call for robust reporting requirements for harmful incidents associated with AI.
• Developers and operators should be held accountable for their AI systems' performance.

10. Other Considerations

• Support for AI applications that improve safety, equity, and sustainability in transportation.

Regulatory Citations

• NIST Cybersecurity 2.0 Framework
• NIST AI Risk Management Framework
• NIST Assessing Risks and Impacts of AI Program

Phone: (775) 684-5800 I it.nv.gov I CIO@it.nv.gov I Fax: (775) 687-9097

Company: State of Nevada
Author(s): Joe Lombardo, Timothy D. Galluzi, Darla J. Dodge, David 'Ax' Axtell, Bob Dehnhardt
File name: Policy on the Responsible and Ethical Use of Artificial Intelligence in Nevada - CIO Signed.pdf

Summary

This policy outlines the responsible and ethical use of Artificial Intelligence (AI) within the Nevada State Government's executive branch, establishing minimum standards for AI deployment while promoting safety, compliance, and innovation across agencies.

1. AI Usage Boundaries

• Permissible uses include brainstorming ideas and summarizing public data.
• Non-permitted uses include creating discriminatory content and using personal data without anonymization.

2. Ethical & Legal Considerations

• AI systems must mitigate harmful biases to avoid discrimination.
• Privacy rights must be preserved by design in AI implementations.

3. Human vs AI Roles

• Critical AI decisions must involve human review to maintain ethical standards.
• Agencies determine the appropriate level of human oversight for their use cases.

4. Oversight & Accountability

• The State Technology Governance Committee (STGC) oversees AI policy implementation.
• Legal and compliance specialists define and oversee AI accountability.

5. Data Governance

• Data must be classified into categories such as aggregate, de-identified, and anonymous.
• AI systems must adhere to stringent data protection standards, including encryption.

6. Risk Management

• Regular security risk assessments are required, with agencies conducting additional assessments as needed.
• Agencies are encouraged to implement additional security measures based on their risk profiles.

7. Transparency & Explainability

• AI use must be well-documented and disclosed to enable accountability.
• Clear documentation of AI methodologies and decision-making processes is required.

8. Training & Awareness

• Mandatory safety training for personnel involved in AI operations is required.

• AI-related content should be included in annual security awareness training for all state employees.

9. Enforcement

• Agencies must report AI-related incidents and participate in regular audits.
• A mandatory reporting system for suspected AI misuse is established.

10. Other Considerations

• Agencies are encouraged to develop their own AI policies that meet or exceed baseline standards.
• Feedback mechanisms will be established to inform policy updates.

Regulatory Citations

• NRS 603A
• NRS 205.473 to NRS 205.513
• NIST AI Risk Management Framework
• NRS 205.0832

---

position Rwanda as a global innovator for responsible and inclusive AIAI

Company: Ministry of ICT and Innovation, Republic of Rwanda
Author(s): Unknown
File name: Artificial_Intelligence_Policy.pdf

Summary

The National AI Policy of Rwanda aims to leverage artificial intelligence for economic growth and improved quality of life while ensuring responsible and inclusive AI practices. It serves as a roadmap to harness AI's benefits while mitigating associated risks, positioning Rwanda as a leading African innovation hub through collaboration with various stakeholders.

1. AI Usage Boundaries

• AI applications must align with national development objectives.
• AI should be used responsibly to enhance public services and economic growth.

2. Ethical & Legal Considerations

• Establish ethical guidelines for AI development and implementation.
• Strengthen AI policy and regulation to ensure public trust.

3. Human vs AI Roles

• Humans are to be reskilled for AI and data skills.
• AI is to enhance public service delivery and efficiency.

4. Oversight & Accountability

• Establish a Presidential Council on AI for advisory roles.
• Create a network of AI Ethics Officers across government institutions.

5. Data Governance

• Develop frameworks for ethical and secure data sharing.
• Improve accessibility and availability of AI-ready data.

6. Risk Management

• Implement safety precautions to prevent harm from AI solutions.
• Establish a risk-sharing fund to support R&D; in the public sector.

