Purpose

ValueMomentum recognizes that while third-party or publicly available tools/applications driven by generative artificial intelligence (AI) technologies, such as chatbots (e.g., ChatGPT, Google's Bard, Microsoft Bing, Microsoft Copilot) and image generators, can drive innovation and improve operational efficiency, they also pose risks related to information security, data privacy, intellectual property, and accuracy.

This document outlines guidelines for the acceptable usage of generative AI technologies to protect ValueMomentum's confidential or sensitive information, trade secrets, intellectual property, and brand. For this document, ValueMomentum's confidential information includes its customer and partner data. Employees are encouraged to responsibly adopt generative AI technology in accordance with this policy.

Scope

This policy applies to all ValueMomentum employees, contractors, and consultants who use any third-party or publicly available generative AI tools/applications, including chatbots (e.g., ChatGPT, Google Bard, Microsoft Bing, Microsoft Copilot) and other tools that mimic human intelligence to generate work products, deliverables, responses, or perform tasks.

Rationale Behind These Guidelines

Generative AI tools are powerful and versatile. However, they have certain limitations that prevent them from fully substituting human intelligence, judgment, or creativity. Following are few key reasons:-

- Generative AI tools process and generate text based on patterns in data, but they do not understand the content in the manner humans do. They lack consciousness and self-awareness.
- Human judgment is influenced by a deep understanding of context, ethics, and emotions, whereas Generative AI tools lack the ability to fully grasp complex human emotions and ethical nuances.
- While Generative AI tools can generate creative content, it does so based on the existing data. Human creativity involves original thought, intuition, and the ability to think out of the box, which Generative AI tools cannot replicate.
- Humans can learn from a wide range of experiences and adapt to new situations in ways that Generative AI tools cannot. Models of Generative AI tools require specific training data and struggle with the tasks outside their training scope.
- Humans can make decisions based on moral and ethical considerations, which are often subjective and complex. Generative AI tools lack the ability to make such nuanced decisions.
- Human interactions are rich with emotional subtleties. Generative AI tools can recognize and respond to emotions, but it cannot truly empathize or understand the depth of human feelings.

Policy Guidelines

Do's

- Generative AI tools are valuable for enhancing productivity and operations, but they are not substitutes for human intelligence, judgment, or creativity.
- Use of generative AI tools must comply with ValueMomentum's policies and legal requirements.
- Employees/contractors/consultants should receive proper training on the responsible use of generative AI tools and understand the consequences of misuse.
- Ensure familiarity with ValueMomentum's Acceptable Usage Policy for generative AI and client data policies to avoid accidental or intentional compromises of sensitive information.
- It is the responsibility of each employee/contractor/consultant to ensure that generative AI tools are used ethically and securely, without compromising confidential information.
- Employees should notify their reporting authority if they use a generative AI tool to assist with a task.
- Since generative AI tools may provide inaccurate or stale information, it is critical to verify outcomes such as work products, deliverables, or responses with human oversight.
- Ensure that the information generated by AI tools is accurate, appropriate, not biased, and compliant with ValueMomentum policies and applicable laws.
- Generative AI tools should only be used for ValueMomentum business purposes, not for personal reasons (e.g., playing games or non-work activities).
- ValueMomentum must implement security controls to protect company and client information when using generative AI tools.
- Only use AI tools authorized by ValueMomentum's IT Security Operations team.
- Generative AI tools should access only approved corporate systems and data repositories, with regulated access to publicly available information on the internet.

