Agentiiv AI Adoption, Usage & Deployment Guidelines

1. Introduction

Agentiiv is committed to using Artificial Intelligence (AI) technologies in a responsible and ethical manner. We recognize the potential of AI to enhance our operations and improve the experiences of all ecosystem participants. These guidelines outline our approach to ensuring that AI systems are developed and used in a manner that aligns with our organizational values, meets regulatory requirements, and delivers value to our clients while mitigating potential risks.

2. Scope and Applicability

These guidelines apply to:

- All AI-driven products and services offered by Agentiiv
- All employees, contractors, and partners involved in AI-related activities
- All stages of the AI lifecycle, from conception to retirement
- departments and functions within Agentiiv that utilize AI technologies

3. General Usage Principles

3.1 **AI use cases across all aspects of our business:** We enable teams to adopt generative AI in a variety of ways to accelerate their work, including but not limited to: content generation, code generation, chatbots, workflow automation, automated answers, and product-embedded AI features.

3.2 **Team judgment and established guardrails:** Teams and individuals use their best judgment when evaluating potential adverse effects associated with the adoption of generative technologies. When in doubt, they consult with the legal, risk

& compliance, or IT teams to get detailed guidance.

3.3 **Transparency:** We inform users when and how AI is being used in decision-making and how those decisions might affect them.

3.4 **Accountability:** Agentiiv is ultimately responsible for any and all output generated by our AI systems. Teams have governance and controls over their AI product(s), which includes documenting intended use cases, conducting impact assessments, and ensuring appropriate use.

3.5 **Bias and Fairness:** We take steps to mitigate bias in our systems and ensure that our use of AI is fair and equitable. We monitor our systems and workflows to ensure that we have not inadvertently introduced bias that could result in any group or population being discriminated against.

3.6 **Data Privacy and Security:** All data used in our AI systems is handled in a secure and responsible manner, complying with all relevant data privacy and security regulations.

3.7 **Protection of IP and Confidential Data:** We restrict all data that contains sensitive Agentiiv information from being input into public or open-source generative AI tools without proper vetting and approval.

3.8 **Continuous Monitoring and Improvement:** We continuously monitor our use of AI and evaluate its impact on our operations and clients, using this information to make improvements to our systems and processes.

4. AI Governance Structure

Agentiiv has established an AI Governance Committee comprised of the executive management and company directors. This committee meets quarterly to review AI initiatives, assess risks, and ensure alignment with company values and regulatory requirements.

5. Data Management and Protection

5.1 Data Classification: Agentiiv uses a four-tier data classification system:

- Public Data
- Internal Use Only
- Confidential
- Highly Sensitive

All data used in AI systems is classified according to this system.

5.2 Data Handling Procedures

- We have established procedures for handling data based on its classification level.
- Encryption is implemented for all Confidential and Highly Sensitive data.
- Data governance documentation reflects data that should be treated with additional privacy and/or security measures when inputting that data into an AI tool.
- Experimentation on public data is encouraged. Systems using confidential or highly sensitive data must be vetted by senior leadership.

6. AI Development and Deployment

6.1 Development Lifecycle
Agentiiv follows a standardized AI development lifecycle:

- Planning and Requirements
- Data Preparation and Validation
- Model Development
- Testing and Validation
- Deployment

- Monitoring and Maintenance

6.2 Testing and Validation

- We conduct rigorous testing of AI agents across various scenarios relevant to their domain expertise.
- A formal validation process is implemented before any AI agent is made available to clients.

7. Ethical AI Usage

7.1 Ethical Guidelines

Agentiiv has developed and adheres to a set of ethical AI principles aligned with our company values. All AI development and usage adheres to these principles.

7.2 Bias Detection and Mitigation

- We conduct regular bias audits for all AI systems.
- We develop and maintain diverse training datasets to minimize bias.

8. Human-AI Collaboration

8.1 Transparency

- We clearly disclose the use of AI tools in all service outputs to clients and end-users.
- We maintain detailed records of AI involvement in service delivery.

