



SitusAMC Vendor Acceptable Use Policy for Artificial Intelligence

Global

July 2025

Table of Contents

	Page
1. Purpose and Scope.....	2
2. Definitions.....	2
3. Use of AI Tools	3
3.1 Prohibited and Permitted Uses.....	3
A. Prohibition on Publicly Available AI Tools:	3
B. Prohibition on Certain Uses of Approved AI Tools:.....	3
C. Prohibition on use of Certain Inputs with AI Tools without Prior Approval:.....	4
3.2 Legal and Ethical Responsibilities	4
A. Privacy and Security.....	4
B. Automated Decision-Making.....	5
4. AI Principles and Standards.....	5
5. AI Impact Assessment	7
6. Revision History	7

1. Purpose and Scope

The purpose of this AI Acceptable Use Policy (the “**Policy**”) is to minimize risks and provide guidelines for SitusAMC Vendors (as defined below) to use Artificial Intelligence (as defined below) in a manner that is ethical, responsible, and compliant with applicable laws, regulations, and company policies. This Policy sets forth the acceptable use of Artificial Intelligence technology by Vendors and provides guidelines for using such technology in a responsible way that:

- Aligns with SitusAMC’s overall strategic goals and vendor management practices;
- Complies with current and anticipated laws, regulations, and industry best practices applicable to AI technology;
- Protects the intellectual property rights of SitusAMC;
- Complies with applicable laws and regulations, including privacy and data protection and employment laws and regulations;
- Avoids bias and disparate impacts;
- Minimizes the risks of class-action lawsuits and regulatory enforcement actions; and
- Preserves the trust placed in SitusAMC by its customers and other stakeholders, including the individuals and entities that furnish confidential, proprietary, and/or personal data to SitusAMC.

This Policy covers all SitusAMC vendors, contractors, external consultants, temporaries, and third parties providing products or services to SitusAMC (collectively, “**Vendors**”) and applies to all use of public and third-party proprietary AI tools in the provision of products or services to SitusAMC, including the use of AI to generate source code, text, or other Outputs (as defined below) such as communications, presentations, reports, and other materials.

This Policy is intended to add to – not contradict, limit, or replace – other applicable SitusAMC policies, standards, legal requirements, and contractual obligations, all of which remain in full force and effect. This includes SitusAMC’s Supplier Code of Conduct.

2. Definitions

Artificial Intelligence (AI) – Any engineered or machine-based system that can, for a given set of objectives, generate Output such as content, predictions, recommendations, or decisions influencing the real or virtual environments with which the AI system interacts, encompassing a broad range of technologies to include traditional algorithms and predictive models, as well as GenAI platforms and technologies.

Authorized User – Any employee, contractor, or third party of Vendor approved to use AI in connection with an agreement between SitusAMC and Vendor.

Generative Artificial Intelligence (GenAI) – A subset of AI systems that can create original content in response to a user’s prompt or request. This content can include text, audio, code, images, video, and other content. GenAI relies on sophisticated machine learning models that simulate the learning and decision-making process of the human brain. GenAI platforms include ChatGPT, Google Gemini, Claude, Github Copilot, Codex, Stable Diffusion, Dall-E and similar tools.

Information Systems – All information technology applications, systems, data, information subscription access agreements, and telecommunication systems used in the conduct of SitusAMC’s business to access, manage, process, or store SitusAMC’s data, including those managed by third

parties. Such systems include but are not limited to software, software-as-a-service, hardware, mobile devices, computers, servers, workstations, routers, hubs, switches, networks, and data communications lines.

Output – Depending on the platform, AI can take in text, code, images, animations, video, and audio, then provide Output in the same or different formats, including predictions, recommendations, or decisions influencing the real or virtual environments with which the AI system interacts.

Permitted Uses – Any uses of AI approved by SitusAMC in writing.

Use Case – A particular application of AI technology to address a specific business need or solve a particular problem.

3. Use of AI Tools

The use of any AI tools, including GenAI, is limited to Permitted Uses that have been expressly approved by SitusAMC or otherwise agreed upon in writing by SitusAMC and the applicable Vendor.

