Guidance on the Use of AI in Administrative & Employment (A&E) Contexts
Supplemental Version: v260515-009

Table of Contents

1. Introduction

The Georgia Institute of Technology ("Georgia Tech", "GT", "Institute") recognizes Artificial Intelligence ("AI") as a catalyst for innovation and operational efficiency across institutional functions. The Institute is committed to enabling its employees, including student employees, contractors, affiliates, and units ("GT Community Members") to use AI Tools in a responsible, secure, and ethical manner. The overarching purpose of this guidance is to balance the benefits of using these technological tools to enhance daily work and decision-making while ensuring AI Tools are used in strict alignment with Institutional values, data security and privacy considerations, and applicable laws.

2. Navigating Georgia Tech's AI Policies

The University System of Georgia (USG) issues universal mandates governing AI that are required to apply across the Institute. However, the practical application of these universal rules varies depending on the context in which a GT Community Member is operating. Because of this, Georgia Tech utilizes a paired Policy approach:

- **Administrative and Employment (A&E) Contexts:** This document is the *Guidance on the Use of AI in A&E Contexts*. It operationalizes the corresponding *AI in A&E Contexts Policy* and serves as the practical manual for business operations, employee conduct, and Institute technologies.
- **Academic and Research (A&R) Contexts:** GT Community Members who also teach, learn, or conduct research must read and comply with the paired *AI in A&R Contexts Policy* and review its accompanying *Guidance on the Use of AI in A&R Contexts*.

It is highly common for individuals – such as student employees, research administrators, or faculty with administrative appointments – to operate in both contexts simultaneously. In these instances, GT Community Members are responsible for understanding and adhering to both sets of Policies and their corresponding guidelines and related artifacts depending on the specific task they are performing.

3. Operationalizing Guiding Ethical Principles and Safeguards for the Use of AI

At Georgia Tech, the use of AI Tools is guided by eight principles and safeguards:

1. Accountability
2. Safeguarding Protected Data
3. Human Oversight and Safety
4. Safeguards against Hallucination
5. Fairness and Bias Mitigation
6. Transparency
7. Accessibility
8. Protection against Prompt Injection Attacks

These principles are operationalized in the A&E Context as follows:

- **Accountability** is a shared responsibility between the individual user and the Institute. For the individual, it means that GT Community Members remain wholly accountable for the accuracy, appropriateness, and compliance of any information they use, publish, or rely upon that includes AI-generated material. For the Institute, it means that the AI Governance Program, AI Governance Officer, AI Governance Committee, and the designees of the Executive Sponsors collaborate to (1) oversee, coordinate, and align Institute usage of AI in Administrative and Employment Contexts within the bounds of Policy, (2) ensure proper responses to audit and investigation requests, and (3) coordinate the resolution of questions, complaints, and reports of noncompliance through existing Institute mechanisms.
- **Safeguarding Protected Data** means that GT Community Members must not submit (1) any data categorized by the Institute as Protected Data or (2) any data including personally identifiable information (“PII”) (including PII that can indirectly identify someone, for example, the combination of unit, job title, and years of service) into an AI Tool not listed on the Institute AI Register or the Local AI Registers. This prohibition extends beyond public Large Language Models (LLMs) to include image generators, audio generators, and data analysis platforms. Even when using Institutionally Approved AI Tools, GT Community Members must adequately safeguard this data from improper disclosure. Finally, users must actively safeguard against AI's ability to "connect the dots," ensuring they do not use AI Tools to analyze separate, non-sensitive data sources in a way that accidentally derives, unmasks, or exposes confidential information.
- **Human Oversight and Safety** AI Tools shall support, but not replace, human judgement, decision making, or accountability. GT Community Members must review and independently verify the accuracy, appropriateness, and reasonableness of information generated by AI Tools prior to relying on such information for substantive business decisions. It also means they accept responsibility for relying on or using any AI-generated content. Due to the risks associated with AI Tools, GT Community Members should evaluate whether any AI Tools are suitable for their specific tasks. Additionally, Human Oversight includes reviewing and approving AI Tools for inclusion on the Institute AI Register or the Local AI Registers.
- **Safeguards against Hallucination** means reviewing and verifying the accuracy of AI-generated business information, because AI models may identify patterns that are nonexistent, creating

nonsensical, inaccurate, or misleading outputs, including content and materials from other authors and/or others' intellectual property.