8.2 Quality Control

- We implement a two-step review process: initial AI-assisted output review followed by human expert review and refinement.
- We regularly assess the quality and accuracy of AI-assisted outputs.

8.3 Roles and Responsibilities

- We have clearly defined the roles of human employees and AI systems in the service delivery process.
- Final decisions and strategic recommendations are always made or approved by qualified human professionals.

9. Content Creation and Generation

9.1 Accountability

Each team member is responsible for all prompts or other inputs to and the usage of all resulting outputs from generative AI for business purposes.

9.2 Assistive Technology

- Generative AI is used as an assistive tool, not an autonomous system.
- Team members remain engaged in all uses of generative AI for Agentiiv's business purposes.

9.3 Data Accuracy

Each team member independently fact-checks and sources all data and information contained in AI-generated output before use.

9.4 Plagiarism Prevention

- Team members are responsible for ensuring the originality of content, including AI-generated content.
- Records of prompts and resulting outputs produced by generative AI are kept.

9.5 Copyright and Intellectual Property Compliance

- We have established guidelines to ensure the responsible use of AI-

generated content in Agentiiv business materials.

- Team members are trained to recognize potential copyright issues and seek guidance when necessary.
- All third-party content incorporated into Agentiiv business materials is verified and properly attributed.
- We maintain a process for regular review of our content to ensure ongoing compliance with copyright laws and intellectual property rights.

9.6 Documentation and Record-Keeping

We maintain logs of content generated by AI and the data sources from which it was derived.

10. AI Agent Management and Regulatory Compliance

- We maintain an up-to-date registry of relevant AI regulations in Canada and the US.
- We conduct quarterly compliance reviews of AI systems and processes.
- We have implemented safeguards to ensure AI-generated content complies with applicable industry standards and regulations.

10.1 Version Control

- We have implemented a robust version control system for all AI agents.
- We maintain a detailed changelog for each version of an AI agent.

10.2 Update Process

Our update process includes:

- Testing updates in a sandbox environment
- Gradual rollout to a subset of users
- Monitoring for unexpected behaviors
- Full deployment upon successful testing

10.3 Rollback Procedures

- We maintain the ability to quickly revert to the previous stable version of any AI agent.
- We regularly test rollback procedures to ensure their effectiveness.

11. Risk Management

We regularly assess risks in the following categories:

- Data privacy and security
- Ethical concerns
- Operational issues
- Reputational impacts

12. Transparency and Accountability

Client Communication

- We clearly communicate the capabilities and limitations of AI agents to clients.
- We provide transparency about the use of AI in all products and services.

13. Continuous Improvement

13.1 Performance Monitoring

We continuously monitor AI agent performance and accuracy. We have established and track key performance indicators (KPIs) for each AI system.

13.2 Feedback Integration

- We regularly collect and analyze user feedback.
- We incorporate validated feedback into system improvements.

14. Third-Party Management

14.1 Vendor Assessment

- We assess all AI vendors and third-party tools against Agentiiv's AI ethics and performance standards.
- We conduct annual audits of third-party AI systems used in Agentiiv's operations.

14.2 Contractual Requirements

- We include specific AI governance and ethical use clauses in all vendor contracts.
- We require vendors to comply with these AI Adoption, Usage & Deployment Guidelines.

15. Employee Training and Education

15.1 AI Literacy Program

- All employees complete a basic AI literacy course.
- Employees directly involved in AI development and management complete advanced AI ethics and best practices training.

15.2 Ongoing Education

- We conduct quarterly workshops on AI ethics, best practices, and emerging trends.
- We provide access to online learning resources for continuous AI education.

15.3 Cybersecurity Training

- All employees undergo regular cybersecurity training to ensure they understand the risks associated with AI systems and how to protect

sensitive data.

- This training is updated regularly to address emerging threats and best practices in AI security.

16. Review and Updates

These guidelines are reviewed and updated annually, or more frequently if required, to ensure they remain current with technological advancements and regulatory changes.