Labeling Work: Vendors must clearly label all AI-generated material as such. Vendors must not represent that the Output of any AI tool is the Vendor's own independent thought or work.

3.1 Prohibited and Permitted Uses

A. Prohibition on Publicly Available AI Tools:

SitusAMC strictly prohibits the use of publicly available tools and the use of personal accounts by Vendors in connection with work performed by such Vendors for SitusAMC.

B. Prohibition on Certain Uses of Approved AI Tools:

AI tools shall not be used:

- To harass, discriminate against, bully, threaten, intimidate, or otherwise harm anyone in violation of SitusAMC policies;
- To create malicious code, confuse or deceive the AI tool, engineer prompt injection attacks, or engage in any deceptive practices;
- To create malicious, illegal, defamatory, explicit, or otherwise offensive or inappropriate content;
- To attempt to circumvent any blocks intended to dissuade illegal and inappropriate activity that is placed on the AI tools or Information Systems;
- To create content that infringes intellectual property rights (including, without limitation, trademarks, trade names, or copyrighted information) or in a manner that increases the risk of returning Outputs that may resemble a copyrighted work or the work of a specific artist or that may resemble a real or fictional person or character;
- To impersonate another person's image, name, voice, or likeness;
- To manipulate vulnerable individuals;
- To replace critical human judgment in situations where ethical, legal, professional, strategic or other complex decisions are required;
- If there is a risk of bias in the Outputs or if use of the AI tool could be unfair, discriminatory or unethical;

- In a manner that could violate applicable laws, regulations, contractual obligations, or internal policies of SitusAMC.

C. Prohibition on use of Certain Inputs with AI Tools without Prior Approval:

The following inputs should not be used without prior approval from SitusAMC Legal:

- Any personal data or personally identifiable information, which means and includes any information relating to an identified or identifiable natural person, such as:
 - an individual's name, public identification numbers, location data, online identifiers, or physical, physiological, genetic, mental, economic, cultural, or social factors;
 - Sensitive personal information or personal data (e.g. a government identifier, race or ethnicity information, etc.);
 - Biometric information; and
 - Information of minors;
- Attorney-client privileged information or attorney work product;
- Security or infrastructure data (e.g., passwords, public keys, or multi-factor authentication tokens);
- Employee compensation, benefits or health/medical data;
- Financial information;
- SitusAMC's confidential information, such as trade secrets, draft code not yet publicly released, prototypes, financial data, business strategies, information that gives SitusAMC a competitive advantage, other sensitive company information not yet in the public domain, and R&D information;
- SitusAMC's intellectual property, such as copyrighted information, trademarks, or trade names, product names or images containing any of the foregoing;
- Third party confidential information (including customer or end-user information);
- Third-party trademarks, trade names or copyrighted information;
- Any hateful, disturbing, sexually explicit, immoral, offensive, or politically charged terms or images or any other term or image that could subject you or SitusAMC to scandal or embarrassment if made public; and
- Any other highly sensitive or otherwise protected information or information that may be inappropriate for the provider of the GenAI tool to use as training data or that we do not want to become part of the Outputs to other users of the GenAI tool.

3.2 Legal and Ethical Responsibilities

AI must not be used in any circumstances that may violate applicable state or federal laws, or regulations, in the United States or globally.

A. Privacy and Security

Use of AI must not undermine security or privacy, and uses of personal information in connection with AI must follow SitusAMC's Privacy Policy. Generally, AI inputs should not include personal or sensitive information.

B. Automated Decision-Making

GenAI must not be used for automated processes or decision-making (“**ADM**”) without SitusAMC’s express written consent. GenAI must not be used for profiling.

4. AI Principles and Standards

SitusAMC follows the defined set of principles described below to guide all activities involving the development, use and deployment of AI systems.

