i2e ARTIFICIAL INTELLIGENCE (AI) USAGE POLICY 2025

CONTENTS

info@i2econsulting.com

CIN - U74140MH2008PTC187484

www.i2econsulting.com

91 Springboard Business Hub, Plot. No. D-5, Road. No. 20, Marol MIDC, Andheri East, Mumbai- 400093, Maharashtra.

1. SCOPE

The policy is applicable to:

- All the employees, contractors, third-party vendors, and partners of i2e Consulting.
- All AI systems, tools, APIs, and platforms (including generative AI).
- AI usage in development, testing, deployment, and operational environments.

2. PURPOSE

This policy provides direction for the purposeful and responsible use of Artificial Intelligence (AI) technologies to foster client trust and ensure the ethical, transparent, and accountable implementation of this technology. This policy applies to i2e Consulting Pvt Ltd's employees, contractors, subrecipients, and others who utilise AI technologies in the course of their work on behalf of i2e Consulting Pvt Ltd.

All employees are expected to interact with generative AI technologies, such as ChatGPT, in a responsible and ethical manner. This encompasses safeguarding privacy and personal data, using the technology for lawful and beneficial purposes, abstaining from deceptive or harmful applications, and fostering transparency regarding the technology's capabilities and constraints.

3. POLICY OBJECTIVES:

- Ensure that AI systems protect the confidentiality, integrity, and availability (CIA) of information assets.
- Mitigate risks associated with AI-based decision-making, automation, and content generation.
- Provide a governance framework for lifecycle management of AI technologies.
- Enabling compliance with relevant laws, standards, and industry best practices.

info@i2econsulting.com

CIN - U74140MH2008PTC187484

www.i2econsulting.com

91 Springboard Business Hub, Plot. No. D-5, Road. No. 20, Marol MIDC, Andheri East, Mumbai- 400093, Maharashtra.

4. INTRODUCTION:

This AI Usage Policy provides guidelines for the use of AI tools by i2e employees. This policy serves to enable employees to harness the full potential of AI in their roles, improve the company's operations, and promote a culture of AI literacy and safety. This policy seeks to ensure the security of our company's and customer's data and foster a secure, professional, and respectful environment for all users.

AI tools may be useful but are not a substitute for human judgment and creativity. This policy applies to the use of any third-party or publicly available AI tools, including those embedded in business applications that mimic human intelligence to generate answers or work products or perform certain tasks. AI tools may provide false answers, outdated information, or biased responses. AI-generated content must be reviewed for accuracy, appropriateness and bias.

i. Ethical Use of Artificial Intelligence (AI) Technologies:

i2e consulting is committed to the ethical and responsible use of Artificial Intelligence (AI) in alignment with our organizational values, policies, and overarching commitment to equity, inclusion, transparency, and accountability.

ii. Alignment with Organizational Values and Ethical Standards

All AI applications and outputs must reflect i2e consulting's core values and ethical standards. Users are expected to conduct themselves in a manner that maintains public trust, supports inclusive practices, and upholds respect for human dignity. Under no circumstances should AI be used in ways that contradict the organization's code of conduct, diversity and inclusion commitments, or community-facing responsibilities.

iii. Respect for Privacy and Data Protection

Users must ensure that the deployment and use of AI systems respects individual privacy rights and comply with applicable data protection regulations. AI should not be used to collect, analyze, or infer sensitive personal information without appropriate legal and organizational authorization. Anonymization or de-identification practices should be employed where applicable to minimize privacy risks.

iv. Prevention of Bias, Discrimination, and Harm

The use of AI systems must actively seek to identify, mitigate, and eliminate algorithmic or data-driven bias that could result in discriminatory or inequitable outcomes. AI tools must not be used to produce or support content that is:

- Inflammatory, derogatory, or offensive in nature;
- Discriminatory against any individual or group based on race, ethnicity, gender, sexual orientation, disability, age, religion, or other protected characteristics;
- Harmful to the physical, mental, or emotional well-being of individuals;
- Misleading or manipulative in a way that undermines trust in the organization or in AI-driven decisions.

info@i2econsulting.com

CIN - U74140MH2008PTC187484

www.i2econsulting.com

91 Springboard Business Hub, Plot. No. D-5, Road. No. 20, Marol MIDC, Andheri East, Mumbai- 400093, Maharashtra.

v. Fairness and Transparency in Outputs and Decisions

Employees must strive for fairness, clarity, and transparency in the use of AI, especially when it is used to assist or inform decision-making processes. Any recommendations or outputs produced by AI systems should be clearly distinguished from those authored solely by humans and should be subject to review, validation, and, when appropriate, revision.