17. Appendices

Appendix A: Glossary of AI Terms

Appendix B: AI Ethics Principles

Appendix C: Compliance Checklist

Appendix D: AI Incident Response Plan

Appendix E: AI Use Cases and Tools

Appendix F: Government Policies and Regulations

Appendix G: Data Classification

Appendix A: Glossary of AI Terms

Introduction

This glossary provides definitions for key terms related to Artificial Intelligence (AI) that are relevant to Agentiiv's work and the AI Adoption, Usage & Deployment Guidelines.

Term	Definition
Artificial Intelligence (AI)	The simulation of human intelligence processes by machines, especially computer systems. These processes include learning, reasoning, and self-correction.
Machine Learning (ML)	A subset of AI that provides systems the ability to automatically learn and improve from experience without being explicitly programmed.
Deep Learning	A subset of machine learning based on artificial neural networks with representation learning. It can be supervised, semi-supervised or unsupervised.
Natural Language Processing (NLP)	The branch of AI concerned with giving computers the ability to understand text and spoken words in much the same way human beings can.
Computer Vision	A field of AI that trains computers to interpret and understand the visual world, processing and analyzing digital images or videos.
Generative AI	AI systems that can generate new content, including text, images, audio, and video, based on training data.
Large Language	A type of AI model trained on vast amounts of text data, capable of understanding and generating human-like

Term	Definition
Model (LLM)	text.
Neural Network	A computer system modeled on the human brain and nervous system, used in machine learning applications.
Algorithm	A set of rules or instructions given to an AI, neural network, or other machine to help it learn on its own.
Training Data	The initial data used to teach an AI system, helping it learn patterns and make predictions.
Bias in AI	Systematic errors in AI systems that can result in unfair outcomes, often reflecting societal biases present in training data or algorithm design.
Explainable AI (XAI)	AI systems that make decisions or predictions that can be easily understood by humans.
AI Ethics	The branch of ethics that deals with the moral implications of creating and using AI systems.
Robotic Process Automation (RPA)	The use of AI to automate repetitive, rule-based digital tasks.
Chatbot	An AI program designed to simulate human conversation through text or voice interactions.
Automated Decision System	An AI system that either assists or replaces human decision-making.
Data Mining	The process of discovering patterns in large data sets involving methods at the intersection of machine learning, statistics, and database systems.

Term	Definition
Reinforcement Learning	A type of machine learning where an agent learns to behave in an environment by performing actions and seeing the results.
Transfer Learning	A machine learning method where a model developed for a task is reused as the starting point for a model on a second task.
AI Governance	The framework for managing, monitoring, and regulating AI systems within an organization or society.
AI Agent	An AI system that perceives its environment and takes actions to achieve specific goals.
Supervised Learning	A type of machine learning where the algorithm is trained on a labeled dataset.
Unsupervised Learning	A type of machine learning where the algorithm is trained on unlabeled data.
AI Model	A specific representation of information that an AI system has learned from training data.
AI Lifecycle	The end-to-end process of building an AI system, including planning, data preparation, model building, deployment, and monitoring.

Appendix B: AI Ethics Principles

Introduction

At Agentiiv, we are committed to developing and using AI systems in an ethical and responsible manner. Our AI Ethics Principles guide all aspects of our AI-related activities and decision-making processes.

2.1 Core Principles

Our use of AI is guided by the following core principles:

Principle	Description
Fairness	AI systems should be designed and used in a way that does not discriminate or create unfair bias.
Transparency	We are open about our use of AI and can explain AI-driven decisions.
Accountability	We take responsibility for the outcomes of our AI systems.
Privacy	We protect individual privacy and adhere to data protection regulations.
Human-centric	AI systems support and enhance human work, not replace it.

2.2 Expanded Ethical Framework

Building upon our core principles, we adhere to the following expanded ethical framework:

1. Fairness and Non-Discrimination

- We strive to ensure our AI systems treat all individuals and groups fairly and without discrimination.
- We actively work to identify and mitigate biases in our AI models and datasets.
- We regularly audit our AI systems for fairness across different demographic groups.