- **Fairness and Bias Mitigation** means GT Community Members must actively evaluate AI outputs for potential biases—such as training, cognitive, algorithmic, or confirmation biases—and should seek input and perspectives from diverse stakeholder groups. To operationalize this, GT Community Members should (1) ensure AI-generated outputs do not lead to business decisions that could disproportionately impact individuals or groups based on their protected classifications under applicable law, and (2) avoid reliance on AI-generated results that may be indicative of potential bias. Furthermore, AI must never be used to create content that is inappropriate, discriminatory, or otherwise harmful to others, the Institute, or the USG.
- **Transparency** means that GT Community Members shall not represent AI-generated content as solely their own original work. Because AI Tools often mimic human behavior, speech, and mannerisms, any AI deployed to interact directly with humans (e.g., customer service chatbots) must explicitly disclose that its outputs or responses are machine generated. Furthermore, when producing administrative documents, reports, or work products, GT Community Members should appropriately disclose significant AI usage to their supervisors or stakeholders so that machine-generated analysis is not misrepresented as human professional judgment.
- **Accessibility** means that basic accessibility principles and practices are applied when deploying AI Tools for administrative operations, and the assurance that any AI Tools required for GT Community Member use are accessible to assistive technologies as defined by applicable laws or regulations.
- **Protection against Prompt Injection Attacks** means actively assessing and mitigating the risk that crafted, malicious inputs can cause an AI Tool to override intended instructions or controls, and to then produce misleading outputs or to disclose Institute information inappropriately.

Operationalizations of the guiding ethical principles are provided to empower GT Community Members to use AI Tools safely and productively in their administrative, operational, and business activities. These principles, in conjunction with the AI Tool Approval Standard (https://oit.gatech.edu/governance/ai/), support Local AI Points of Contact in assessing AI Tools not listed on the Institute AI Register of Institutionally Approved AI Tools (https://oit.gatech.edu/governance/ai/). The Institute shall maintain documented examples and use cases demonstrating how these principles are operationalized in practice. These artifacts shall support training, governance reviews, and audit activities.

4. Administrative and Employee Use of AI

This section operationalizes the AI Policy by providing specific guidance for GT Community Members involved in administrative, operational, or business activities performed for or on behalf of Georgia Tech.

Permissible Tasks and Data Alignment

Use of approved AI Tools is permitted for Institute business purposes; however, AI should be used strictly as a tool and may not replace the critical thinking, professional judgment, or decision-making of a GT Community Member.

- **Approved AI Tools, Tiers, and Scopes:** GT Community Members may use AI Tools listed on the Institute or Local AI Registers, but strictly within the tool's approved tier, data scope, and use scope. Because vendors often offer multiple licensing tiers of the same tool, approval for a secure, GT-licensed edition does not automatically authorize the use of its free or public equivalent.

Furthermore, to maintain a clear separation between personal and Institute activities, and to prevent administrative conflicts should the Institute formally license the tool for use, GT Community Members must never use their Georgia Tech credentials or email addresses to access unapproved, public, or personally licensed tiers of these AI Tools. Even when using fully approved AI Tools, GT Community Members must always adequately safeguard information from improper disclosure.

- **The Protected Data Rule:** Inputting Protected Data into an unapproved AI Tool is strictly prohibited.
- **Procuring AI Tools for Work:** GT Community Members must not independently purchase, expense, or deploy unapproved AI Tools for work purposes. All Institute technology acquisitions require formal procurement processes to ensure mandatory cybersecurity reviews, third-party risk assessments, and contract negotiations are met—specifically to ensure vendors do not utilize Georgia Tech data to train their external AI models the data and remain the property of the Institute. https://procurement.gatech.edu/purchasing/dept-resources
- **Credential Protection for Personal Use:** If a GT Community Member personally purchases an AI Tool for their own personal use, they are prohibited from accessing or registering for that tool using their Georgia Tech organizational email addresses or login credentials.

