College of Engineering
Information Technology Purchasing Policy

Type	College IT Policy	**Policy Owner**	College of Engineering IT
Effective Date	December 2018	**Last Revised**	September 2026
Review Date	Summer 2029 with earlier review as needed	**Contact**	Diego Remolina Executive Director Academic & Research Computing diego.remolina@coe.gatech.edu

Reason for Policy

This policy establishes College-wide requirements for acquiring, approving, tracking, supporting, and disposing of Information Technology (IT) assets and services. Its purpose is to protect institutional data, maintain security and supportability, control lifecycle costs, meet licensing and contractual obligations, reduce unnecessary technology diversity, and provide reliable and consistent IT support for faculty, researchers, staff, and students.

Policy Statement

All IT-related hardware, software, services, subscriptions, cloud resources, artificial intelligence (AI) tools, vendor-hosted systems, and technology-enabled research systems must be coordinated through the College, the Unit IT group, or the individual formally designated by the Unit. These parties are collectively referred to as the IT Purchasing Team.

Individuals who are not acting on behalf of the designated IT Purchasing Team may not independently purchase or renew IT services; execute statements of work; initiate trials; provide vendor access to Georgia Tech systems, networks, devices, or data; or accept terms that create contractual, licensing, financial, data-sharing, or other institutional obligations without the required review and approval.

Scope

This policy applies to IT-related acquisitions used for College instruction, administration, research, or business, regardless of funding source, purchasing method, location, or whether the asset or service is used on or off the Georgia Tech network. It supplements applicable Georgia Tech, University System of Georgia (USG), State, federal, contractual, cybersecurity, privacy, accessibility, export-control, records, and procurement requirements.

Required Controls

Prior review and approval. The IT Purchasing Team must be engaged before quote finalization, purchase, renewal, trial, vendor commitment, system integration, network connection, or use with Georgia Tech data. Required Georgia Tech approval and signature processes must be completed before commitment or use.

Approved sourcing. State-approved and Georgia Tech-approved vendors and procurement channels must be used when they can meet the documented business, instructional, research, security, warranty, lifecycle, and support requirements. Secondary-market purchases, assembled systems, and nonstandard sources require prior written IT Purchasing Team approval.

Software, cloud, AI, and IT services. These acquisitions must be reviewed for security, privacy, licensing, accessibility, contractual obligations, data handling, technical compatibility, supportability, administrative ownership, renewal terms, and compliance with applicable OIT review processes.

Research instruments, embedded systems, cloud, and HPC. The IT Purchasing Team must be consulted before requesting final quotes, acquisition, renewal, commitment, or implementation. For high-performance computing and other significant computational needs, existing Georgia Tech shared computational resources, including the Partnership for an Advanced Computing Environment (PACE), must be evaluated

before acquiring duplicative dedicated infrastructure. When standard controls are not technically feasible, the applicable exception or risk-acceptance process must be completed before purchase or deployment.

Warranty, lifecycle, and data protection. Desktops, laptops, workstations, servers, tablets, and similar computing devices must include at least a three-year manufacturer warranty, vendor warranty, or equivalent support coverage, except as permitted under the Limited Warranty Exclusions section below, and must be planned and tracked for a minimum three-year service lifecycle. Devices capable of storing Georgia Tech data must use an approved data-protection model during repair, return, exchange, replacement, surplus, or disposal.

Inventory. IT assets must be recorded in an approved inventory or asset-tracking system, including items below the property-control threshold when tracking is necessary for security, support, warranty, licensing, lifecycle, data accountability, or disposition.

Disposition. IT equipment may not be traded in, transferred, returned, recycled, donated, surplused, or disposed of without prior IT review, data-sanitization verification, inventory reconciliation, and any required property, procurement, finance, or asset-management approval.

Limited Warranty Exclusions

The three-year warranty requirement may be waived only for low replacement-cost, limited-purpose devices for which replacement is demonstrably more economical than repair and the device does not create material security, data, compliance, accessibility, support, or operational risk. A waiver is valid only when the device class appears on a College-approved exclusion list or when a documented recommendation from the designated IT Purchasing Team is approved by the College IT policy owner or a formally authorized College-level designee. Units and local IT groups may not create blanket exclusions, lower the three-year standard, or apply waivers retroactively. Primary or general-purpose computing endpoints are not eligible solely because a selected vendor offers less than three years of coverage.

Exceptions, Enforcement, and Guidance

Exceptions to Institute, USG, cybersecurity, privacy, contractual, regulatory, or procurement requirements must follow the applicable governing process. Exceptions to College requirements must be documented and approved by the College IT policy owner or a formally authorized College-level designee before purchasing, renewal, deployment, continued use, or disposition. Unauthorized acquisitions may be denied support or network access, suspended, canceled, replaced, or referred for procurement, cybersecurity, privacy, finance, or leadership review.