2. Transparency and Explainability

- We are committed to being transparent about when and how we use AI in our products and services.
- We strive to make our AI systems as explainable as possible, especially in high- stakes decision-making contexts.
- We provide clear information about the capabilities and limitations of our AI systems to our clients and users.

3. Accountability

- We take responsibility for the decisions and actions of our AI systems.
- We establish clear lines of accountability within our organization for AI-related decisions.
- We are committed to addressing and rectifying any unintended negative consequences of our AI systems.

4. Privacy and Data Protection

- We respect and protect individual privacy in all our AI applications.
- We adhere to data protection regulations and best practices in data collection, storage, and processing.
- We implement strong safeguards to prevent unauthorized access or misuse of personal data.

5. Human-Centric Approach

- We design and deploy AI systems with the primary goal of benefiting humanity.
- Human oversight and decision-making remain central in critical processes.
- We prioritize human well-being and rights in all AI applications.

6. Security and Safety

- We prioritize the security and safety of our AI systems to prevent harm to individuals or society.
- We implement robust security measures to protect our AI systems from external threats and vulnerabilities.
- We conduct thorough safety testing before deploying any AI system.

7. Scientific Excellence and Integrity

- We base our AI development on sound scientific principles and rigorous research.
- We are committed to continuous learning and improvement in our AI practices.
- We promote a culture of intellectual honesty and open discussion about the challenges and limitations of AI.

8. Environmental Responsibility

- We consider the environmental impact of our AI systems and strive to minimize their carbon footprint.
- We explore and implement energy-efficient AI technologies and practices.

9. Collaboration and Shared Benefit

- We engage with the broader AI community to share knowledge and best practices.
- We seek to develop AI solutions that provide widespread societal benefits.
- We collaborate with stakeholders to address ethical challenges in AI.

10. Respect for Human Rights

- We ensure our AI systems respect and uphold fundamental human rights.
- We do not develop or deploy AI for purposes that violate internationally recognized human rights.

11. Ethical Use

- We prohibit the use of our AI systems for illegal, harmful, or deceptive purposes.
- We actively consider and mitigate potential dual-use risks of our AI technologies.

12. Continuous Ethical Assessment

- We regularly review and update these ethical principles to reflect evolving AI technologies and societal norms.
- We conduct ongoing ethical assessments of our AI projects throughout their lifecycle.

Conclusion

By adhering to these principles, Agentiiv aims to develop and deploy AI systems that are not only technologically advanced but also ethically sound and socially beneficial. These principles guide our decision-making processes and help ensure that our AI initiatives align with our core values and societal expectations.

Last Updated: August 1, 2024
Approved by: Karla Congson, CTO

Appendix C1:

AI Compliance Checklist for Contractors

Introduction

This checklist is designed to help Agentiiv service business employees ensure compliance with our AI Adoption, Usage & Deployment Guidelines when using AI tools in their work.

1. General Compliance

[ ] I have read and understood the Agentiiv AI Adoption, Usage & Deployment Guidelines

[ ] I have completed the required AI literacy training

[ ] I am aware of who to contact if I have questions or concerns about AI usage

2. Ethical AI Usage

[ ] I understand and adhere to Agentiiv's AI Ethics Principles in my work

[ ] I consider potential biases when using AI-generated content or insights

3. Data Protection

[ ] I only use approved AI tools for client or sensitive data

[ ] I do not input confidential or sensitive data into public AI tools

[ ] I classify data appropriately before using it with AI tools

4. Content Creation and Generation

[ ] I understand that I am responsible for all prompts and outputs from generative AI

[ ] I independently fact-check and source all AI-generated content before use

[ ] I ensure the originality of content and avoid plagiarism

[ ] I follow copyright and intellectual property compliance guidelines

[ ] I maintain logs of AI-generated content used in client deliverables

5. Human-AI Collaboration

[ ] I clearly disclose the use of AI tools in all service outputs to clients

[ ] I implement the required two-step review process: AI-assisted output review followed by human expert review

[ ] I understand that final decisions and recommendations must be approved by qualified human professionals