Respecting Intellectual Property ("IP") and Confidentiality
Any AI usage that violates Institute Policies, applicable laws, regulations, intellectual property rights, contractual obligations, or employment standards is strictly prohibited. GT Community Members must exercise caution to protect both internal and external rights when writing prompts or uploading documents to AI Tools:

- **Third-Party IP:** GT Community Members must not use AI Tools to infringe upon third-party copyrights or misrepresent external work as their own. This includes avoiding the input of copyrighted materials, proprietary vendor code or information, or licensed operational frameworks into AI Tools without explicit authorization.
- **Proprietary Institute Information and Confidentiality Risks:** While the Protected Data Rule set forth above governs what data can be input into AI Tools, GT Community Members must also understand the IP risks associated with data exposure. Uploading Georgia Tech proprietary administrative information to public or unapproved AI Tools can compromise Georgia Tech's Institutional rights, competitive advantage, and legal standing. Furthermore, users must exercise caution with public AI Tools whose Terms of Service may claim ownership over uploaded materials, as this could inadvertently surrender the Institute's IP rights to a third party. Examples of proprietary information carrying high IP or confidentiality risks include unreleased financial forecasts, draft Requests for Proposals (RFPs) before they are made public, internal HR restructuring plans, or cybersecurity architecture diagrams. Exposing this information could also result in the violation of existing Institutional Non-Disclosure Agreements (NDAs) or third-party vendor contracts.

Verifying Accuracy for Business Operations
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. GT Community Members remain wholly accountable for the accuracy of any information they use, publish, or rely upon for Institute business.

Administrative factchecking requires cross-referencing AI outputs against the Institute's official systems of record. To independently verify AI-generated factual output for business operations, GT Community Members should:

- **Cross-reference hard data:** Verify financial, operational, or HR data against official enterprise platforms (e.g., Workday).
- **Verify Institutional metrics:** Check AI outputs against published reports from Enterprise Data Services or Institutional Research.
- **Consult primary sources:** Confirm original source Policy texts and supporting artifacts rather than solely relying on an AI's summary of the rules.
- **Examine for logical flaws:** Review the AI-generated content for internal inconsistencies, check for outdated information, and ensure the AI correctly understood the business context of the prompt.
- **Gain direct supervisor confirmation:** Seek approval before executing a novel or high-impact business process suggested by an AI Tool.

If a reliable source cannot be found to independently verify the information generated by the AI Tool, that information cannot be used for official work purposes.

Disclosure and Citation of AI Use
To ensure accountability and transparency in business operations, GT Community Members must appropriately disclose and cite the use of AI in administrative work products, reports, and communications.

Disclosure is required for significant AI usage, such as utilizing an AI Tool to draft a full report, conduct primary data synthesis, or generate a conceptual framing for a business proposal. Disclosure is not required for incidental AI use, such as basic spell-checking or standard search algorithms.

When disclosure is required, the following standardized statement should be included in the document's front matter or a dedicated "AI Disclosure" section:

> *"This [report/memo/document] was developed with the assistance of [AI Tool Name]. The final content has been reviewed, validated, and verified for accuracy by [Name/Role], who takes full responsibility for the content. For more information on the extent of AI usage, please contact [Primary Author]".*

When formally citing AI sources, the following citation formats provide guidance: APA, MLA, Chicago, and IEEE.

Any AI Tool deployed to interact directly with humans (e.g., customer service chatbots) must explicitly disclose its machine-generated nature at the beginning of the interaction.

5. Safeguarding Data and Preventing Exposure

This section provides the operational procedures required to protect the privacy of Georgia Tech's data and prevent the unintended exposure of Protected Data or PII when using AI Tools.

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 Data or PII.

GT Community Members and units deploying AI must implement safeguards to ensure AI Tools are not used to analyze disparate, non-sensitive data sources in a way that derives, unmasks, or exposes Protected Data or PII.