Implementation details, review criteria, examples, and procedures are provided in the COE IT Purchasing Policy Companion Guide. The Companion Guide supports this policy by providing further detail but does not reduce or supersede its requirements.

COE IT Purchasing Policy Companion Guide

Implementation guidance, decision criteria, and examples

1. Purpose and Use of This Guide

This guide explains how to apply the COE IT Purchasing Policy while keeping the governing policy concise. It provides implementation details for purchasers and IT reviewers. If this guide conflicts with the policy or a higher-level requirement, the policy or higher-level requirement controls.

- Engage the designated IT Purchasing Team before requesting or negotiating quotes whenever product selection, licensing, warranty, security, data handling, vendor terms, accessibility, integration, lifecycle, or supportability may be affected.
- Use Workday, ticketing, procurement, inventory, or equivalent systems to retain the request, funding approval, IT review, warranty and lifecycle decision, required institutional approvals, and final purchase record.
- Verbal discussion, informal awareness, or after-the-fact notice does not constitute approval unless the responsible approving authority documents acceptance.

2. Intake and Review Checklist

- Business, instructional, or research need; alternatives considered; expected service life; and total cost of ownership.
- Funding source, fund-owner authorization, vendor, procurement channel, tax-exempt status, and signature-authority requirements.
- Security, privacy, data classification, contractual, accessibility, export-control, records, and compliance considerations.
- Hardware compatibility, operating system, endpoint management, network, integration, administrative ownership, and support model.
- Software licensing, user counts, renewal terms, auto-renewal, data portability, administrative ownership, and termination obligations.
- Warranty duration and response level, accidental-damage needs, media-retention or sanitization method, and planned lifecycle.
- Inventory, delivery, deployment, support assignment, replacement funding, surplus, and disposition plan.

3. Hardware Sourcing and Assembly

Standard office, administrative, instructional, and general-purpose computers shall be purchased through approved channels and must support institutional security, inventory, warranty, lifecycle, and support requirements.

Before approving secondary-market, used, outlet, auction, assembled, or component-based systems, the IT Purchasing Team should document warranty status, counterfeit risk, compatibility, security exposure, supportability, expected lifecycle, inventory requirements, data-protection implications, funding restrictions, and approved-vendor alternatives.

End users, PIs, laboratory personnel, and administrative staff may not independently procure parts and assemble IT systems without prior approval. Assembled systems must follow applicable counterfeit-part, procurement, property, inventory, and fabricated-property requirements.

4. Research Instruments and Embedded Computing

Instrument-connected and embedded systems may have specialized vendor, operating-system, timing, or research constraints. IT review should occur before the quote or purchase commitment so that security, networking, data protection, remote vendor access, lifecycle, support, and exception requirements can be addressed without disrupting the research objective.

Where standard controls cannot reasonably be applied, the purchaser and IT Purchasing Team should document the limitation, alternatives considered, compensating controls, support expectations, responsible party, and replacement or review date. Institute-level exceptions must use the applicable Institute process.

5. Software, SaaS, Cloud, AI, and IT Services

Software and technology services include perpetual licenses, subscriptions, SaaS, cloud resources, hosted applications, managed services, support services, AI tools, AI-enabled services, and vendor access to systems or data. Free trials and no-cost services are in scope when they create terms, data-handling, integration, support, accessibility, or security obligations.

The IT Purchasing Team should coordinate applicable reviews with Procurement and Business Services, Georgia Tech Research Corporation, Legal Affairs, Cyber Security, data stewards, accessibility reviewers, records officials, or other responsible offices. Only individuals with applicable signature authority may accept terms or commit Georgia Tech.

AI acquisitions and uses must follow current Georgia Tech policies, standards, guidance, approval requirements, data-protection requirements, and third-party risk-review requirements. Approval status, data classification, intended use, integration, administrative ownership, and renewal responsibility should be documented.

6. Warranty, Support Coverage, and Lifecycle

Next-business-day or equivalent business support should be selected when available and cost-effective. Warranty coverage should, where practical, align with the expected service life of the system so that support does not expire well before the planned replacement date.

Five-year warranty or equivalent support coverage and a five-year planned lifecycle are strongly recommended for servers, high-end or specialized workstations, shared research systems, and any computing system with a total acquisition cost of $3,000 or greater. The IT Purchasing Team may require coverage beyond three years when justified by replacement difficulty, operational importance, research impact, system cost, supportability, or data-protection requirements.