6. Client Communication

[ ] I clearly communicate to clients when and how AI is being used in our services

[ ] I am transparent about the capabilities and limitations of the AI tools we use

7. Continuous Improvement

[ ] I provide feedback on AI tool performance to help improve our systems

[ ] I stay updated on the latest AI-related training and guidelines provided by Agentiiv

8. Incident Reporting

[ ] I know how to report any issues or concerns related to AI usage

[ ] I am aware of the escalation process for AI-related incidents

Conclusion

By completing this checklist, you are ensuring that your AI-related work aligns with Agentiiv's guidelines and ethical standards for service business employees. If you are unable to check any of these boxes, please consult with your supervisor before proceeding.

Date: _____

Name: _____

Signature: _____

Appendix C2:

AI Compliance Checklist for Enterprise- Level AI Governance

Introduction

This checklist is designed for Agentiiv's AI Governance Committee and leadership to ensure company-wide compliance with our AI Adoption, Usage & Deployment Guidelines.

1. Governance and Policy

[ ] AI Governance Committee is established and meets quarterly

[ ] AI Adoption, Usage & Deployment Guidelines are up-to-date

[ ] AI Ethics Principles are clearly defined and communicated

2. Risk Management

[ ] Comprehensive AI risk assessment is conducted regularly

[ ] Risk mitigation strategies are in place and documented

[ ] Incident response plan for AI-related issues is established

3. Data Management and Protection

[ ] Data classification system is implemented and enforced

[ ] Data handling procedures for AI systems are established

[ ] Compliance with relevant data privacy regulations is ensured

4. AI Development and Deployment

[ ] Standardized AI development lifecycle is established

[ ] Rigorous testing and validation processes are in place

[ ] Formal approval process for AI system deployment is implemented

5. Ethical AI Assurance

[ ] Regular bias audits of AI systems are conducted

[ ] Diverse and representative training datasets are used

[ ] Ethical impact assessments are performed for new AI initiatives

6. Transparency and Accountability

[ ] Clear communication about AI usage to clients and stakeholders is ensured

[ ] Accountability framework for AI-related decisions is established

7. Third-Party Management

[ ] Assessment criteria for AI vendors and tools are established

[ ] Contracts with AI vendors include governance and ethical use clauses

[ ] Regular audits of third-party AI systems are conducted

8. Employee Training and Awareness

[ ] AI literacy program for all employees is implemented

[ ] Specialized training for AI developers and managers is provided

[ ] Regular updates on AI ethics and best practices are communicated

9. Continuous Improvement

[ ] KPIs for AI system performance are established and tracked

[ ] Feedback mechanism from users and clients is implemented

[ ] Regular reviews of AI guidelines and practices are conducted

10. Regulatory Compliance

[ ] Registry of relevant AI regulations is maintained

[ ] Quarterly compliance reviews of AI systems are conducted

[ ] Processes to adapt to new AI regulations are in place

11. Environmental Responsibility

[ ] Environmental impact of AI systems is assessed

[ ] Initiatives to minimize AI carbon footprint are implemented

12. Documentation and Reporting

[ ] Comprehensive documentation of AI systems and processes is maintained

[ ] Regular reporting on AI compliance to board and stakeholders is conducted

Conclusion

This checklist ensures that Agentiiv's enterprise-level AI governance aligns with our guidelines and ethical standards. The AI Governance Committee should review this checklist regularly and address any areas of non-compliance.

Last Updated: August 1, 2024

Approved by: Karla Congson, CTO

Appendix D: AI Incident Response Plan

1. Purpose

This AI Incident Response Plan outlines the steps to be taken in the event of an AI-related incident or ethical breach at Agentiiv. It is designed to ensure a swift, coordinated, and effective response to minimize potential harm and maintain trust with our stakeholders.