7. Transparency & Explainability

• Promote transparency in AI applications to build public trust.
• Engage in participatory consultations to update ethical guidelines.

8. Training & Awareness

• Invest in a National Skills Building Program for AI and data skills.
• Adapt education curricula to include AI and digital technologies.

9. Enforcement

• Strengthen regulatory authorities to ensure compliance with AI standards.
• Promote ethical guidelines through government-led initiatives.

10. Other Considerations

• Foster international collaboration to benchmark AI competitiveness.
• Support private sector AI adoption through targeted investments.

Regulatory Citations

• Not specified in this policy

Procedures Artificial Intelligence & Generative A rtificial Intelligence

Company: Unknown
Author(s): Unknown
File name: Corporate Artificial Intelligence Policy.pdf

1. AI Usage Boundaries

• Not specified in this policy

2. Ethical & Legal Considerations

• Not specified in this policy

3. Human vs AI Roles

• Not specified in this policy

4. Oversight & Accountability

• Not specified in this policy

5. Data Governance

• Not specified in this policy

6. Risk Management

• Not specified in this policy

7. Transparency & Explainability

• Not specified in this policy

8. Training & Awareness

• Not specified in this policy

9. Enforcement

• Not specified in this policy

10. Other Considerations

• Not specified in this policy

Scope 3

Company: Chartered Institute of Public Finance and Accountancy (CIPFA)
Author(s): Unknown
File name: Generative-Artificial-Intelligence-(AI)-Policy.pdf

Summary

The CIPFA Generative AI Policy establishes guidelines for the ethical and acceptable use of generative AI in assessments, ensuring fairness, integrity, and confidentiality while maintaining the value of qualifications. It applies to all assessment-related activities and emphasizes the importance of human oversight and accountability in the use of AI technologies.

1. AI Usage Boundaries

• Generative AI is not permitted in summative assessments or live exams.
• AI may be used in formative assessments with clear guidelines and monitoring.

2. Ethical & Legal Considerations

• Maintain academic integrity and avoid plagiarism.
• Ensure AI systems do not exhibit bias or discrimination.

3. Human vs AI Roles

• Human oversight is required in the use of AI for formative assessments.
• AI should be used as a tool to support, not replace, human judgment.

4. Oversight & Accountability

• ATPs are responsible for validating AI-generated results.
• Malpractice related to AI use will be reviewed by the Examination Panel.

5. Data Governance

• AI systems must be regularly monitored to minimize bias.
• Data manipulation and unauthorized access to assessment content are prohibited.

6. Risk Management

• Establish robust policies to prevent AI-related malpractice.
• Investigate any unauthorized use of AI under the Academic Offences Policy.

7. Transparency & Explainability

• Students must be informed about permitted AI use in assessments.
• AI outputs should be critically evaluated and validated.

8. Training & Awareness

• Educators should guide students on ethical AI use in assessments.
• Students should seek feedback from educators on AI integration.

9. Enforcement

• Violations of AI use guidelines will be addressed according to the Assessment Offences Policy.
• Malpractice includes cheating, unauthorized AI use, and data manipulation.

10. Other Considerations

• AI is not allowed as a sole marker in summative assessments.
• CIPFA aims to uphold the integrity and reputation of its qualifications.

Regulatory Citations

• Ofqual General Conditions of Recognition

Section 1: Preamble 3

Company: United Nations
Author(s): High-Level Committee on Management (HLCM) Task Force
File name: Framework for a Model Policy on the Responsible Use of AI in UN System_0.pdf

Summary

The framework outlines a model policy for the responsible use of AI within UN System Organizations, emphasizing ethical governance, risk management, and accountability to enhance operational efficiency while safeguarding human rights and addressing potential risks associated with AI deployment.

1. AI Usage Boundaries

• Applicable to AI systems and AI-supported services used by UN System Organizations.
• Encourages adherence to ethical standards and existing internal regulations.

2. Ethical & Legal Considerations

• Emphasizes transparency, fairness, and accountability in AI deployment.
• Addresses data protection, privacy, and potential for discriminatory outcomes.