Additional coverage, including accidental-damage protection, may be required or recommended for portable, costly, difficult-to-replace, operationally critical, research-critical, shared, or otherwise high-risk devices.

The warranty requirement is separate from media protection. Devices that may store Georgia Tech data must have an approved method for protecting data when the device is repaired, replaced, exchanged, or returned.

7. Low Replacement-Cost Warranty Exclusion Process

The limited exclusion exists only to avoid purchasing warranty coverage when a device is economically treated as replace-on-failure. It must not become a route for purchasing ordinary computers with inadequate warranties.

A device may qualify only when all applicable criteria are satisfied:

- Replacement is reasonably expected to cost less than warranty coverage plus likely repair and administrative costs.
- The device is limited-purpose and is not the user's primary or general-purpose computing endpoint.
- Loss of the device would not materially interrupt instruction, research, administration, safety, or critical operations.
- The device does not store protected, regulated, confidential, sensitive, or unpublished institutional data, or an approved design prevents local storage of such data.
- The device does not create a material cybersecurity, accessibility, compliance, licensing, integration, or support burden.
- A documented replacement plan and responsible funding source exist.
- The device class is on a College-approved exclusion list, or the designated IT Purchasing Team recommends an item-specific waiver and the College IT policy owner or authorized College-level designee approves it before purchase.

Examples of device classes that may qualify. College-approved exclusion classes may include Raspberry Pi, Arduino, equivalent single-board computers, microcontrollers, development boards, embedded-computing devices, and other low-cost, limited-purpose devices reasonably treated as replace-on-failure.

Tablets with a total configured acquisition cost below $1,000 may qualify when used as secondary, shared, kiosk, field, laboratory, display, testing, or other limited-purpose devices and all other exclusion criteria are met. The configured cost includes storage, memory, and factory-configured options. Tablet-style or detachable computers used as primary or general-purpose computers do not qualify. Tablets costing $1,000 or more remain subject to the three-year warranty requirement unless a specific College-level exception is approved.

An example device class is not automatically exempt. The IT Purchasing Team may require warranty coverage based on cost, intended use, data-storage capability, operational importance, replacement difficulty, supportability, or other risk considerations.

Waivers must identify the item or approved device class, rationale, purchaser, responsible support group, data-handling limitation, approval date, and any expiration or review date. Units may not infer additional excluded device classes from prior approvals.

8. Data Protection During Warranty Service and Return

Where storage media can be removed and retained, select a manufacturer or vendor program that permits Georgia Tech to retain failed media, or use another approved data-protection method. If no approved method is available, a device containing Georgia Tech data must not be transferred with storage media intact.

Devices with soldered or otherwise non-removable storage do not require a media-retention warranty solely because the storage cannot be removed. Such devices must use full-disk encryption consistent with applicable Computer Security Standard requirements, appropriate recovery-key management, and an IT-verified wipe, erase, or sanitization process where supported before vendor return, exchange, repair, replacement, surplus, or disposal.

A factory reset or user-initiated wipe alone does not establish compliance. IT must verify the sanitization result, remove the device from management systems, reconcile inventory, and document the approved disposition or transfer.

9. Inventory and Lifecycle Management

Inventory requirements are not limited to capital-property thresholds. Track devices when necessary for cybersecurity, endpoint management, warranty, licensing, location, support assignment, lifecycle, data accountability, and disposition.

Recommended inventory fields include purchaser, funding source, owner, assigned user, location, serial number, asset tag, warranty dates, warranty-waiver status, media-protection method, planned replacement date, operating system, management status, lifecycle status, support group, and disposition status.

The minimum lifecycle planning baseline for computing devices is three years. Standard desktops, laptops, and general-purpose endpoints will often remain in service for three to five years when they continue to meet security, reliability, supportability, and business needs. Servers, high-end or specialized workstations, shared research systems, storage systems, and systems costing $3,000 or more should be planned for a five-year lifecycle when practical and when manufacturer support, security requirements, and operational needs permit.

Continued use beyond the planned lifecycle is permitted when the system remains secure, supportable, reliable, and suitable for its purpose; the planned lifecycle is a budgeting and support baseline, not an automatic retirement date. Reliance on IT equipment more than ten years old is considered high risk because of security, supportability, reliability, compatibility, and replacement-part limitations and should be avoided whenever practical.

Hardware, software, operating systems, firmware, and services that reach end-of-life or end-of-support may be required to be upgraded, replaced, isolated, restricted, or retired. Continued use may require risk acceptance, compensating controls, limited support, network restrictions, and a defined review or replacement date.