2. Scope

This plan covers all AI-related incidents, including but not limited to:

- Ethical breaches
- Data privacy violations
- Algorithmic bias incidents
- AI system malfunctions
- Unauthorized access to AI systems
- Misuse of AI tools by employees or clients

3. Incident Response Process

5 Detection and Reporting
5 Assessment and Classification
5 Containment
5 Investigation
5 Mitigation and Resolution
5 Recovery
5 Post-Incident Review

4.1 Detection and Reporting

- Any employee who suspects or discovers an AI-related incident must immediately report it to their supervisor and the AI Incident Response Team.
- Reports can be made via email to karla@agentiiv.com

4.2 Assessment and Classification

The AI Incident Response Team will:

a) Assess the severity of the incident using the following scale:

Level 1: Minor incident with minimal impact
Level 2: Moderate incident with potential for limited harm
Level 3: Serious incident with significant potential for harm
Level 4: Critical incident with severe consequences

b) Classify the type of incident (e.g., ethical breach, data privacy violation, etc.)

4.3 Containment

- Implement immediate measures to contain the incident and prevent further harm.
- This may include temporarily disabling affected AI systems, revoking access, or halting related processes.

4.4 Investigation

- Conduct a thorough investigation to determine the root cause of the incident.
- Document all findings, including timeline, affected systems, and potential impact.

4.5 Mitigation and Resolution

- Develop and implement a plan to resolve the incident and mitigate its effects.
- This may involve system fixes, policy changes, or additional safeguards.
- Internal Communication: Keep relevant employees informed about the incident and response efforts.
- External Communication: If necessary, prepare statements for clients, partners, or the public, in consultation with Legal and Communications teams.

4.7 Recovery

- Restore affected systems and processes to normal operations.
- Implement any necessary changes or improvements identified during the incident response.

4.8 Post-Incident Review

- Conduct a detailed review of the incident and response efforts.
- Identify lessons learned and areas for improvement in AI systems, policies, or procedures.
- Update the AI Incident Response Plan and related documents as needed.

4. Specific Response Protocols

Ethical Breaches
Data Privacy Violations
Algorithmic Bias Incidents
AI System Malfunctions
Unauthorized Access

5.1 Ethical Breaches

- Immediately cease the operation of the AI system in question.
- Conduct an ethical audit to identify the nature and extent of the breach.
- Develop and implement corrective measures to align the system with Agentiiv's AI Ethics Principles.

5.2 Data Privacy Violations

- Identify the scope of the data breach and the individuals affected.
- Notify relevant authorities and affected individuals as required by law.
- Implement measures to prevent future breaches and enhance data protection.

5.3 Algorithmic Bias Incidents

Suspend the use of the affected AI system or component.

- Analyze the system for sources of bias and develop a plan to mitigate them.
- Retrain the system using more diverse and representative data sets.

5.4 AI System Malfunctions

- Take the malfunctioning system offline immediately.
- Conduct a thorough technical analysis to identify the cause of the malfunction.
- Develop and test a fix before redeploying the system.

5.5 Unauthorized Access

- Revoke all access to the affected systems immediately.
- Conduct a security audit to identify how the breach occurred.
- Implement additional security measures to prevent future unauthorized access.

5. Training and Preparedness

- All employees will receive training on this AI Incident Response Plan annually.
- The AI Incident Response Team will conduct simulation exercises at least twice a year to ensure readiness.

6. Plan Maintenance

This AI Incident Response Plan will be reviewed and updated annually, or more frequently if significant changes occur in our AI systems or the regulatory environment.

Last Updated: August 1, 2024
Approved by: Karla Congson, CTO

Appendix E: AI Use Cases and Tools

Introduction

This appendix outlines the approved AI use cases and tools at Agentiiv, along with associated risks and guardrails. This list is subject to regular review and updates by the AI Governance Committee.