info@i2econsulting.com

CIN - U74140MH2008PTC187484

www.i2econsulting.com

91 Springboard Business Hub, Plot. No. D-5, Road. No. 20, Marol MIDC, Andheri East, Mumbai- 400093, Maharashtra.

5. DEFINITIONS:

i. **Artificial Intelligence:**
Artificial Intelligence, or AI, refers to the ability of computer systems or software to perform tasks that usually require human intelligence. These tasks can include understanding language, recognizing patterns, learning from experience, solving problems, and making decisions.

ii. **GenAI:**
Generative AI refers to a type of artificial intelligence that can create new content, such as text, images, audio, video, or code, based on patterns learnt from existing data. These systems are designed to generate outputs that resemble human-created work and can be used for tasks like writing emails, producing reports, creating designs, or summarizing large documents.

iii. **Machine Learning:**
Machine Learning (ML) is a branch of artificial intelligence that enables computer systems to learn from data and improve their performance over time without being explicitly programmed for every task.

iv. **Large Language Models:**
Large Language Models (LLMs) are a type of artificial intelligence designed to understand, interpret, and generate human language. They are trained in vast amounts of text data and use advanced algorithms to predict and produce language-based outputs, such as answering questions, writing documents, summarizing information, or translating languages.

v. **Natural Language Processing:**
Natural Language Processing (NLP) is a field of artificial intelligence that enables computers to understand, interpret, and respond to human language in a meaningful way. NLP allows machines to read, analyze, and generate text or speech just as humans do.

info@i2econsulting.com

CIN - U74140MH2008PTC187484

www.i2econsulting.com

91 Springboard Business Hub, Plot. No. D-5, Road. No. 20, Marol MIDC, Andheri East, Mumbai- 400093, Maharashtra.

6. THREATS RELATED TO AI TOOL USAGE:

i. Unauthorized Use Leading to Data Leakage

Use of AI tools without appropriate authorization or oversight increases the risk that sensitive or proprietary information could be shared externally or within unsecured internal environments. Employees may unintentionally expose critical data by inputting it into third-party AI services without proper clearance or understanding of data privacy implications.

ii. Malicious Content in AI-Generated Outputs

AI-generated content may inadvertently contain hidden malware links, unsafe code snippets, or sensitive information embedded within seemingly harmless outputs. Distributing or implementing such content without proper review can expose systems to security threats or compliance violations.

iii. Accidental Exposure of Confidential Data

Misconfiguration or careless use of AI tools causes unintended data leaks. Exposure of proprietary or personal information may violate privacy laws and contracts, result in regulatory fines, and damage client relationships. It can also provide competitors with sensitive insights, weakening the organization's competitive position.

iv. AI-Driven Phishing and Deepfake Attacks:

Cybercriminals use AI to generate realistic phishing emails or deepfake content that deceives employees. Successful attacks can result in theft of credentials, unauthorized financial transactions, or disclosure of confidential data. They can also undermine trust within and outside the organization, leading to brand damage and loss of stakeholder confidence.

info@i2econsulting.com

CIN - U74140MH2008PTC187484

www.i2econsulting.com

91 Springboard Business Hub, Plot. No. D-5, Road. No. 20, Marol MIDC, Andheri East, Mumbai- 400093, Maharashtra.

7. GUIDELINES & RISKS:

i. ACCEPTABLE USE OF AI TOOLS:

Employees are encouraged thoughtfully to use AI Tools to support their work, enhance creativity, and improve productivity. These tools can be especially helpful in a variety of tasks, including but not limited to:

- **Brainstorming and Idea Generation:**
  Use AI Tools to explore new concepts, gather inspiration, or generate ideas related to ongoing projects, campaign planning, or problem-solving.
- **Creating Formulas or Automation Support:**
  AI Tools can assist in building or refining formulas for Excel, Google Sheets, or other spreadsheets and data tools, helping streamline your workflow.
- **Drafting Basic Content:**
  Use AI Tools to help draft initial versions of emails, letters, memos, or general communication, keeping in mind that human review and editing are always required before sending.
- **Summarizing Information and Outlining Projects:**
  AI tools can summarize research, articles, or lengthy content and help create structured outlines for reports, blog posts, presentations, or other deliverables. This can support broader understanding and full topic coverage.
- **Research Support:**
  AI Tools can be a starting point for gathering content or background information for reports, presentations, or documentation. However, it is essential to verify all AI-generated data or claims through credible and trusted sources. AI output should never be used “as-is” for official purposes.