10. Trade-In, Return, Recycling, Surplus, and Disposal

Trade-in or return of institutional equipment is generally prohibited unless reviewed and approved in advance by IT and all applicable property, procurement, finance, or asset-management personnel. The review must address inventory, ownership, financial treatment, device-management removal, data sanitization, and approved disposition.

Unauthorized transfer, trade-in, return, recycling, surplus, or disposal can create data exposure, financial loss, loss of asset accountability, audit findings, security risk, or regulatory and policy noncompliance.

11. Cloud and High Performance Computing

The IT Purchasing Team must be consulted before purchasing, renewing, deploying, or materially changing cloud, hosted research computing, high-performance computing, or clustered computing resources. For HPC and significant computational needs, existing Georgia Tech shared resources, including the Partnership for an Advanced Computing Environment (PACE), must be evaluated before duplicative in-house resources are acquired. Additional information on PACE participation is available at: https://pace.gatech.edu/participation

A standalone accelerated-computing server is not treated as a cluster solely because of its processor type. When multiple systems will operate as a single computing resource, or an in-house cluster is proposed, complete a documented technical, business, security, data, network, lifecycle, and supportability review before purchase or deployment.

12. Donations

Consult the IT Purchasing Team before accepting donated hardware, software, subscriptions, services, AI tools, or cloud resources. Donations remain subject to security, privacy, licensing, contractual, accessibility, inventory, data-protection, supportability, and lifecycle review. Coordinate recognition and acceptance with the assigned Development Officer and applicable purchasing or institutional offices.

13. Excluded Low-Risk Items

Low-risk accessories may be purchased directly when they do not independently connect to a network, store institutional data, require software or licensing review, provide vendor access, or trigger another review requirement. Typical categories include ordinary cables, adapters, power strips, landline or cordless phones, privacy screen filters, and basic removable media used only for data permitted by applicable Georgia Tech requirements.

Specialized networking, fiber, high-speed interconnect, laboratory, building, life-safety, storage, or cellular devices are not automatically excluded. The IT Purchasing Team may require review whenever compatibility, safety, security, data protection, accessibility, supportability, procurement, warranty, lifecycle, or inventory risk exists.

14. Exceptions and Documentation

A College exception request should document the business or research need, item or service, funding source, data classification, security and privacy impact, accessibility, supportability, warranty, lifecycle, cost, alternatives considered, compensating controls, responsible party, approval duration, and review date.

Local IT may recommend an exception but may not independently approve one that reduces College-wide warranty, lifecycle, standard-computing, data-protection, inventory, or disposition requirements. College approval does not waive any higher-level requirement.

15. Quick Decision Path

1. Is the acquisition IT-related, or does it store, process, transmit, access, or support Georgia Tech data or operations? If yes, engage the designated IT Purchasing Team.
2. Before any commitment, determine required procurement, signature, security, privacy, data, accessibility, licensing, contractual, and institutional reviews.
3. For computing devices, apply the three-year minimum warranty/support requirement and the three-year minimum lifecycle planning baseline. Use the limited warranty exclusion only for qualifying low replacement-cost, limited-purpose devices.
4. For servers, high-end or specialized workstations, shared research systems, and computing systems costing $3,000 or more, strongly prefer five-year warranty/support coverage and a five-year planned lifecycle.
5. Select and document the warranty-service data-protection method, then record approval, purchase, warranty, inventory, support ownership, lifecycle, and disposition information in the appropriate system.

Document Control and Revision History

This page forms part of the official policy record. It documents the current controlled version and the revision history based on the available 2018, 2023, and 2026 policy documents.

Current Document Control

Document Title	College of Engineering Information Technology Purchasing Policy and Companion Guide
Current Version	2.0
Status	Active
Original Effective Date	December 2018
Current Revision Date	September 2026
Next Review	Summer 2029, with earlier review as needed
Policy Owner	College of Engineering IT

Review and Publication Record

Action	Periodic review and comprehensive revision of an existing policy
Reviewed By	College of Engineering IT
Review Completed	September 2026
Approval Record	Policy-owner review; no separate signature required for this periodic review

Revision History

Version	Revision Date	Review Type	Summary of Changes	Record
1.0	December 2018	Initial publication	Established coordinated IT purchasing, sourcing, lifecycle, assembly, warranty, donation, and exclusion requirements.	Original
1.1	July 2023	Periodic revision	Updated ownership and review data; added software review, asset tracking, off-site insurance, cloud/HPC, PACE, and removable-media guidance.	Revised
2.0	September 2026	Comprehensive revision	Separated policy from companion guidance; expanded services, cloud, AI, warranty, lifecycle, inventory, data protection, disposition, exceptions, and documentation.	Current