Policy Name: Artificial Intelligence (AI) in Administrative and Employment Contexts Policy

Policy Owner: Office of the Executive Vice President for Administration and Finance

Policy Contact: AI Governance Officer, aigovernance@gatech.edu

Reviewed By: University System Office, Executive Leadership Team, Policy Steering Committee, Office of the Executive Vice President for Academic Affairs and Provost, Office of the Executive Vice President for Research, Office of General Counsel, Office of Internal Audit, Office of Information Technology, Office of Procurement and Business Services

Policy Steering Committee Approval: June 2026

Policy Purpose: The purpose of this policy is to establish clear guidelines and a supportive governance structure for the ethical, responsible, and secure use of Artificial Intelligence (AI) in administrative, operational, and business activities performed on behalf of Georgia Tech. This policy seeks to balance University System of Georgia compliance obligations with the Institute's commitment to enabling safe, innovative, and productive access to emerging technologies.

Summary of Substantive Policy Elements:

- **Defines Covered Audiences:** Applies to Georgia Tech employees (including student employees), affiliates, and units performing administrative, operational, or business activities.
- **Establishes Enterprise Coordination:** Formally creates the Institute AI Governance Program and the cross-functional AI Governance Committee to align decision-making and support local divisions.
- **Introduces a Structured Review Process:** Details a risk-based evaluation standard that routes proposed software tools to either the centralized Institute AI Register or unit-level Local AI Registers, helping employees navigate safe pathways for AI adoption.
- **Prioritizes Data Privacy:** Outlines clear guardrails to safeguard Protected Data and Personally Identifiable Information (PII), ensuring sensitive information is only shared with AI tools that feature verified security controls.
- **Delineates Acceptable Operational Boundaries:** Identifies and provides guidance on avoiding high-risk or inappropriate AI activities, such as unauthorized system integrations, privacy risks, or automated employment actions without human review.
- **Emphasizes Human Accountability:** Reinforces that AI is an assistive tool meant to support, rather than replace, human critical thinking and professional judgment; outlines expectations for employees to verify the accuracy of AI-generated content before relying on it for official work.
- **Promotes Professional Development:** Focuses on empowering employees through ongoing compliance training and self-service educational resources to build widespread AI literacy and risk awareness across the campus.

Georgia Institute of Technology

Artificial Intelligence (AI) in Administrative and Employment Contexts Policy

Policy No.
Type of Policy: Administrative
Effective Date: TBD
Last Revised: New Policy
External Requirement for Review: TBD
Compliance Reporting: TBD
Policy Owner: Office of the Executive Vice President for Administration and Finance
Policy Contact: AI Governance Officer, aigovernance@gatech.edu

1. Reason for Policy

The growing availability and use of Artificial Intelligence ("AI") are providing new opportunities for teaching, learning, research, administrative, and related activities. The Georgia Institute of Technology ("Georgia Tech", "GT", "Institute") recognizes AI as a catalyst for innovation, productivity, and efficiency, and is committed to enabling responsible access to these tools. As these new capabilities become available, all employees (including student employees), affiliates, and units (hereinafter collectively referred to as "GT Community Members") must understand how to utilize AI in an ethical, responsible, and secure manner in their Georgia Tech-related activities. While AI provides new capabilities, it is designed to assist and must never replace the critical thinking, professional judgment, or decision-making responsibilities of GT Community Members.

This Policy outlines requirements in compliance with the University System of Georgia's ("USG") various Policies and supporting artifacts, including, but not limited to, the IT Handbook, AI Companion Guide, and Board of Regents Policy Manual.

This Policy applies in connection with the Georgia Tech AI in Academic and Research Contexts Policy, which notes additional requirements related to all students and GT Community Members who work in an academic or research setting.