Administrative examples of prohibited exposure:

- **Employee Medical Privacy:** Cross-referencing an employee's public calendar availability with an anonymized list of departmental HR accommodation requests to deduce which specific employee has a protected medical disability.
- **Procurement and Blind Vendor Evaluations:** A GT Community Member serving on a "blind" vendor selection committee feeds the anonymized vendor proposals along with public vendor press releases into an AI Tool, asking it to deduce the identities of the bidding vendors and thereby compromising the integrity of the procurement process.
- **Donor Confidentiality:** An employee feeds an anonymized list of recent philanthropic gifts along with public county property tax records into an AI Tool to successfully unmask the identity of a high-wealth donor who legally executed an agreement for their financial support to remain anonymous.

Applying Procedural Safeguards
Even when using approved AI Tools within their approved data scope, GT Community Members must adequately safeguard data from improper disclosure. To operationalize this protection in daily workflows, GT Community Members should practice the following safeguards:

- **Data Minimization:** Only input the minimum amount of data necessary for the AI Tool to perform its required task. Do not upload entire spreadsheets or document repositories if only a single paragraph needs analysis.
- **Sanitize Prompts:** Manually review prompts and uploaded documents to ensure hidden metadata, lingering identifiers, or unnecessary Protected Data are removed before processing.
- **Respect Access Controls:** When deploying AI Tools (e.g., internal departmental chatbots or search assistants), units must ensure the system's permissions are configured so that an GT Community Member cannot use the AI to query administrative data they would not normally be authorized to view.

6. AI Tool Review and Approval

GT Community Members must not independently purchase, deploy, or use an AI Tool for Administrative and Employment Contexts until formal approval is granted and the tool is listed on an AI Register. All AI Tools are evaluated in accordance with the AI Tool Approval Standard.

Information Required for Submission

To initiate the review process, GT Community Members must gather the following information about the proposed tool before contacting their Local AI Point of Contact or using the central intake form <insert link here>:

- Tool name and Vendor
- AI Tool Type(s) and AI Model Type(s)
- Brief description of any institutional data that will interact with the tool
- Primary business purpose and organizational benefit
- Designated Georgia Tech AI Tool Point of Contact (name, unit, email)

Risk Assessments and DPIAs
The approval pathway for any proposed AI Tool depends heavily on its intended use and its associated risk profile. During the review process outlined in the AI Tool Approval Standard, proposed AI Tools will be assessed for enterprise risk with appropriate input from Institute stakeholders.

- **Formal Security Assessments:** Based on the risk profile, a tool may require formal risk and cybersecurity assessments prior to deployment.
- **Data Protection Impact Assessments (DPIAs):** If the risk-profile assessment indicates that the tool will process large volumes of Protected Data or presents significant privacy risks, the unit must formally conduct and document a Data Protection Impact Assessment (DPIA) prior to approval in accordance with USG Business Procedures Manual section 12.06.

Approval Pathways
Based on the AI Tool Approval Standard, AI Tools will be routed through approval pathways based on a primary triaging question: Is this tool intended for broad Institute use, or does it carry a high-risk profile?

- **If Yes (Institute AI Register):** AI Tools intended for broad Institute use, or those carrying higher risk profiles (e.g., processing large volumes of Protected Data), are evaluated by Institute teams using standards and an approach approved by the AI Governance Committee. If approved, they become Institutionally Approved AI Tools and are added to the Institute AI Register. If not approved, use of the tool is prohibited. Notwithstanding the foregoing, AI Governance Committee denials may be appealed to the Executive Sponsors.
- **If No (Local AI Register):** AI Tools intended for limited, unit-specific workflows with lower risk profiles may be reviewed and have approval shepherded by a designated Local AI Point of Contact. AI Tool evaluation and approval will be based on the AI Tool Approval Standard and the guiding ethical principles and safeguards. If approved, it is categorized as a Limited Use AI Tool and added to the Local AI Register. If a Local AI POC denies a tool, the decision may be appealed up the unit's administrative reporting chain. The AI Governance Committee will approve the scope of authority allowed for this pathway.
- **Intelligent Automations:** While discrete AI Tools are reviewed through the pathways above, implementations involving Robotic Process Automation (RPA), Agentic AI, or AI integrated into autonomous workflows may carry inherent enterprise risk and are governed by established Institute automation governance standards.

