UNIVERSITY OF
South Carolina
Molinaroli College of
Engineering and Computing

POLICY: **IT Equipment Management**

DATE: **April 22, 2026**

This policy applies to all units within the Molinaroli College of Engineering and Computing (MCEC). The College policy is subordinate to related policies outlined in Information Technology Policies and Guidelines. In cases of inconsistencies between this policy and the university, state, or federal policies, the university, state, or federal policy rules are the final authority.

I. Definitions:

University Technology Equipment: Any computing device or peripheral funded by, acquired through, or connected to University operations. This includes equipment purchased with University funds or through grants awarded to University personnel, which remains University property. Examples include, but are not limited to, desktop and laptop computers, monitors, chargers, docking stations, printers, and other IT devices.

ITS: Information Technology Services

ITS Staff: Member of the MCEC staff in the college central Information Technology Service (ITS) department and Department of Information Technology (DoIT) staff.

Unused Devices: University owned devices that are not actively in use for university-related work, including disconnected or stored equipment in private offices or labs, devices assigned to former personnel, or legacy equipment preserved for data retention but no longer actively used.

End-of-Term Equipment: Equipment originally assigned to individuals whose affiliation with the University has ended (graduation, separation, end of assignment, etc.).

Research Computing Infrastructure (RCI): The comprehensive research technology ecosystem provided by the University of South Carolina Division of Information Technology Research Computing program. RCI includes computing hardware, research data storage systems, networking, software environments, security controls, and professional support services designed to enable, manage, and sustain advanced research activities.

High Performance Computing (HPC): A component of the University's Research Computing Infrastructure consisting of centralized, shared high-performance computing

resources. These resources include computing clusters, research computing nodes, GPU resources, high-memory systems, and other specialized computing platforms designed to support computationally intensive research workloads.

Research Data Storage: Centralized, managed storage services provided through the University's Research Computing program for the storage, protection, backup, and lifecycle management of research data.

High-End Workstation: A desktop-class computing device intended for advanced research computing workloads, typically including high-core-count CPUs, GPUs, large memory configurations, or other specialized hardware, and costing more than the average computer purchase price for general-purpose office use within MCEC. Total acquisition cost includes required peripherals and accessories necessary for operation.

BYOD (Bring Your Own Device): Personally owned computing devices such as laptops, tablets, or smartphones that are used to access University networks, systems, or data for academic, research, or administrative purposes. BYOD devices are not managed by ITS and are subject to separate security and usage guidelines as established by University policy.

Obsolete Technology: Any device or system that can no longer meet one or more of the College's operational requirements, including: (a) inability to run an operating system version currently supported by the OS vendor; (b) failure to meet College and University security compliance standards; (c) failure to achieve minimum performance thresholds necessary for its assigned role; or (d) hardware condition where repair cost exceeds the value of replacement. Obsolete technology is not eligible for new deployment and must be decommissioned or repurposed in accordance with this policy. Exceptions can be made for systems running required research instruments for which there is no reasonable upgrade path.

II. Purpose:

The purpose of this policy is to establish clear standards and expectations for the use, acquisition, and management of technology resources within MCEC and, in doing so, to strengthen the College by improving the reliability and security of IT systems, reducing avoidable inefficiencies and duplication, supporting long-term sustainability, managing total cost of ownership across the College, and ensuring compliance with security, procurement, and data governance standards. Ideal IT outcomes are defined not

only by immediate functionality, but by long-term maintainability, security, scalability, and institutional resilience. ITS will partner with faculty and staff to deliver solutions that meet research and instructional needs while promoting the College's long-term operational goals.

