

P2016 - AI Governance and Responsible Use Policy

Contents

Purpose:.....	3
Scope:.....	3
Statement:.....	3
Policy Sections:.....	7
.....	7
Policy References:.....	8
Related Procedure References:.....	8
Related Regulatory Information:.....	8

Purpose:

Overview

At Integrity, we're excited to embrace the power of Artificial Intelligence as a tool that helps us work smarter, serve partners better and accelerate our Mission—while staying firmly grounded in our Core Values. This AI Governance and Responsible Use Policy outlines how we can safely and ethically leverage approved AI tools, protect privacy and confidential data, uphold regulatory requirements, and maintain human oversight in all AI-supported work. By using approved AI tools thoughtfully and ethically, we enable smarter solutions, stronger partnerships and a future-ready organization that leads with Integrity in everything we do, all to help more families plan for the good days ahead.

About This Policy

This Policy establishes the approved list of Artificial Intelligence (AI) tools, permitted use cases, alignment with Integrity core values, and mandatory rules governing compliant and ethical use of AI within the organization. Access to AI tools is limited, conditional, and provided for designated business purposes in coordination with the user's manager and relevant business unit, subject to annual re-evaluation.

This Policy may be supplemented or further restricted by business unit, segment or division specific policies

Scope:

This Policy applies to all employees, contractors, and third-party personnel when using Artificial Intelligence on electronic and computing devices whether owned or leased by Integrity, LLC ("Integrity") or otherwise used by such individuals to conduct business on behalf of Integrity. For clarity, to "conduct business on behalf of Integrity" means acting in the name of Integrity or any of its affiliates, or exercising delegated authority to represent, bind, or speak for Integrity or any of its affiliates, and expressly excludes individuals or entities that neither use Integrity's or its affiliates' names nor act under granted authority.

This Scope may be further restricted by business unit, segment or division specific policies or addendums to this policy.

Statement:

Core Values for Responsible AI

All AI use must reflect the following values as follows:

- **Protect Confidentiality**

Minimize the input of confidential, proprietary, trade secret, or sensitive information; avoid PII unless explicitly authorized and safeguarded; prefer anonymized or fictional data for testing.

- **Ensure Accuracy**

Treat AI outputs as drafts; verify facts, watch for hallucinations, and review/edit all AI-generated content prior to sharing or publication.

- **Legal and Regulatory Compliance**

All AI use must comply with applicable federal, state, and industry regulations, including the Centers for Medicare & Medicaid Services (CMS), the Health Insurance Portability and Accountability Act (HIPAA), the California Consumer Privacy Act (CCPA) and related state privacy laws (such as CPRA, VCDPA, CPA, CTDPA, UCPA), as well as insurance-specific standards like NAIC Model Laws and state insurance privacy statutes and wealth-management regulatory requirements, including federal and state securities privacy, suitability, and recordkeeping obligations, and related SEC and FINRA guidance. Users must also adhere to international frameworks where relevant (e.g., GDPR), internal company policies, and industry best practices.

- **Ethical and Transparent Use**

Do not deceive, impersonate, or manipulate; disclose AI-generated content where appropriate; avoid biased, offensive, or discriminatory outputs.

- **Appropriate Business Purpose**

Use AI to enhance productivity in furtherance of the Integrity's mission, values, and strategic goals; do not use AI to bypass responsibilities or create inappropriate content.

- **Accountability**

Users are responsible for how they use AI and for the content it generates.

- **Human-in-the-Loop Oversight**

All AI-generated outputs must be subject to meaningful human review and approval before any external distribution, decision-making, or implementation. Automated actions without human validation are strictly prohibited.

Access, Approval, and Periodic Review

- Access to approved AI tools is granted contingent on acknowledgment of this policy.
- Access to any unapproved AI tool requires submittal to the AI Governance Committee for its review and approval of such use as well as submittal in accordance with **P1512 – Third Party Risk Management Policy**.
- All AI tool use must be consistent with assigned job duties and business unit objectives
- Access is temporary and subject to annual review and renewal at Integrity's discretion.
- By receiving access, users acknowledge they understand scope and limitations, will use access solely for work duties, and will uphold relevant policies and published expectations.
- Misuse or deviation may result in revocation of access and/or further action under organizational policy; continued access depends on ongoing compliance and commitment to ethical and responsible AI practices.

Approved AI Tools, Intended Uses, and Value Alignment

The AI Governance Committee will maintain and regularly update a list of approved AI tools. Use outside the stated purposes requires prior written approval from the AI Governance Committee. All uses must apply the **Core Values for Responsible AI** stated above.

Prohibited Uses

The following uses of AI are prohibited:

- Uses that deceive, impersonate, manipulate, or otherwise mislead stakeholders.
- Generation or dissemination of biased, offensive, or discriminatory content.
- Using AI to bypass assigned responsibilities or to create inappropriate content.
- Any use that violates data protection laws, industry regulations, any contractual relationship Integrity has with a third party or internal compliance policies.