Refer to the Georgia Tech AI Governance website for corresponding guidelines, standards, procedures, and resources. Learn More

2. Policy Statement

This Policy governs the procurement, implementation, and use of AI in Administrative and Employment Contexts. While a complete glossary is maintained in Section 4 (Definitions), the following core concepts are defined here to establish the immediate scope of this Policy:

Artificial Intelligence (AI) refers to a technology family that enables computers to perform a variety of advanced functions, including the ability to process visual cues, understand and translate spoken and written language, analyze data, and make complex recommendations. This technology family includes, but is not limited to, Generative AI (GenAI), Large Language Models (LLMs), and Machine Learning (ML).

AI Tools refer to any software, platform, device, or cloud service – whether Institute-licensed, open-source, embedded within another product, or publicly accessible on the web – whose core functionality relies on an AI technology as defined above.

2.1 Guiding Ethical Principles and Safeguards

This Policy is guided by the following ethical principles and safeguards:

- Accountability
- Safeguarding Protected Data
- Human Oversight and Safety
- Safeguards against Hallucination
- Fairness and Bias Mitigation
- Transparency
- Accessibility
- Protection against Prompt Injection Attacks

GT Community Members who use AI Tools in Administrative and Employment Contexts must act in a manner consistent with these guiding ethical principles. Furthermore, users must employ due care to safeguard against AI abuse, reduce the risk of misleading outputs or outputs resulting from Prompt Injection Attacks or other adversarial manipulation, and ensure any AI that interacts directly with people clearly discloses that its responses are generated by AI. Using generated content that is inappropriate, discriminatory, or otherwise harmful to others, the Institute, or the USG is prohibited.

2.2 AI Tool Authorization and Registers

The Institute maintains inventories of authorized AI Tools, which the AI Governance Program must review at least annually. The specific data elements and tracking criteria required for these inventories are defined in the accompanying guidelines and standards. GT Community Members must access and utilize AI Tools in

accordance with the approval pathways outlined below. GT Community Members may appeal decisions that deny the use of an AI Tool in accordance with the procedures outlined in the accompanying Guidance.

2.2.1 Accessing AI Tools

GT Community Members must use AI Tools that are either an (1) Institutionally Approved AI Tool or a (2) Limited Use AI Tool as designated by a Local AI Point of Contact.

GT Community Members must not independently purchase, expense, or deploy an unapproved AI Tool onto Georgia Tech systems or for work on Georgia Tech matters until it has been formally evaluated and added to an AI Register.

While this Policy applies to students acting in their capacity as employees, rules regarding a student's personal use of AI or AI use in Academic or Research Contexts are governed by the Georgia Tech AI in Academic and Research Contexts Policy.

The use of Georgia Tech equipment, credentials or email addresses to access unapproved, public, or personally licensed or personally purchased AI Tools is prohibited.

2.2.2 Institute Register of Approved AI Tools

Georgia Tech maintains an Institute AI Register of Institutionally Approved AI Tools providing additional details for each. The AI Governance Program evaluates, approves, and adds tools to this register in accordance with the AI Tool Approval Standard. GT Community Members are authorized to use Institutionally Approved AI Tools for their approved scope in ways consistent with this Policy. Learn More

2.2.3 Local AI Register of Approved Limited Use AI Tools

GT Community Members may use AI Tools that are not listed on the Institute Register only after they have been reviewed and approved by the designated Local AI Point of Contact for their unit. Section 2.7.1 below describes the appointment process for Local AI Points of Contact.

Local AI Points of Contact will facilitate the evaluation of proposed tools to determine if they are appropriate based on consideration for the local unit's needs and the ethical principles and safeguards outlined in Section 2.1 above. Local AI Points of Contact may only authorize access to tools that meet the requirements and utilize the pre-approved pathways established by the AI Tool Approval Standard. AI Tools that are reviewed and approved by the Local AI Points of Contact will be categorized as Limited Use AI Tools, and Local AI Points of Contact shall maintain unit-level registers (Local AI Register) for ease of use for GT Community Members.

Any use of a Limited Use AI Tool must be solely for the approved scope and be consistent with the guiding ethical principles and safeguards listed in Section 2.1.