Periodic Review and Re-Review Requirements
The approval of an AI Tool is not permanent. Because AI technologies, vendor capabilities, and regulatory landscapes evolve rapidly, the Institute mandates both event-driven re-reviews and scheduled periodic reviews of all approved AI Tools to ensure ongoing Institute safety.

Mandatory Re-Review Triggers
Local AI Points of Contact and business unit leaders must immediately suspend use and submit an AI Tool for formal re-review if any of the following events occur:

- **Contract and Terms of Service Updates:** Significant changes to the vendor's contract language, End User License Agreement (EULA), or Terms of Service that alter how Institutional data is processed, stored, or used to train external models.
- **Material Technical Changes:** A vendor acquisition, a major software update, or the sudden integration of new AI capabilities into a previously approved standard software platform. In the event of new embedded AI features, units must disable or suspend the use of that specific new AI capability pending a formal review of that module; however, the overarching software platform remains approved for continued standard use.
- **Scope and Risk Escalation:** Any change in how the administrative unit uses the tool that would elevate its risk profile (e.g., a tool originally approved for processing public data is now proposed for processing Protected Data, or a tool approved for a single user is expanded for broad Institute use).

Periodic Review of the AI Registers
To complement case-by-case approvals, the AI Governance Program will initiate a periodic review of the Institute AI Register and Local AI Registers at least annually, or as needed due to significant shifts in USG Policy or Institutional strategy. During this review, stakeholders will evaluate whether:

- The tool’s documented business purpose and scope of approval still match its current operational use; and
- Duplicative AI Tools across the Institute can be consolidated to reduce risk, simplify support, and reduce administrative costs.

Following a periodic review, an AI Tool may be approved to continue as-is, have its approved scope updated, be forced into a formal re-review, or be formally sunset and retired (requiring the unit to execute its Business Continuity Plan).

Minimum Safeguards in Vendor Agreements
Before the purchase, deployment, or activation of AI capabilities in a supplier tool, the proposed tool will be evaluated for enterprise risk in accordance with the AI Tool Approval Standard.

For AI Tools assessed as carrying a high-risk profile or intended for broad Institute integration, Georgia Tech Procurement may require the supplier to provide a written philosophical and operational framework explaining their responsible use of AI (RAI) prior to execution (https://procurement.gatech.edu/purchasing/dept-resources). Procurement, in coordination with relevant cybersecurity and compliance stakeholders, will review this framework to confirm the agreement is consistent with the Institute's guiding principles:

- **Safeguarding Protected Data:** The agreement must protect Institute data consistent with Policy and law, strictly limiting the use of Institute data to providing the contracted service. Vendors must not train shared or foundation models on Institute data without express written permission from authorized Institute personnel. The contract must also support data return and permanent deletion upon termination or within a reasonable time period following termination.

- **Accountability:** The agreement must define vendor responsibilities for monitoring misuse, reporting issues, and contain the vendor's commitment of timely corrective action when enterprise risks or defects are identified.
- **Transparency:** The vendor must provide technical documentation about appropriate uses and known limitations and actively notify the Institute of any material changes that could affect the tool's risk profile or approved scope.
- **Accessibility:** The vendor must support accessibility requirements applicable to Institute GT Community Members and users, cooperating in remediation where needed.
- **Human Oversight and Safety:** For AI Tools used to inform official business decisions or administrative records, the tool must technically support and allow for meaningful human review and safety verifications in practice.
- **Fairness and Bias Mitigation:** The vendor must assess and mitigate material, foreseeable bias relevant to Institute business cases (such as HR or financial operations), provide high-level testing results upon request, and commit to remediation if material bias is identified in production use.
- **Safeguards against Hallucination:** The vendor must acknowledge the risk of inaccurate outputs, support and implement controls that reduce this risk (e.g., providing citations), and commit to correction when defects materially affect business outcomes.
- **Safeguards against Prompt Injections:** The vendor must implement reasonable, current protections against prompt injections, jailbreaks, and related adversarial inputs, including maintaining a robust and timely patching program for emerging threats.

The Institute shall maintain records demonstrating that agreements address these safeguards, including retaining the vendor's written RAI framework. Any exception to these provisions requires formal approval by Procurement with OGC concurrence; such decisions must be securely stored in Institute-approved repositories in accordance with USG retention schedules.