3. Human vs AI Roles

• AI should enhance human decision-making and operational efficiency.
• Personnel should focus on higher-level tasks as routine tasks are automated.

4. Oversight & Accountability

• Establishes an institutional accountability structure for AI impact assessments.
• Encourages multidisciplinary approaches to risk management.

5. Data Governance

• Promotes adherence to UN Principles on Personal Data Protection and Privacy.
• Requires systematic mapping, measurement, and management of AI-related risks.

6. Risk Management

• Introduces principles, rules, and controls for mitigating AI-related risks.
• Calls for continuous monitoring and re-assessment of AI risks.

7. Transparency & Explainability

• AI deployment must be transparent and accountable.
• Organizations should ensure clarity in AI decision-making processes.

8. Training & Awareness

• Capacity-building for staff is essential to ensure compliance with AI policies.
• Encourages consultations with stakeholders prior to policy updates.

9. Enforcement

• Framework serves as guidance rather than mandatory requirements.
• Organizations are encouraged to issue detailed policies and guidelines.

10. Other Considerations

• Framework aims for consistency and harmonization among UN System Organizations.
• Addresses the need for ethical guidelines in AI integration.

Regulatory Citations

• Proposed Normative Foundations for an International Data Governance Framework: Goals and Principles
• International Data Governance – Pathways to Progress
• UN Principles on Personal Data Protection and Privacy
• UN Secretary General’s Roadmap for Digital Cooperation: Ensuring the Protection of Human Rights
• UN Secretary-General’s Guidance on Human Rights Due Diligence for Digital Technology Use

• EU AI Act
• ISO/IEC 42001 -2023 : Information technology — Arti■cial intelligence — Management

---

This document is the sole property of Firstsource Solutions Limited. Any use or duplication of this document

Company: Firstsource Solutions Limited | RESTRICTED | March 11, 2025
Author(s): Unknown
File name: Global-AI-Policy-V1.pdf

1. AI Usage Boundaries

• Not specified in this policy

2. Ethical & Legal Considerations

• Not specified in this policy

3. Human vs AI Roles

• Not specified in this policy

4. Oversight & Accountability

• Not specified in this policy

5. Data Governance

• Not specified in this policy

6. Risk Management

• Not specified in this policy

7. Transparency & Explainability

• Not specified in this policy

8. Training & Awareness

• Not specified in this policy

9. Enforcement

• Not specified in this policy

10. Other Considerations

• Not specified in this policy

Regulatory Citations

• HIPAA / FIPS to encrypt data both at rest
• SOX -controlled data, Company trade secrets, or internal security controls

---

This policy is intended to enable our technical, bus iness, and legal decision-makers to leverage AI

Company: O’Melveny & Myers LLP
Author(s): Heather Meeker, Amit Itai
File name: example_ai_policy.pdf

Summary

This AI policy outlines guidelines for implementing and deploying AI tools while emphasizing ethical considerations, legal compliance, and risk mitigation, with a focus on bias prevention and diversity.

1. AI Usage Boundaries

• AI should improve products and processes while avoiding biases and discrimination.
• Clear objectives must be defined for AI tools, including data sources.

2. Ethical & Legal Considerations

• Avoid replicating human biases in AI tools.
• Ensure compliance with internal AI standards regarding bias prevention.

3. Human vs AI Roles

• Implement 'Human-in-the-loop' for AI hiring tools.
• Human review and intervention are necessary in AI decision-making.

4. Oversight & Accountability

• Establish a diversity team to examine AI development and data.
• Regular audits of AI input and output data are required.

5. Data Governance

• Increase transparency regarding data and AI use.
• Document key decision-making processes in AI development.

6. Risk Management

• Evaluate development processes and system outputs of AI tools.
• Track AI models and their applications for compliance and accountability.

7. Transparency & Explainability

• Develop AI tools that enhance traceability and explainability of decisions.
• Provide real-time insights into AI decision-making processes.

8. Training & Awareness

• Conduct training programs on AI biases and diversity for all employees.
• New hires must review AI policy and guidelines.