2.2.4 Third-Party AI Tools and External Collaborations

AI Tools procured from third-party suppliers or developed alongside external collaborators carry varying levels of enterprise risk. GT Community Members must submit proposed third-party AI Tools for risk assessment in accordance with the AI Tool Approval Standard. Based on the tool's intended use and its associated risk profile, the Institute may require formal risk and security assessments prior to deployment. When formal assessments are required, the Institute may require procurement and service agreements to include provisions ensuring the supplier or partner adheres to the Institute's guiding ethical principles and safeguards, data protection requirements, and safety standards, as detailed in the accompanying Guidance.

2.3 Responsible Use and Accountability

Through this Policy and supporting artifacts, Georgia Tech maintains a standard for responsible AI use in Administrative and Employment Contexts. Because AI use can implicate additional Georgia Tech requirements and expectations, GT Community Members must comply with this Policy in conjunction with all other relevant Policies, including those in academic, research, administrative, and information technology contexts.

2.3.1 Verifying the Accuracy After AI Use

AI must be utilized as a tool and must never replace the critical thinking, professional judgment, or decision-making responsibilities of a GT Community Member.

GT Community Members must verify the accuracy, appropriateness, and reasonableness of information generated by AI Tools before using or relying on it, as AI output can be inaccurate, biased, hallucinated, or contain copyrighted material. If a GT Community Member cannot find a reliable source to independently verify the information generated by the AI Tool, they must not use that information for official work purposes.

GT Community Members remain wholly accountable for the accuracy of any information they use, publish, or rely upon that includes AI-generated material; and

must retain records of substantive decisions or actions taken based on AI-generated outputs in accordance with Institute record retention requirements.

2.3.2 Disclosure of AI Use

GT Community Members must appropriately disclose and cite significant AI usage in administrative work products. AI interacting directly with people must clearly disclose its machine-generated nature. Specific standards for disclosure templates and citation formats are provided in the accompanying Guidance.

2.3.3 Respecting Intellectual Property (IP) and Regulatory Requirements

Any AI usage that violates applicable laws, regulations, intellectual property rights, or employment standards and Policies is prohibited. GT Community Members must not use AI Tools to infringe upon third-party copyrights or expose the proprietary or protected information of Georgia Tech or any third parties.

2.4 Data Protection and Privacy

Georgia Tech is committed to protecting the integrity, security, and privacy of institutional data. The use of AI Tools must align with the Institute's data categorization standards and comply with all corresponding Cybersecurity Data Protection Safeguards, Cybersecurity Protected Data Practices, and data privacy Policies.

2.4.1 Safeguarding Protected Data

Consistent with existing institutional Policies and legal requirements, GT Community Members must safeguard any information that includes personally identifiable information (PII) or is categorized by the Institute as Protected Data.

GT Community Members must not submit any data categorized by the Institute as Protected Data or any data that incorporates personally identifiable information (PII) that can directly or indirectly identify another individual, including combinations of data elements that could reasonably identify an individual, unless it is an approved scope for an approved AI Tool on an AI Register. Inputting Protected Data into an unapproved AI Tool (including public LLMs, image generators, audio generators, or data analysis platforms) is prohibited.

Even when using approved AI Tools within their approved scope, GT Community Members must adequately safeguard data from improper disclosure.

2.4.2 Preventing the Exposure of Derived Information

AI Tools can aggregate and analyze multiple sources of data to derive sensitive insights, even when individual data elements are not independently sensitive. GT

Community Members and units deploying AI must ensure that AI Tools are not used in a manner that results in the unintended identification, exposure, or inference of protected or sensitive information.

2.5 Prohibited Misuse and Security Incidents

Georgia Tech enforces the responsible use of AI to protect the Institute, its data, and its community. The Georgia Tech Cybersecurity team and the Human Resources team will manage suspected misuse or security incidents involving AI Tools in accordance with existing institutional incident response procedures and human resources processes.

