AI & Data Integrity Policy

Purpose

Artificial Intelligence (AI) technologies can improve efficiency, productivity, communication, research, and decision-making. At the same time, AI introduces risks related to privacy, cybersecurity, intellectual property, accuracy, and data protection.

The purpose of this policy is to establish clear expectations for the responsible use of AI while protecting company information, customer information, and business operations.

This policy applies to all employees, contractors, consultants, temporary personnel, interns, and any third party authorized to access company systems or information.

Approved Business Use of AI

Employees may use approved AI tools to assist with:

- Research and information gathering
- Drafting emails and communications
- Creating presentations and reports
- Brainstorming ideas and content
- Data analysis and summarization
- Administrative tasks
- Software development assistance
- Customer service support

AI may be used as a productivity tool but shall not replace human judgment, professional expertise, or management oversight.

Protection of Company Information

Company information is a valuable business asset.

Employees shall not enter, upload, share, or disclose the following information into public or unauthorized AI systems:

- Confidential business information

- Customer information
- Employee personal information
- Financial records
- Proprietary business processes
- Trade secrets
- Internal policies and procedures
- Legal documents
- Contract information
- Security controls or configurations
- Passwords, credentials, or access codes
- Non-public intellectual property

When in doubt, information should be treated as confidential and should not be shared with an AI system.

Personal AI Accounts

Employees may not use personal AI accounts for company business unless specifically authorized by management.

Where AI tools are approved for business use, employees should use company-authorized accounts whenever available.

Data Integrity Requirements

Information generated by AI may contain inaccuracies, omissions, outdated information, or fabricated content.

Before relying upon AI-generated information, employees must:

- Review all outputs for accuracy
- Verify facts and data
- Confirm calculations and figures

- Review citations and references
- Validate recommendations
- Apply independent professional judgment

AI-generated content shall not be considered final without human review.

Employees remain responsible for the accuracy and quality of their work regardless of whether AI was used.

Intellectual Property Protection

Employees shall not use AI systems in a manner that may expose, disclose, or compromise company intellectual property.

Protected information includes:

- Proprietary methodologies
- Internal business processes
- Product designs
- Strategic plans
- Pricing information
- Source code
- Client materials
- Research and development information

All intellectual property created during the course of employment remains the property of the organization unless otherwise agreed in writing.

Ethical Use of AI

AI shall be used in a lawful, ethical, and professional manner.

Employees shall not use AI to:

- Create fraudulent or deceptive content
- Misrepresent facts

- Violate intellectual property rights
- Discriminate against individuals or groups
- Harass or intimidate others
- Circumvent company policies
- Engage in unlawful activity
- Generate malicious software or harmful code

All applicable laws, regulations, and company policies remain in effect when using AI technologies.

Customer and Third-Party Information

Customer, client, vendor, and third-party information must be handled with the same care and protection as company information.

Employees shall not submit customer or third-party information to an AI system unless:

- The use is authorized by the organization;
- Appropriate safeguards are in place; and
- Such use complies with contractual, legal, and regulatory obligations.

AI-Assisted Decision Making

AI may assist with analysis and recommendations; however, significant business decisions should not be based solely on AI-generated outputs.

Appropriate human review should be applied to decisions involving:

- Financial matters
- Employment decisions
- Customer relationships
- Legal matters
- Regulatory compliance
- Security controls

- Business strategy

Human accountability remains required for all final decisions.

Security Requirements

Employees must immediately report any suspected:

- Unauthorized AI use
- Data leakage
- Security incident
- Privacy concern
- Exposure of confidential information
- AI-related cybersecurity issue

Reports should be made to management, information technology personnel, or the designated compliance contact as soon as practical.

Training and Awareness

Employees using AI technologies are expected to remain informed regarding:

- Safe AI practices
- Data protection requirements
- Cybersecurity responsibilities
- Privacy obligations
- Company policies

Additional training may be required based on job responsibilities.

Violations

Failure to comply with this policy may result in:

- Removal of system access

- Corrective action
- Disciplinary action
- Contract termination
- Legal action where appropriate

The organization reserves the right to monitor and review the use of company systems and approved AI technologies for compliance purposes.

Policy Review

This policy should be reviewed periodically and updated as technology, regulatory requirements, and business needs evolve.

Employee Acknowledgment

I acknowledge that I have received, read, and understand the AI & Data Integrity Policy.

I agree to comply with the requirements contained in this policy and understand that failure to do so may result in disciplinary action.

Employee Name: _____

Signature: _____

Date: _____

Optional Industry-Specific Enhancement

This policy is designed as a general-purpose AI & Data Integrity Policy suitable for many organizations and industries.

Organizations operating in highly specialized, or industry-specific environments may benefit from supplemental language addressing their unique operational, regulatory, contractual, privacy, cybersecurity, or professional obligations.

Industry-specific addendums may be available for sectors including:

- Professional Services
- Healthcare
- Education
- Financial Services
- Insurance
- Manufacturing
- Construction
- Retail & Hospitality
- Technology
- Nonprofit Organizations
- Municipal and Government Organizations

Organizations seeking a more tailored policy may also elect to obtain a customized version incorporating company-specific terminology, operational requirements, contact information, responsibilities, and industry considerations.

Need a More Tailored Policy?

The standard AI & Data Integrity Policy is designed to work for most organizations.

For businesses operating in regulated or specialized industries, VigilantMIND also offers:

Industry-Specific Addendums (+$30) for exact terms contact consult@vigilantmindai.com

Enhance your policy with industry-focused language addressing common operational, privacy, security, and compliance considerations.

Customized Policy Package (+$100) for exact terms contact consult@vigilantmindai.com

Includes your company name, branding, designated contacts, responsibilities, effective dates, and tailored policy language aligned with your organization's operations.

Most organizations choose the Industry-Specific or Customized version to create a policy that better reflects their business and demonstrates a stronger commitment to responsible AI use.

==========