9. Enforcement

• Compliance with this policy is mandatory for all engineering teams.

• Disagreements with the policy must be addressed with Legal.

10. Other Considerations

• Consider the impact of AI tools on various stakeholders, including minorities.
• Keep track of AI models used and their implementations.

Regulatory Citations

• Not specified in this policy

---

to reshape the global balance of power, spark entirely new industries, and revolutionize the way we live and work. As our global competitors race to exploit these technologies, it is a national security imperative for the United States to achieve and maintain unquestioned and unchallenged global technological dominance. To secure our future, we must harness the full power of American innovation."

Company: Unknown
Author(s): Unknown
File name: Americas-AI-Action-Plan.pdf

1. AI Usage Boundaries

• Not specified in this policy

2. Ethical & Legal Considerations

• Not specified in this policy

3. Human vs AI Roles

• Not specified in this policy

4. Oversight & Accountability

• Not specified in this policy

5. Data Governance

• Not specified in this policy

6. Risk Management

• Not specified in this policy

7. Transparency & Explainability

• Not specified in this policy

8. Training & Awareness

• Not specified in this policy

9. Enforcement

• Not specified in this policy

10. Other Considerations

• Not specified in this policy

Regulatory Citations

• 15 U.S.C. § 4656
• 33 U.S.C. § 1344
• 26 U.S.C. § 132
• 47 U.S.C. § 223

ToeffectuatethemissionandpurposesoftheArizonaDepartmen tofAdminis tration(the“Departmen t”),theDepartmen tshallmaint aina“coordinatedstatewideplanforinformationtechnology ”implemen tedandmaintainedthroughpolicies,and“adoptingstat ewidetechnical,coordinationandsecuritystandards”asauthoriz e dbyArizonaRevisedStatuteA.R.S.§18-104(A)(1)(a).TheDepartme n tshallalso“formulatepolicies,plansandprogramstoeffectuateth egovernmen tinformationtechnologypurposesofthedepartmen t”pursuanttoA.R.S.§18-104(A)(13).

Company: Arizona Department of Administration
Author(s): Unknown
File name: P2000 - Generative AI Policy.pdf

Summary

The Arizona Department of Administration's policy on Generative Artificial Intelligence (GenAI) aims to provide a structured approach to the use of AI technologies in public service, emphasizing compliance with legal standards, data privacy, and the responsible use of AI tools to enhance government operations while maintaining public trust.

1. AI Usage Boundaries

• Generative AI is a tool for public servants, not a substitute for their responsibilities.
• Usage must comply with statewide IT and cybersecurity policies.

2. Ethical & Legal Considerations

• Generative AI must be used in a fair and equitable manner.
• Privacy of individuals must be protected, and personal information should not be collected without consent.

3. Human vs AI Roles

• Public servants remain responsible for the outcomes of AI usage.
• Human operators must review AI outputs for accuracy and appropriateness.

4. Oversight & Accountability

• Budget Unit CIOs must oversee compliance with policies regarding Generative AI.
• Budget Units are accountable for decisions made using Generative AI.

5. Data Governance

• No confidential data should be added to publicly accessible AI services.
• Compliance with records management and privacy laws is mandatory.

6. Risk Management

• Risk assessments must be conducted before deploying Generative AI.
• Budget Units must ensure proper licensure of model training data.

7. Transparency & Explainability

• Budget Units must disclose the use of Generative AI and provide attribution.
• Documentation of AI models and methods used is required for transparency.

8. Training & Awareness

• Mandatory training on Generative AI usage is required for all users.
• Annual training updates must be completed by users.

9. Enforcement

• All Generative AI software must be reviewed for compliance with security and privacy requirements.
• Violations of the policy may lead to disciplinary actions.

10. Other Considerations

• Collaboration with the State CIO and CISO is necessary before deploying Generative AI.
• Legal issues surrounding AI inputs must be evaluated by Budget Units.

Regulatory Citations

• A.R.S. §18-104(A)(13)
• Arizona Policy P8410: System Privacy
• P8110 Data Classification Policy
• A.R.S. §18-104(A)(1)(a)