A. AI systems should be valid and reliable	<p>AI systems should be subject to ongoing testing and/or monitoring to confirm they are performing as intended;</p> <p>Such testing should, when available, include testing the suitability, completeness, representativeness, timeliness and accuracy of the data used to train the model. Validation can take the form of comparing model performance on data available at the time of model development to the performance observed on data post-implementation, measuring performance against expert review or other methods. It may also be appropriate to conduct an audit to assess whether AI models are subject to controls that appropriately account for any risks and weaknesses in validation.</p>
B. AI systems should be safe	<p>Safe operation of AI systems may be improved through:</p> <ul style="list-style-type: none"> • Responsible design, development, deployment, and termination practices; • Applying a systemic risk-management approach to each phase of the AI system life-cycle on a continuous basis to address risks related to AI systems, including privacy, security and unfair discrimination; • Comprehensive training of those deploying and using the AI system on responsible use of the AI system; • Responsible decision-making by those deploying and using the AI system; and • Identification, documentation, and remediation of risks based on empirical evidence of incidents.
C. AI systems should be secure and resilient	<p>SitusAMC requires AI tools to be deployed in resilient ecosystems, meaning that they are able to: (i) withstand unexpected adverse events or unexpected changes in their environment or use; and (ii) maintain their functions and structure in the face of internal and external change. To that end, any AI tool provisioned by Vendor to SitusAMC must comply (as applicable) with all relevant SitusAMC policies and procedures, including information security, data destruction, business continuity and code of conduct.</p> <p>Similarly, AI tools must have reasonable protections in place to maintain the confidentiality, integrity, and availability of non-public information (particularly user information) and to prevent the unauthorized access and use of such information and the tool at large. This applies to all stages of the AI system’s life cycle, including design, development, validation, implementation (both systems and business), use, on-going monitoring,</p>

	updating and retirement.
D. AI systems should be accurate, accountable, and transparent	<p>Accountability requires ongoing monitoring and auditing of relevant systems, including reporting protocols and requirements, and, when necessary, escalation for further resolution. Logs should be reviewed regularly for suspicious or unauthorized activity.</p> <p>GenAI Outputs must be vetted for accuracy. Vendors should exercise caution when relying on GenAI-generated content and are expected to review and independently confirm the accuracy of Outputs before using them.</p> <p>Disclosure of AI Technology Use: When using AI technology, Vendors are expected to disclose its use. Content generated by AI should be appropriately labeled, marked, or footnoted by Vendor as such.</p> <p>Documentation and Citation Requirements: AI Outputs must be internally documented. Vendors must consider whether sources or databases should be cited and cite accordingly.</p> <p>Process and Procedure Documentation: Vendors are expected to clearly document all processes and procedures for designing, developing, verifying, using, updating, and/or monitoring AI systems. These processes and procedures should be included in the AI Impact Assessment.</p>
E. AI systems should be explainable and interpretable	<p>Vendor should ensure that its AI systems are easily accessible, explainable, and interpretable, including by:</p> <ul style="list-style-type: none"> • Maintaining inventories and descriptions of AI tools; • Recording detailed documentation of the development and use of AI systems; • Assessing the interpretability, repeatability, robustness, regular tuning, reproducibility, traceability, model drift, and the auditability of these AI systems; • Communicating with third parties who use AI systems to ensure alignment with the guidelines above; and • Documenting any and all of the above phenomena as well as any mitigations or follow up measures.
F. AI systems should be privacy-enhanced	<p>Privacy values such as anonymity and confidentiality must guide choices for AI system design, development, and deployment. AI systems and their use should be designed to support privacy-enhancing technologies for AI, as well as data-minimizing methods such as de-identification and aggregation.</p>
G. AI systems should be fair – with unlawful bias managed	<p>The use of AI must be ethical, responsible, and free from bias or discriminatory outcomes. Steps should be taken to detect and address algorithmic bias. Vendors should not use AI to generate content that is illegal, discriminatory, offensive, or inappropriate.</p>

5. AI Impact Assessment

Upon SitusAMC's request, Vendor will: (i) complete SitusAMC's AI Impact Assessment ("**AIIA**") process, which includes completing a detailed risk assessment questionnaire; and (ii) comply with the processes and mitigating controls described in each AIIA. Vendor will promptly notify SitusAMC prior to (i) changing any processes or mitigating controls in a manner that could adversely affect the controls or standards of protection approved through the AIIA process and (ii) prior to change changes to the agreed use case described in the AIIA.

6. Revision History

Version	Description
1.0	Published July 25, 2025