III. Policy:

a. IT Procurement

To ensure compatibility and alignment with existing technology infrastructure and organization goals, only authorized ITS staff may order IT hardware, peripherals, software, infrastructure components, and related technology systems. ITS staff will work with faculty and staff to coordinate technology purchases. ITS will evaluate functional requirements, ensure compatibility with existing infrastructure, confirm security and compliance alignment, optimize total cost of ownership, and ensure adherence to University procurement policies.

b. Computer and Systems Issuance

In alignment with strategic organization goals and efficiencies, ITS will issue computing systems based on documented role requirements and operational needs. **ITS will not issue multiple computers when fewer systems can adequately meet the functional requirements.** Each issued system introduces maintenance, licensing, security, and lifecycle management. ITS will seek to provide support to meet all work requirements while limiting overhead in the form of additional maintenance time, administrative labor, licensing obligations, and associated financial costs to the College.

c. Printer Standards

MCEC operates under a shared printer model to improve cost efficiency, streamline supply management, enhance serviceability, and strengthen network security. As of January 2026, individual desktop printers are being phased out. Existing individual desktop printers will be supported only until replacement is required. When replacement becomes necessary, printers will be transitioned to the shared device model to ensure consistent support standards, reduced duplication of resources, and more effective long-term management of printing infrastructure. Exceptions to this transition may be made only in very few instances and must be approved by the Assistant Dean of Business Operations.

d. Research and High-Performance Computing

MCEC promotes the responsible and strategic use of centralized Research Computing Infrastructure (RCI) and Research Data Storage resources to maximize institutional investment, reduce duplication,

protect research data, and ensure sustainable, enterprise-grade support for advanced research activities. Before purchasing high-end computing systems, faculty must consult with ITS and University Research Computing to determine whether existing High-Performance Computing (HPC) resources can meet the research need, evaluate cost-effectiveness and scalability, avoid unnecessary duplication of specialized systems, and ensure that facilities, power, cooling, and security requirements are properly addressed. To ensure integrity and availability of research work, data must be stored in professionally managed, secure, and scalable centralized storage environments; faculty may not purchase standalone Network Attached Storage (NAS) systems or independent research data storage appliances for research purposes, and all significant research data storage needs must utilize centrally managed Research Data Storage services. Centralized storage ensures secure, access-controlled environments, and redundancy, compliance with University data governance and information security policies, and alignment with sponsored research obligations. When feasible, high-performance computational workloads will utilize centralized HPC resources to strengthen reliability, enhance security, and align research growth with long-term infrastructure planning across the College, while faculty remain responsible for understanding and complying with sponsor-specific retention and regulatory requirements.

e. Wall Mount Displays

To ensure safety, consistency, and long-term reliability across MCEC facilities, all television displays and screens must be ordered and installed through ITS. Centralizing this process allows the College to maintain uniform technical standards, ensure proper mounting and structural integrity, route cabling cleanly through walls and ceilings where feasible, and provide all necessary hardware, materials, and professional installation services. This approach reduces safety risks, avoids inconsistent installations, protects building infrastructure, and ensures systems are properly integrated with existing technology environments. The requested unit will share the cost of the television and installation, which includes all required labor and associated materials. MCEC ITS will work with USC facilities to ensure that proper environmental surveys are conducted before performing installs that could release asbestos, lead, or other hazardous materials. Unauthorized installations are not permitted, as centralized coordination ensures quality control, operational sustainability, safety, and alignment with the College's long-term facilities and technology goals.

f. Equipment Ownership, Care, and Accountability

All MCEC IT equipment remains University property and must be used primarily for University-related purposes in support of the College's academic, research, and administrative mission. To protect institutional resources and ensure long-term operational effectiveness, all equipment will be inventoried, managed, and tracked by ITS to maintain accurate records, enable efficient support, and support responsible lifecycle planning. IT equipment cannot be introduced into the College environment in a manner that bypasses ITS and ITS responsibility for equipment management.