Do Not's

- Do not use AI tools to make or assist in employment-related decisions, including recruitment, hiring, performance evaluations, promotions, or terminations due to the following reasons:-

    - Generative AI tools can inadvertently perpetuate or even amplify biases present in the training data. This can lead to unfair treatment of candidates or employees based on gender, race, age, or other protected characteristics.
    - Generative AI decision-making processes can be opaque, making it difficult to understand the rationale behind decisions are made. This lack of transparency can lead to mistrust and challenges in explaining decisions to affected individuals.
    - Assigning responsibility for decisions made by Generative AI tools can be complex. If Generative AI tool makes a flawed decision, it's unclear who is accountable i.e., the employees, or the organization.
    - Employment decisions often involve nuanced ethical judgments that Generative AI tool may not be equipped to handle. Human oversight is crucial to ensure decisions are made with empathy and ethical considerations.
    - Employment laws and regulations require adherence to fair practices and non-discrimination. Ensuring Generative AI tools comply with these laws can be challenging and may expose organization to legal risks.

- Employment decisions impact individual's lives significantly. The human touch in understanding individual circumstances, providing feedback, and making empathetic decisions is irreplaceable by Generative AI tools.

- Do not upload or input any confidential, proprietary, or sensitive ValueMomentum information (e.g., passwords, financial data, personally identifiable information, technical designs, customer application code, customer business specifications) into Generative AI tools due to the following reasons:-

  - Generative AI tools, especially those hosted on external servers, may not have the same level of security as internal systems. This increases the risk of data breaches and unauthorized access to organization.
  - Sensitive information, such as personally identifiable information (PII), must be protected to comply with privacy laws and regulations. Sharing this data with Generative AI tools can lead to violations of these laws for organization.
  - Proprietary information, such as technical designs or application code, is valuable intellectual property of organization. Exposing this data to Generative AI tools can result in intellectual property theft or misuse for organization.
  - Using Generative AI tools without proper safeguards can lead to non-compliance to the applicable data protection regulations / acts along with legal repercussions for organization.
  - When data is input into Generative AI tools, it's often unclear who owns the data and how it might be used. This lack of clarity can lead to misuse or unauthorized sharing of sensitive information of organization.
  - Mishandling sensitive information can damage trust with customers, partners, and employees. Maintaining strict control over confidential data is essential to uphold the organization's reputation.

- Do not use Generative AI tools to generate unauthorized content, manipulate information, or falsify data during client interactions due to the following reasons:-

  - Manipulating or falsifying information breaches ethical standards. Honesty and integrity are fundamental in maintaining trust and credibility with our clients.
  - Creating unauthorized or false content can lead to legal consequences, including breaches of contract, fraud, and violations of copyrights and intellectual property laws.
  - Engaging in deceptive practices can severely damage an organization's reputation in front of our clients.
  - Generative AI tool generated content may not always be accurate. Relying on it for critical client interactions can lead to misinformation, misunderstandings, and poor decision-making.
  - Clients expect transparency and honesty. Using Generative AI tools to manipulate or falsify information undermines this trust and may impact our client relationships.
  - Using Generative AI tools to generate false content may result in non-compliance and hefty penalties on organization.

- Do not claim work generated by AI tools as original work due to the following reasons:-

  - Original work means human creativity and effort, which Generative AI tools lack. Human work carries unique qualities that Generative AI tools cannot fully replicate.

- Generative AI tool based outputs are based on existing data, making them derivative.
- For intellectual property protection, legal frameworks require human creators for originality claims and not Generative AI tool based outputs.
- Misleading others about Generative AI tool involvement is unethical.

- Do not integrate any AI tool with ValueMomentum's internal software without prior written approval from the CISO due to the associated security risks, non-compliance, legal issues, data privacy risks system integrity issues.
- Do not use AI tools that are not on the approved list from IT. Malicious chatbots may attempt to steal or solicit sensitive information.

Violations

Violating this policy, including client data usage policy requirements, may result in disciplinary action up to and including immediate termination. Legal action may also be pursued in cases of severe violations.

Version History

Version #	Author	Nature of Amendment	Date	Reviewed By	Approved By
1.0	P. Umamahesh	Baseline-1	25 Sep 2024	Bharath Iyengar, Lakshmikanth N	Gopikrishna G