2.5.1 Prohibited Misuse and Incident Reporting

GT Community Members must not use AI to conduct activities that violate applicable laws, regulations, privacy standards, or Institute or USG Policies. Impermissible activities span both malicious acts and unauthorized administrative uses, including but not limited to:

- Malicious & Fraudulent Acts: Utilizing AI for financial fraud, launching malicious cyberattacks (such as phishing or social engineering), or propagating misinformation.
- Privacy & Surveillance Violations: Gathering personal information without an individual's permission, or using AI for the unauthorized monitoring, tracking, or profiling of employees, students, or visitors.
- Discriminatory & Unfair Outcomes: Generating discriminatory outputs that result in unequal treatment, or delegating professional judgment to AI to automate employment, grievance, or disciplinary decisions without appropriate human review.
- Unauthorized Enterprise Deployment: Bypassing institutional processes to deploy, scale, or integrate AI Tools into live operations, public-facing services, or enterprise systems without formal institutional authorization and risk assessment.

GT Community Members should promptly report any suspected AI misuse or ethical concerns, but must immediately report any associated data incidents or breaches to the Georgia Tech Cybersecurity team (email soc@gatech.edu or call 404-385-2927).

2.5.2 Emergency Suspension of AI Services

If an AI Tool is confirmed to generate operational, reputational, data privacy, security, or malicious consequences, the Georgia Tech or USG Chief Information Officer or Chief Information Security Officer may require its immediate suspension. Upon such a directive, GT Community Members shall immediately cease operation of the AI Tool. The Institute will conduct a formal investigation and if appropriate execute an approved mitigation plan before the AI Tool may resume use. Units utilizing AI Tools

that support critical business functions must maintain business continuity plans and documented knowledge of the underlying business processes to provide alternate means for achieving required results during such suspensions.

2.6 Education and Awareness

Georgia Tech provides ongoing education and awareness campaigns on AI risks, ethics, safety, responsible use, regulatory compliance, and Policy awareness. To support this, the Institute coordinates education and awareness offerings, hosts self-service support materials (such as user guides and FAQs), establishes participation expectations, including requirements for maintaining documented evidence of training completion and participation, and assesses education and awareness effectiveness.

GT Community Members must maintain compliance with all required training.

2.7 Institutional Oversight and Accountability

This Policy establishes the Institute AI Governance Program to provide Institute-wide coordination and alignment for AI governance. The AI Governance Program is led by an AI Governance Officer appointed by the AI Governance Committee. AI Governance Committee members are appointed annually by the Chief Information Officer (CIO) and the Executive Sponsors, which include the Executive Vice President for Administration and Finance (EVPAF), the Provost and Executive Vice President for Academic Affairs (EVPAA), and the Executive Vice President for Research (EVPR). The AI Governance Officer will collaborate with designees of the Executive Sponsors and together, provide Institute-wide coordination, alignment, and escalation for AI governance within the boundaries of this Policy.

The AI Governance Program maintains a published process to receive and route questions and complaints related to AI use in Administrative and Employment Contexts, coordinating resolution through existing institutional mechanisms. The AI Governance Program coordinates and enables AI governance across the Institute, while decisions that only impact academics and research remain under the authority of the EVPAA and EVPR and their designees, respectively.

2.7.1 Unit Oversight, Accountability, and Local AI Points of Contact

Executive Sponsors, members of the President's Cabinet, and Deans must designate one or more Local AI Points of Contact to support their division or unit.

A Local AI Point of Contact serves as a liaison to the Institute AI Governance Program and a resource for localized guidance. While they serve as the administrative decision-maker with the authority to grant or deny access to Limited Use AI Tools for their unit, this authority must be exercised within the pathways and requirements established centrally by the AI Tool Approval Standard. To ensure

compliance with Institute security, privacy, and inventory rules, all GT Community Members must have proposed Limited Use AI Tools reviewed and approved by their Local AI Point of Contact in accordance with this Standard prior to use.

The appointing leaders (e.g., Executive Sponsors, members of the President's Cabinet, Deans) must provide the names of their designated Local AI Points of Contact to the AI Governance Program for publishing, notify the Program when changes are necessary, and review their appointments for accuracy at least annually.