Employees are responsible for the care, physical protection, secure and appropriate use of assigned equipment, and for promptly reporting any issues so that disruptions can be minimized and risks addressed quickly. Supervising faculty and staff are accountable for ensuring that students and student workers adhere to all standards. This structured stewardship model promotes accountability, protects shared investments, reduces loss and inefficiency, and supports the College's goals of reliability, sustainability, and responsible resource management. **Prompt reporting of lost, stolen, or damaged equipment to MCEC ITS within 24 hours is required and enables rapid response and risk mitigation that protects both individual users and the broader College community.** Hardware modification, repair, or upgrades must be performed or approved by ITS.

g. Security and Configuration Requirements

To protect the integrity, availability, and confidentiality of MCEC's technology environment, all devices connected to University networks must meet University security standards, including the use of vendor-supported operating systems, current security patches, and approved endpoint protection tools. All systems users must use password protection. Systems with direct remote access from outside University networks also require multi-factor authentication (MFA). Single-Sign On (SSO) integrated into existing University authentication service is required for systems with direct remote access whenever possible. Exceptions for SSO will be made when systems are critical to the core mission of the college and system integration is not possible. Data and projects with regulatory requirements will be subject to additional security controls. These standards strengthen the College's security posture, reduce institutional risk, and support the continuity of teaching, research, and administrative operations in alignment with MCEC's strategic goals.

h. Software Licensing

To protect the College's operational stability, legal compliance, and security posture, only properly licensed and authorized software may be installed on University-owned devices. Software must be obtained directly from the original developer, an authorized vendor, or a known and trusted institutional distribution source. Pirated software, unauthorized copies, or software obtained from unverified or untrusted sources is strictly prohibited. Operating systems and applications must remain updated with current security patches to reduce vulnerabilities and ensure reliable performance, with limited exceptions permitted when documented research requirements necessitate specific software versions and appropriate risk mitigation measures are in place. Unsupported and obsolete operating systems must not be installed, as they introduce security and compatibility risks that affect the broader technology environment. Adhering to these standards safeguards institutional resources, supports research continuity, reduces exposure to licensing and cybersecurity risk, and advances MCEC's goals of maintaining a secure, sustainable, and professionally managed technology infrastructure.

i. Lifecycle Management

MCEC follows a condition-based lifecycle and replacement model to ensure that technology resources remain secure, reliable, and aligned with the College's operational and financial goals, rather than relying on age alone as the determining factor for replacement. Devices must be retired when they can no longer run a vendor-supported operating system, fail to meet security compliance standards, do not satisfy performance requirements necessary for assigned roles, or require repair costs that exceed replacement value. For planning purposes, laptops generally have an anticipated useful life of approximately five to six years, and desktops six to eight years, provided they continue to meet operational and security standards. Devices approaching obsolescence within one year will be evaluated by ITS for phased replacement to prevent disruption and avoid emergency expenditures; however, this does not guarantee replacement, and devices that remain functional and sufficient for business needs will continue in use. This structured lifecycle approach promotes fiscal responsibility, reduces downtime, strengthens cybersecurity, and supports the College's long-term sustainability and strategic planning objectives.

j. Obsolete Technology and Unsupported Systems

To protect the security, stability, and long-term viability of the College's technology environment, all systems must run current, vendor-supported operating systems. **Obsolete systems must not connect to campus wired or wireless networks and will receive limited or no IT support, as unsupported platforms introduce security vulnerabilities, compatibility issues, and operational risk that affect the broader community.** In limited cases where research systems cannot meet current operating system requirements, those systems may operate offline only following ITS review and documented exception to ensure risks are appropriately managed. Additional obsolete systems may not be introduced into the environment, and ITS will work collaboratively with researchers to prevent dependency on unsupported technologies that could disrupt research continuity or expose the College to avoidable risk. This approach strengthens institutional resilience, safeguards shared infrastructure, and advances MCEC's goals of maintaining a secure, sustainable, and professionally managed technology ecosystem.

k. Device Storage, Redeployment, and Retention

To ensure responsible stewardship of institutional resources and maintain accurate technology inventory and security controls, unused devices may not be retained in private offices or laboratories without prior agreement and ITS approval. **Equipment that is no longer in active use must be returned to ITS for redeployment, secure storage, or proper disposal so that resources can be efficiently reassigned; storage costs minimized, and unnecessary duplication avoided.** When devices are disposed of, ITS will use a decommissioning process that includes secure erasure in accordance with University data protection standards to protect sensitive information and reduce institutional risk.