Category	Potential Use Cases	Approved Tools	Guardrails
AI Agents	• Domain-specific expertise • Answering complex queries • Assisting with research and analysis	Agentiiv	Guardrails: • Regular audits of AI agent outputs • Clear communication of AI agent limitations to users • Strict data handling and privacy protocols • Mandatory human review for critical decisions
Content Generation	• Creating marketing materials • Drafting reports • Generating blog posts • Creating images and videos • Generating audio content	Runway ML Midjourney Dall E HeyGen Eleven Labs Play HT Agentiiv	Guardrails: • Limit AI-generated content to 50% of final output • Mandatory human review and fact-checking • Use of plagiarism detection tools • Regular audits of AI-generated content • Clear guidelines on copyright and fair use
Code Generation	• Accelerating software development • Automating routine coding tasks	GitHub Copilot Cursor	Guardrails: • Mandatory code review by senior developers • Use in non-critical components only • Regular security audits of AI-generated code
Process Automation	• Workflow optimization • Document processing • Task automation across platforms	Zapier Make	Guardrails: • Thorough testing before deployment • Regular audits of automated processes • Strict access controls and data handling protocols • Periodic review of automation efficiency

Plagiarism and Fact Check	• Verifying content originality • Fact-checking AI-generated content	Originality AI	Guardrails: • Use as a supplementary tool, not a replacement for human judgment • Regular updates to the tool's database • Cross-verification with other sources for critical conte

Note

The use of AI tools for any purpose not listed in this appendix must be approved by the AI Governance Committee prior to implementation.

Guidelines for Using AI ToolsAlways verify the output of AI tools before using it in any client-facing or critical internal work.

1. Be aware of the limitations and potential biases of the AI tools you are using.
2. Regularly update your knowledge about the AI tools through provided training and documentation.
3. Report any unexpected behavior or potential issues with AI tools to the IT department immediately.
4. Adhere to all data protection and privacy policies when using AI tools, especially when handling sensitive information.
5. Do not use unapproved AI tools or services without explicit permission from the AI Governance Committee.

Review and Update

This appendix will be reviewed and updated quarterly by the AI Governance Committee to ensure it remains current with Agentiiv's AI strategy and technological advancements.

Last Updated: August 1, 2024
Approved by: Karla Congson, CTO

Appendix F: Government Policies and Regulations

Introduction

Policy and regulatory development for the management of generative AI is a rapidly evolving field. Below are links to several key policies that serve as a starting point in understanding current policy and legislation as well as how these policies are expected to evolve. It is the responsibility of teams to understand these policies and legislations when using Generative AI in any client-facing product.

1. Canada

Artificial Intelligence and Data Act (AIDA)

- Includes Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems
- Link: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

CMA's Privacy & Compliance Guide (PIPEDA)

- Link: https://thecma.ca/docs/default-source/cma-public-guides/overview-cma-privacy-compliance-guide.pdf?sfvrsn=2745e0b7_2

CMA's Canadian Marketing Code of Ethics and Standards

- Link: https://thecma.ca/resources/code-of-ethics-standards

2. USA

Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety

- Includes Blueprint for the AI Bill of Rights
- Includes AI Risk Management Framework
- Link: While there isn't a single document, the White House has outlined various actions and principles. For the most up-to-date information, visit: https://www.whitehouse.gov/ostp/ai-bill-of-rights/

3. EU

Regulation on a European Approach for Artificial Intelligence

- Link: https://ec.europa.eu/info/law/law-topic/digital-single-market/enforcement-artificial-intelligence_en

4. International

Organization for Economic Cooperation and Development (OECD) Global Partnership on AI

- Link: https://www.oecd.ai/

Note

This list is not exhaustive, and regulations are subject to change. Agentiiv must regularly review and update its compliance strategies to align with the latest regulatory requirements.

Key Compliance Considerations

1. Data Privacy: Ensure all AI systems comply with relevant data protection laws, including PIPEDA in Canada.
2. Transparency: Clearly communicate when and how AI is being used, especially in client-facing applications.
3. Fairness and Bias: Regularly audit AI systems for potential biases and take steps to mitigate them.
4. Accountability: Establish clear lines of responsibility for AI system outputs and decisions.
5. Security: Implement robust security measures to protect AI systems and associated data.
6. Ethical Use: Adhere to ethical AI principles in all AI development and deployment activities, in line with CMA's Canadian Marketing Code of Ethics and Standards.
7. Marketing Practices: Ensure all AI-driven marketing activities comply with CMA's guidelines and relevant regulations.