2.7.2 Governance of Intelligent Automations

Intelligent Automation (i.e., AI, Agentic AI, Robotic Process Automation) implementations carry inherent enterprise risk. While discrete, human-prompted AI Tools are governed by the AI Tool Approval Standard, autonomous implementations – such as Robotic Process Automation (RPA), Agentic AI, and AI integrated into autonomous workflows – will be assessed for risk prior to development, deployment, and use in accordance with established Institute automation governance standards. Regardless of the risk profile, all implementations must maintain strict access controls, operate within their approved scope, and be continuously monitored to prevent drift from their intended purpose.

Based on the risk profile, Intelligent Automations will be subject to a proportionate level of formal governance and documentation. Depending on the assessed risk, implementations may require formal governance committee oversight, documented 'go/no-go' deployment approvals, comprehensive operational lifecycle logs, and synchronization with underlying business process changes. Furthermore, the assessed risk profile will determine if, and to what extent, formal engagement is required with Georgia Tech's Department of Internal Auditing and the Cybersecurity team regarding ongoing risk management.

2.7.3 Monitoring for Legal and Regulatory Changes

The Office of General Counsel (OGC) monitors AI-related legal, privacy, and regulatory developments on an ongoing basis in an effort to ensure AI Tools comply with applicable laws and standards. The OGC coordinates with the AI Governance Officer to update relevant stakeholders (e.g., AI Governance Committee, Executive Sponsors) as appropriate. Such updates may necessitate reviews and updates to this Policy, its supporting artifacts, and other related Policies.

2.7.4 Monitoring for Compliance and Record Retention

The designated leaders, committees, and personnel defined in Section 6 (Responsibilities) are responsible for ensuring compliance with USG and Institute Policies. These named entities must self-monitor to ensure compliance, maintain formal audit trail records sufficient in both detail and retention lengths to

demonstrate such compliance during audits or investigations, and store those records in approved secure repositories.

2.7.5 Policy Maintenance and Review

The AI Governance Program shall establish a regular schedule to formally review and update all institutional AI governance Policies and supporting artifacts. The AI Governance Program must review this AI Policy annually, or more frequently as needed, to reflect emerging legal, technological, or organizational changes.

3. Scope

This Policy governs the use of AI by all Georgia Tech employees (including student employees), affiliates, and units in the performance of any administrative, operational, or business activity for or on behalf of Georgia Tech. Additional Policies and supporting artifacts, including the Academic & Research AI Policy and the Faculty Handbook, may also address permissible uses of AI in specific contexts.

4. Definitions

4.1 **Academic and Research (A&R) Contexts**: Academic and research work, including but not limited to teaching, learning, coursework, assessment, laboratory or field research, research data analysis, and preparation of scholarly communications

4.2 **Administrative and Employment (A&E) Contexts**: Any administrative, operational, or business activity performed for or on behalf of Georgia Tech that falls outside the specific scope of Academic and Research Contexts.

4.3 **Agentic AI**: AI models that are given agency to autonomously execute multi-step workflows using AI agents.

4.4 **AI Tool**: AI Tools refer to any software, platform, device, or cloud service – whether Institute-licensed, open-source, embedded within another product, or publicly accessible on the web – whose core functionality relies on an AI system.

4.5 **Artificial Intelligence (AI)**: A technology family that enables computers to perform a variety of advanced functions, including the ability to process visual

cues, understand and translate spoken and written language, analyze data, and make recommendations from heuristic analyses.

4.6 **Generative AI (GenAI)**: A form of AI capable of generating text, images, videos or other data using generative models, often in response to prompts.

4.7 **Hallucination**: Conditions when an LLM process identifies patterns or objects that are nonexistent, creating nonsensical or inaccurate outputs.

4.8 **Human Oversight**: Independent human judgement that is applied to review and validate AI outputs before acceptance.

4.9 **Institute AI Register**: The Institute system of record for Institutionally Approved AI Tools.

4.10 **Institutionally Approved AI Tool**: An AI Tool approved by the AI Governance Committee and listed on the Institute AI Register.