l. Equipment Return

To maintain accurate inventory, protect institutional data, and ensure responsible stewardship of College resources, all MCEC equipment must be returned at the end of employment, contract, or academic assignment. Prompt return of equipment enables timely redeployment, lifecycle planning, and continuity of support for the broader community. If equipment was taken off campus without pre-arranged return shipping, the employee is responsible for shipping costs to ensure that institutional resources are recovered without additional expense to the College. Users must remove personal files prior to return to protect individual privacy. This structured return process safeguards University property, strengthens data protection practices, and supports MCEC's goals of operational efficiency, accountability, and long-term sustainability.

m. Equipment Deployment and Location

To ensure security, reliability, and consistent support across the College, desktop computers and non-mobile IT equipment may not be moved or relocated without ITS involvement. ITS staff are required to maintain accurate IT equipment inventory. Accurate IT equipment inventory allows staff to respond quickly to support and security concerns. IT equipment must remain in USC-owned buildings unless an exception is granted by MCEC ITS staff. Research field work may at times require non-mobile equipment to be located off-campus. In such cases, ITS staff must be notified in advance to ensure appropriate tracking and support. Centralizing fixed equipment within approved facilities allows for proper environmental controls, network management, physical security, and coordinated support, all of which reduce operational risk and improve service continuity. Individually managed servers or infrastructure located outside approved facilities are not permitted, as decentralized systems create avoidable security, compliance, and maintenance challenges that affect the broader technology environment. Laptop and Laptop accessories may be issued for approved off-campus use to support flexible work and research needs. These deployment standards strengthen infrastructure integrity, protect shared resources, and advance MCEC's goals of sustainability, security, and operational excellence.

n. Personally Owned Devices (BYOD)

Use of personally owned devices (BYOD) is voluntary, and University-owned equipment is preferred when feasible to ensure consistent security, support, and lifecycle management across the College. When personal devices are used to access University systems, users must maintain appropriate security controls and updates, protect University data, and use multi-factor authentication (MFA) and VPN where applicable to safeguard institutional resources. Personally owned devices may connect to campus wireless networks but must not connect to wired networks, and sensitive or regulated data must not be stored or processed on personal devices to protect compliance obligations and reduce institutional risk. **ITS does not provide repair or troubleshooting support for personally owned devices, ensuring that College resources remain focused on institutionally managed systems. Personally owned non-mobile devices such as desktop computers and printers are not permitted to**

be used in college facilities, as they introduce unmanaged infrastructure, increase network and security risks, and complicate asset tracking, support, and lifecycle management. Upon separation from the University, all University-related data must be removed or transferred from personal devices. These standards promote flexibility while protecting shared infrastructure, strengthening data security, and advancing MCEC's goals of operational resilience, compliance, and responsible technology stewardship.

IV. Statement of Compliance:

All users of University technology resources are expected to follow this policy. Compliance is essential to maintaining the efficient and safe functionality of technology systems and network resources.

Note: In cases of non-compliance, individuals may be subject to disciplinary action as outlined in the IT Responsible Use of Data, Technology, and Credentials Policy (UNIV 1.52), Faculty Progressive Discipline (ACAF 1.82), and/or HR Disciplinary Action and Termination Cause (HR 1.39).

V. Related University, State, and Federal Policy Documents and Guidance:

- USC Policy IT 1.00 Information Technology Procurement
  https://www.sc.edu/policies/ppm/it100.pdf

- USC Policy IT 3.00 Information Security
  https://www.sc.edu/policies/ppm/it300.pdf

- USC Policy UNIV 1.52 Responsible Use of Data, Technology, and User Credentials
  https://www.sc.edu/policies/ppm/univ152.pdf

- USC Policy UNIV 1.51 Data and Information Governance
  https://www.sc.edu/policies/ppm/univ151.pdf

- USC Policy RSCH 1.05: Data Access, Retention, and Ownership
  https://www.sc.edu/policies/ppm/rsch105.pdf

- USC Policy ACAF 1.82 Faculty Progressive Discipline
  https://www.sc.edu/policies/ppm/acaf182.pdf

- USC Policy HR 1.39 Disciplinary Action and Termination for Cause
  https://sc.edu/policies/ppm/hr139.pdf