7. Prohibited Misuse and Security Incidents

This section operationalizes the Institute's strict prohibitions against the malicious or inappropriate use of AI Tools and outlines the incident response procedures required to protect Georgia Tech's operations, data, and community.

Intentional Misuse and Disciplinary Action
The intentional misuse of AI Tools is strictly prohibited. GT Community Members must not use AI to conduct activities that violate applicable laws, regulations, privacy standards, or Institute Policies. Specifically, GT Community Members must never use AI Tools to:

- **Commit Fraud:** Utilizing AI to manipulate, scam, or cheat individuals or organizations, such as facilitating financial fraud.
- **Invade Privacy:** Gathering personal information without explicit authorization to invade an individual's privacy.
- **Launch Cyberattacks:** Leveraging AI systems to facilitate malicious cyber activities, including, but not limited to vulnerability exploitation, phishing attempts, or social engineering.

- **Propagate Misinformation:** Creating and distributing false, misleading, or fabricated information.
- **Generate Discriminatory Outcomes:** Using AI systems in a way that creates bias or discriminatory situations resulting in the unequal treatment of individuals or groups.

Incident Reporting
GT Community Members are responsible for identifying and reporting AI-related risks

- **Reporting Misuse:** GT Community Members shall promptly report any suspected AI misuse or ethical concerns to their direct manager or the Institutional compliance team.
- **Reporting Security Incidents:** If the use of an AI Tool by a GT Community Member is suspected of causing a data breach, exposing Protected Data, or triggering a security incident, it must be immediately reported to the Georgia Tech Cybersecurity team in strict accordance with the Institute's Incident Response Plan.

Emergency Suspension of AI Services
To protect the Institute, the Georgia Tech or USG Chief Information Officer (CIO) or Chief Information Security Officer (CISO) may immediately suspend the use of any AI Tool that is strongly suspected to generate operational, reputational, data privacy, data confidentiality, security, or malicious consequences.

- **Cease Operation:** Upon receiving a suspension directive, GT Community Members must immediately cease all use of the specified AI Tool.
- **Investigation and Mitigation:** The Institute will conduct a formal investigation and, if appropriate, execute an approved mitigation plan before the suspended AI Tool is permitted to resume operations.

Business Continuity Planning
Because AI Tools can be suspended or experience unexpected outages, units utilizing AI Tools that support critical business functions or other types of Intelligent Automations must maintain robust business continuity plans. Administrative units must maintain documented knowledge of the underlying business processes, Policies, and procedures to ensure that human workers can successfully continue operations and achieve required results using alternate means if the AI Tool becomes unavailable.

8. Education and Awareness

This section operationalizes the Institute’s approach to AI training and awareness for GT Community Members performing administrative, operational, and business activities. It establishes the mandatory training requirements, outlines the ongoing awareness campaigns, and details the mechanisms used to track compliance and measure effectiveness.

Mandatory AI Training
All GT Community Members must complete mandatory AI ethics and safety training. This training ensures GT Community Members understand AI risks, responsible use, and compliance obligations.

- **New Hires:** Incoming employees must complete foundational AI training as part of their new hire onboarding.

- **Existing Employees:** Ongoing professional development and AI training updates will be deployed to existing staff through the Institute's established annual compliance campaigns.
- **Monitoring and Compliance:** The Institute will centrally track and monitor training progress, quiz scores, and completion status. Administrators must maintain these Learning Management System (LMS) records as formal audit evidence of completion.

Ongoing Awareness Campaigns
Due to the rapidly evolving nature of AI technologies, the Institute actively promotes AI Policies, procedures, and safety guidelines through a multi-channel ongoing awareness campaign.

- **Centralized Hub:** The Georgia Tech AI Governance website serves as the active, central repository for Policies, standards, acceptable use guidelines, and training schedules.
- **Targeted Communications:** The AI Governance Officer will coordinate with designees of Executive Sponsors and Institute Communication's staff to distribute email announcements, administrative newsletters, and internal publications (e.g., The Daily Digest) to communicate Policy updates, emerging risks, and compliance reminders.
- **Measuring Engagement:** The Institute will utilize web analytics to track visits, page views, and user engagement with AI resources to measure the reach and effectiveness of the awareness campaign.