Important: Pre-Use Approval Required

Before using any AI tool for work purposes, employees must **contact the InfoSec Department** at infosec@i2econsulting.com to request approval. This step ensures that:

- The tool meets the organization's security and compliance standards
- There is no risk of exposing company or client data to untrusted or malicious AI systems
- Proper usage guidelines and training can be provided, if necessary

info@i2econsulting.com

CIN - U74140MH2008PTC187484

www.i2econsulting.com

91 Springboard Business Hub, Plot. No. D-5, Road. No. 20, Marol MIDC, Andheri East, Mumbai- 400093, Maharashtra.

ii. UNACCEPTABLE USE OF AI TOOLS:

Use of AI technologies may not include specific i2e Consulting information including company name, confidential or sensitive information or data, intellectual property and brand. Employees are also prohibited from representing work generated by AI tools as their own original work. Examples of unacceptable use of AI include, but are not limited to:

- **Company Identification or Branding:**
  Employees may not enter or reference the organization's official name—**i2e Consulting Pvt. Ltd.** or any related branding elements in AI tools or platforms.

- **Confidential or Personally Identifiable Information (PII):**
  Employees must not disclose or use any form of PII, including but not limited to:

  Full names, contact information, addresses, or social security numbers of staff, clients, or partners.

- **Passwords, Login Credentials, or System Access Information:**
  Passwords, security tokens, internal system links, and any other authentication credentials are not to be stored, entered, or processed through AI tools.

- **Protected Health Information (PHI):**
  Any medical or health-related information, including patient data, insurance details, or treatment history, is strictly prohibited from being input into AI systems.

- **Personnel and Human Resources Information:**
  AI tools must not be used to process or generate content related to personnel matters, including performance evaluations, Disciplinary actions, Recruitment materials or candidate assessments, Compensation or employment records.

- **Content from Confidential or Proprietary Documents:**
  Information from documents marked as **"confidential," "sensitive," "internal use only," or "proprietary"** must not be entered into or used to generate content through AI tools.

- **Non-Public Company Information:**
  This includes, but is not limited to:
  - Strategic plans and internal goals
  - Business processes or project documentation
  - Internal communication and workplace culture insights
  - Any unpublished materials or information not intended for public distribution.

- **Sharing of Customer data.**

AI tools must not be used on customer data to maintain privacy. This helps prevent unauthorized access and protects sensitive customer information.

info@i2econsulting.com
CIN - U74140MH2008PTC187484
www.i2econsulting.com
91 Springboard Business Hub, Plot. No. D-5, Road. No. 20, Marol MIDC, Andheri East, Mumbai- 400093, Maharashtra.

8. NON- COMPLIANCE:

Compliance with this AI Usage Policy is mandatory for all employees, contractors, and affiliated personnel. AI Tools will be monitored by Cybersecurity Team Continuously and Any deviation from the defined guidelines will be treated as a violation of company policy and may result in strict disciplinary action, up to and including termination of employment, depending on the severity of the breach.

Examples of non-compliance include, but are not limited to:

- Using AI tools to process or transmit confidential, proprietary, or personally identifiable information (PII/PHI) without prior authorization.
- Utilizing unapproved AI platforms or bypassing established review procedures.
- Publishing or presenting AI-generated content as original without proper validation or attribution.
- Repeated disregard for safe usage practices or failure to follow guidance issued by the InfoSec team.

i2e Consulting Pvt. Ltd. reserves the right to:

- Monitor and audit AI tool usage.
- Investigate suspected policy violations.
- Take appropriate action in accordance with HR and security protocols.

It is the responsibility of every employee to ensure that their use of AI tools aligns with this policy. Managers and team leads are expected to reinforce compliance within their teams and escalate concerns to the InfoSec Department via **infosec@i2econsulting.com**.

Review and Updation:

This policy will be reviewed semi-annually by the Cyber Security Department.

Verified By:	**Approved By:**
Shashank Gidbidi	**Srinivasa Kanagala**
Technical Lead – Cyber Security	**CDO**

info@i2econsulting.com

www.i2econsulting.com

91 Springboard Business Hub, Plot. No. D-5, Road. No. 20, Marol MIDC, Andheri East, Mumbai- 400093, Maharashtra.

CIN - U74140MH2008PTC187484