Conclusion

It is crucial for all teams working with AI to familiarize themselves with these regulations and guidelines, and to consult with the legal department when implementing AI in new products or services, especially those that are client-facing.

Last Updated: August 1, 2024
Approved by: Karla Congson, CTO

Appendix G: Data Classification

1. Purpose

This data classification system defines categories of data based on their level of sensitivity and the potential impact to Agentiiv should the data be disclosed, altered, or destroyed without authorization. The classification of data will inform baseline security controls for the protection of data, particularly when used in AI systems.

2. Data Classification Levels

Agentiiv uses a four-tier data classification system:

2.1 Level 0: Public Data

Description: Data that Agentiiv has designated as being generally accessible to the public.

Risk: There is no risk of unauthorized disclosure, but issues could arise from unauthorized modifications affecting the authenticity/integrity of the data.

Examples:

- Press releases
- Published reports
- External job postings
- Agentiiv website content
- Open-source software code

2.2 Level 1: Internal Use Only

Description: Data that Agentiiv has not chosen to make public. These data should not be disclosed broadly to the public or to people other than those whom the data owner or steward authorizes/approves.

Risk: Unauthorized disclosure, alteration, or destruction could result in a low-level negative impact to Agentiiv and its stakeholders.

Examples:

- Work-related communications
- Internal processes and procedures
- Non-sensitive business data

2.3 Level 2: Confidential

Description: Data that are confidential in nature and for which access and use are limited to specific individuals.

Risk: Unauthorized disclosure, alteration, or destruction could result in a moderate level of risk to Agentiiv or have an adverse effect on Agentiiv and its stakeholders.

Examples:

- Employee records
- Unpublished research or product information] Client data (non-sensitive)
- Financial data (non-sensitive)

2.4 Level 3: Highly Sensitive

Description: Data that are highly sensitive and confidential. Protection of these data is required by law/regulation and/or confidentiality/data use agreements.

Risk: Unauthorized disclosure, alteration, or destruction could cause a significant level of risk to Agentiiv or have severe adverse effects on its stakeholders.

Examples:

- Personal identifiable information (PII)
- Financial information (e.g., credit card numbers, bank account details)
- Intellectual property
- Client data (sensitive)
- Passwords and encryption keys

3. Data Handling Requirements

The following table outlines the handling requirements for each data classification level:

Risk Level	Storage	Transit	Access
Level 0 (Public)	No special protection required	May be transmitted via unsecured channels	No constraints
Level 1 (Internal)	Standard protection measures	May be transmitted via unsecured channels	Role-based access
Level 2 (Confidential)	Enhanced protection measures	Must be transmitted via secured channels	Controlled access, authorized accounts only
Level 3 (Highly Sensitive)	Strict protection measures, possible encryption	Must be transmitted via secured, encrypted channels	Strictly controlled access, periodic audits required

4. AI-Specific Considerations

- Public Data (Level 0): May be freely used in AI systems, including public or open-source AI tools.
- Internal Data (Level 1): May be used in Agentiiv's internal AI systems but not in public AI tools without approval.
- Confidential Data (Level 2): Use in AI systems must be approved by senior leadership. Not to be used in public AI tools.
- Highly Sensitive Data (Level 3): Use in AI systems requires strict oversight and approval from the AI Governance Committee. Never to be used in public AI tools.

5. Responsibilities

- All employees are responsible for handling data in accordance with its classification level.
- The AI Governance Committee, in collaboration with the Data Steward(s), is responsible for ensuring AI systems adhere to these data classification guidelines.
- Regular audits will be conducted to ensure compliance with this data classification policy.

6. Training

All employees will receive training on this data classification system and its application to AI systems as part of their AI literacy program.

7. Review and Updates

This data classification system will be reviewed annually and updated as necessary to reflect changes in Agentiiv's data landscape and AI capabilities.

Last Updated: August 1, 2024
Approved by: Karla Congson, CTO