Data Handling and Privacy

- Use anonymized or fictional data for testing or exploration of AI capabilities.
- When handling any data, ensure compliance with GDPR, HIPAA, CCPA, Gramm-Leach-Bliley Act (GLBA), SEC Regulation S-P, and applicable internal policies; if in doubt, consult the Integrity Legal & Compliance Department at compliance@integrity.com.
- Do not upload client, customer, or employee PII (names, addresses, phone numbers) to AI tools unless expressly authorized and approved safeguards are in place.

Quality Assurance and Human Oversight

- Treat all AI outputs as drafts or suggestions, not final content.
- Fact-check and verify all material used for decision-making or external sharing; review and edit before any internal distribution or publication.
- Remain vigilant regarding hallucinations and other accuracy risks.

Transparency and Ethical Communications

- Be transparent when content is AI-generated in client-facing or public communications, using pre-approved disclosure language by the Legal & Compliance department.
- Do not use AI to impersonate individuals or misrepresent authorship or expertise.

Monitoring, Enforcement, and Consequences

- Integrity may monitor AI use for compliance with this Policy and other applicable policies.
- Misuse or deviation may result in immediate revocation of AI access and/or further action consistent with organizational policy.
- Continued access is contingent on ongoing compliance and demonstrated commitment to ethical and responsible AI practices.

Authority and Relationship to Other Policies

Use of AI tools must strictly adhere to all applicable Integrity policies, including but not limited to the Acceptable Use Policy. Users must also comply with applicable data protection laws and industry-specific regulations, as well as internal compliance policies.

Exceptions

Any exception to this Policy requires prior written approval from AI Governance Committee, with documented controls ensuring adherence to the Core Values and legal/regulatory obligations.

Policy Review and Updates

This Policy will be reviewed at least annually and updated as needed to reflect changes in law, technology, and business priorities, including the annual re-evaluation of access.

Terms	Definition
AI Solution	Any AI system, model, or algorithm or any product or service that incorporates an AI system, model, or algorithm as a material component of the product or service.
Artificial Intelligence (“AI”)	A multidisciplinary field of technology focused on developing systems capable of performing functions that ordinarily require human cognitive abilities, including but not limited to perception, reasoning, learning, and language understanding. AI systems may operate through software, hardware, or integrated platforms and are designed to achieve outcomes that approximate or optimize intelligent behavior. For purposes of this policy, AI encompasses, without limitation, the following subfields and techniques: • Machine Learning (ML) – Algorithms that enable systems to learn from data and improve performance over time without explicit programming. • Natural Language Processing (NLP) – Technologies that allow systems to interpret, generate, and respond to human language. • Computer Vision – Methods enabling systems to process and analyze visual information. • Neural Networks and Deep Learning – Architectures that model complex patterns and relationships in data. • Expert Systems and Robotics – Systems designed to replicate specialized decision-making or physical tasks.

- | | |
|--|--|
| | <ul style="list-style-type: none">• Generative AI – A subset of machine learning focused on creating new content, including text, images, audio, or other media. |
|--|--|

This definition applies to all organizational uses of AI, including development, procurement, deployment, and governance.

Policy Sections:

Policy References:

Policy Status	Document Name	Category	Document Author	Document Owner	Document Version Number	Last Published Date
 Awaiting Document Owner Approval	P2000 - Acceptable Use Policy	2000 - Information Technology	Matt Williams	Matt Williams	2.0	4/8/2025
 Awaiting Document Owner Approval	P2005 - Data Protection and Lifecycle Policy	2000 - Information Technology	Matt Williams	Matt Williams	2.0	4/8/2025
 Awaiting Document Owner Approval	P2008 - Information Security Policy	2000 - Information Technology	Matt Williams	Matt Williams	2.0	4/8/2025
 Awaiting Document Owner Approval	P2003 - Business Continuity and Disaster Recovery Policy	2000 - Information Technology	Matt Williams	Matt Williams	2.0	4/8/2025

Related Procedure References:

Related Regulatory Information:

P2016 - AI Governance and Responsible Use Policy

Document Author	Name: Title: Email:	Sumit Dhawan Manager Cybersecurity Compliance Sumit.Dhawan@integrity.com
Document Owner	Name: Title: Email: Approved Date:	Matt Williams Senior Director Cybersecurity & Cloud Engineering CISO matthew.williams@integrity.com 2/24/2026
Legal Management Approval	Name: Title: Email: Approved Date:	Duncan McQueen Assistant General Counsel Duncan.McQueen@integrity.com 3/4/2026
Executive Management Approval	Name: Title: Email: Approved Date:	Harsh Singla Chief Product and Technology Officer Harsh.Singla@integrity.com 3/30/2026

Last Published Date: 3/30/2026

Document Version Number 5.0