4.11 **Intelligent Automation (IA)**: Sometimes called cognitive automation, refers to the use of automation technologies such as Artificial Intelligence, Agentic AI, business process automation, and Robotic Process Automation, to streamline and scale decision-making across organizations.

4.12 **Large Language Model (LLM)**: A computational model recognized for the ability to achieve general-purpose language generation and other natural language processing tasks such as classification.

4.13 **Limited Use AI Tool**: An AI Tool reviewed and approved by a Local AI Point of Contact based on the requirements established by the AI Tool Approval Standard and the guiding ethical principles and safeguards outlined in Section 2.1.

4.14 **Local AI Register**: A local system of record for Limited Use AI Tools.

4.15 **Machine Learning (ML)**: A branch of AI and computer science that focuses on using data and algorithms to enable AI to imitate the way that humans learn, gradually improving its accuracy.

4.16 **Prompt Injection Attack**: A type of cyberattack that crafts inputs that cause an AI Tool to override intended instructions or controls, produce misleading outputs, or disclose information inappropriately.

4.17 **Protected Data**: A data protection categorization where information is generally not available to parties outside of the Georgia Tech community. This is the default data protection categorization for Organizational Data. A Protected Data categorization does not always mean that the data contained therein is confidential or non-disclosable and such data may by subject to disclosure under the Georgia Open Records Act or other applicable laws and regulations. For more information, see the Data Governance and Management

Policy (https://policylibrary.gatech.edu/information-technology/data-governance-and-management-policy).

4.18 Robotic Process Automation (RPA): A form of business process automation that utilizes software robots (also known as bots) to execute predefined, rule-based workflows. While RPA is a key component of the broader Intelligent Automation ecosystem, it operates on structured logic rather than the heuristic learning models utilized by true Artificial Intelligence.

5. Procedures

This Policy is supported by additional related Institute guidelines, standards, and supporting artifacts, including the accompanying Guidance on the Use of AI in Administrative and Employment Contexts. If there is a conflict, this Policy will be the authoritative source.

6. Responsibilities

6.1 Academic Domain: The Provost & Executive Vice President for Academic Affairs and designated college and school leaders provide academic direction and ensure Policy-aligned implementation in Academic Contexts. Academic colleges designate a college-level AI point of contact; schools, departments, and units may designate their own points of contact or adopt the college point of contact.

6.2 Administrative Domain: The Executive Vice President for Administration and Finance and their designated administrative leaders provide direction and ensure Policy-aligned implementation in Administrative and Employment Contexts.

6.3 AI Governance Committee: Provides strategic guidance, direction, and sponsorship for Institute AI governance; designates the AI Governance Officer.

6.4 AI Governance Officer: Leads the Institute's AI Governance Program; serves as the Institute point of coordination for AI governance and convenes designees of the Executive Sponsors to align decisions across Academic, Research, and Administrative Domains.

6.5 AI Governance Program: Coordinates AI governance across the Institute, including coordination with the Academic, Research, and Administrative Domains.

6.6 AI Tool Points of Contact: Each approved AI Tool must have a designated primary point of contact (e.g., the Institute tool/service manager) that works with the Institute or Local AI Points of Contact to understand and evaluate AI Tools.

6.7 Chief Information Officer (CIO): Provides the underlying technology infrastructure and systems support for the AI Governance Program;

possesses the authority to immediately suspend any AI Tool that is confirmed to generate severe operational, privacy, or security consequences; coordinates with the Executive Sponsors on resources necessary to support and sustain the AI Governance Program.

6.8 Chief Information Security Officer (CISO): Ensures the Cybersecurity Program is appropriately resourced to manage AI Tool evaluations, tool and environment controls, and emerging AI risks; possesses the authority to immediately suspend any AI Tool that is confirmed to generate severe operational, privacy, or security consequences.