Workshops and Professional Development
To supplement mandatory compliance training, Georgia Tech offers ongoing, operational professional development focusing on practical AI use and specific enterprise risks.

- **Workshops and Orientations:** The Institute conducts regular orientation sessions and workshops featuring approved tool demonstrations, administrative use cases, and discussions on appropriate use and risks.
- **Attendance and Feedback:** To rigorously prove compliance and measure effectiveness, the Institute implements monitoring procedures for these voluntary sessions. Administrators will collect sign-in sheets or registration logs as evidence of participation and deploy post-session feedback surveys to continuously improve the training program.

Self-Service Support Materials
To support the daily workflow of administrative units, the AI Governance Program and designated Local AI Points of Contact will create and maintain clear, accessible self-service support materials. This includes providing easily discoverable user manuals, localized operational guidance, and Frequently Asked Questions (FAQs) to guide GT Community Members on the responsible use of AI Tools and the proper handling of machine-generated content.

9. Institutional Oversight, Compliance, and Policy Maintenance

This section operationalizes the Institute's requirements for AI oversight, legal monitoring, and record-keeping, ensuring that Georgia Tech maintains strict compliance with University System of Georgia (USG) mandates and its own institutional standards.

Institutional Oversight and Dispute Resolution

The AI Governance Program provides Institute-wide coordination and alignment for AI governance. To ensure questions, disputes, and compliance concerns are handled appropriately:

- **Routing Questions and Complaints:** The AI Governance Program maintains a published process (https://oit.gatech.edu/governance/ai/) to receive and route questions and complaints related to AI Use in Administrative and Employment Contexts, coordinating adjudication and resolution through existing institutional mechanisms (e.g., unit-level leadership, Employee Relations, or the Office of the Ombuds).
- **Local AI Points of Contact:** Vice Presidents, Associate Vice Presidents, and other Institute unit leaders may designate a Local AI Point of Contact for their specific division or unit to serve as the local decision-maker for AI access. The names of these individuals must be provided to the AI Governance Program, published for the Institute community, and reviewed for accuracy at least annually.

Monitoring Legal and Regulatory Changes
Because AI regulations are rapidly shifting, the Institute maintains active legal monitoring to ensure compliance.

- **Ongoing Monitoring:** The Office of General Counsel (OGC) monitors AI-related legal, privacy, and regulatory developments on an ongoing basis. When a significant change is noted, OGC will issue an advisory memo to the AI Governance Officer and the AI Governance Committee and inform Executive Sponsors of any high-risk developments.
- **Legal Review Documentation:** To confirm that AI Tools comply with applicable privacy laws and industry standards, specific personnel must produce and maintain documented legal review memos.

Audit Records and Secure Storage
Institute leaders, Local AI Points of Contact, and compliance personnel have a responsibility to self-monitor for compliance with USG and Institute Policies.

- **Audit Trails:** Named roles and committees (e.g., the AI Governance Officer, Local AI Points of Contact) must maintain formal audit trail records sufficient to demonstrate compliance during internal or external audits and investigations. Records must be retained in accordance with applicable USG and Institute records retention schedules.
- **Secure Repositories:** All AI-related compliance records and audit trail documentation must be stored in approved secure repositories (e.g., Microsoft OneDrive, SharePoint sites, or departmental file servers).

Policy Maintenance and Review
To ensure Policies remain responsive to the evolving technology landscape, the Institute mandates strict, auditable governance review procedures.

- **Annual Review Schedule:** The AI Governance Program shall establish a regular schedule to formally review and update all institutional AI governance Policies and supporting artifacts. The Artificial Intelligence (AI) in Administrative and Employment Contexts Policy must be reviewed annually, or as needed, to reflect emerging legal, technological, or organizational changes.

- **Operational Logs and Revision Histories:** To prove active governance, the Institute must formally track and document all changes to AI governance artifacts and key meeting decisions. Administrators must maintain operational logs that document review dates, findings, and a formal change log or revision history for all AI Policies.