6.9 Cybersecurity Program (Cybersecurity): Supports the AI Governance Program by orchestrating the risk and security evaluations required by the AI Tool Approval Standard. This includes conducting formal cybersecurity risk assessments, generating comprehensive risk profiles based on a proposed tool's data access and integrations, and establishing the necessary security controls and deployment approvals required for both discrete AI Tools and complex Intelligent Automations.

6.10 Department of Internal Auditing (DIA): Advises and supports the AI Governance Program; where appropriate, directs and advises units on the ongoing risk management of AI and other complex Intelligent Automations; possesses the authority to audit institutional compliance with this Policy.

6.11 Employees, Student Employees, and Affiliates: Follow Institute and unit rules established under this Policy, apply the Guidance on the Use of AI in Administrative and Employment Contexts where applicable, and act in accordance with all other relevant Policies.

6.12 Executive Sponsors: The Provost & Executive Vice President for Academic Affairs (Provost & EVPAA); the Executive Vice President for Research (EVPR); and the Executive Vice President for Administration and Finance (EVPAF) provide strategic oversight for this Policy, designateAcademic, Research, and Administrative Domain point of contacts, and provide the resources necessary to support and sustain the AI Governance Program.

6.13 Local AI Point of Contacts: Serve as a support network and local liaisons to help GT Community Members navigate the Institute's AI requirements and assist in evaluating proposed AI Tools in accordance with the AI Tool Approval Standard.

6.14 Office of General Counsel (OGC): Monitors AI-related legal, privacy, and regulatory developments on an ongoing basis to support compliance with applicable laws and standards; advises and supports the AI Governance Program; and provides guidance on requisite AI-specific safeguards and language within third-party procurement contracts.

6.15 Research Domain: The Executive Vice President for Research and designated research leaders provide research direction and ensure Policy-aligned

implementation in Research Contexts; and the Office of the EVPR designates research Points of Contact appropriate to its portfolio.

6.16 **Units**: Where appropriate, implement unit-specific guidance; may adopt additional local requirements for AI use within their unit but they are not permitted to exempt GT Community Members from Institute AI provisions.

7. Enforcement

Georgia Tech, the University System of Georgia, and/or the State of Georgia may periodically audit compliance with this Policy.

For more information, or to share suspected instances of noncompliance with this Policy, please contact the AI Governance Program at aigovernance@gatech.edu.

8. Related Information

Resource	Link
Georgia Tech Guidance on the Use of AI in Administrative and Employment Contexts	https://oit.gatech.edu/sites/default/files/2026-06/A%26E%20Supplemental%20v260515-009.pdf
Georgia Tech AI in Academic & Research Contexts Policy	https://www.policylibrary.gatech.edu/artificial-intelligence-ai-academic-research-contexts
Georgia Tech Guidance on the Use of AI in Academic & Research Contexts	https://oit.gatech.edu/sites/default/files/2026-06/A%26R%20Supplemental%20v260515-006.pdf
Georgia Tech AI Governance Program	https://oit.gatech.edu/governance/ai
Georgia Tech AI Tool Approval Standard	https://oit.gatech.edu/sites/default/files/2026-06/AI%20Tool%20Approval%20Standard%20v260415-006_1.pdf
Georgia Tech Cybersecurity Program (Data Protection Safeguards, Protected Data Practices)	https://security.gatech.edu/
Georgia Tech Data Privacy Program	https://generalcounsel.gatech.edu/data-privacy/landing-page
Georgia Tech Data Governance & Discovery Program	https://oit.gatech.edu/governance/data/overview

Georgia Tech Data Governance & Management Policy	https://policylibrary.gatech.edu/information-technology/data-governance-and-management-policy
USG IT Handbook	https://usg.policystat.com/policy/19852110/latest/
USG IT Handbook AI Companion Guide	https://usg.policystat.com/doc_attachment/view/70020976/
USG Board of Regents Policy Manual	https://usg.policystat.com/policy/20084036/latest/
USG Business Procedures Manual	https://usg.policystat.com/policy/19655231/latest/

9. Policy History

Revision Date	Author	Description
TBD	Data Governance Officer on behalf of the Office of the Executive Vice President for Administration and Finance	New Policy