Georgia College & State University
Information & Instructional Technology

Faculty and Staff Equipment and Software Policy

Established 2004

Record of Modifications

Contents

1 INTRODUCTION 4
1.1 PURPOSE 4
1.2 ASSOCIATED STRATEGIC PLANNING ITEMS 4
1.3 UNIVERSITY RIGHTS & REMEDIES 5
1.4 DEFINITIONS 6
2 PURCHASING 7
2.1 PRE-PURCHASE REVIEW REQUIREMENTS 7
2.2 RECEIVING AND INVENTORY 7
2.3 SOFTWARE 7
2.4 HARDWARE 8
2.5 REPLACEMENT CYCLE 8
3 OPERATIONAL PRACTICES 9
3.1 DEPLOYMENT PROCEDURES 9
3.2 NEW FACULTY 9
3.3 REDEPLOYMENT 9
3.4 SECURITY 9
3.5 SERVE HELPDESK 10
3.6 ACCEPTABLE USE 11
4 RELATED DOCUMENTATION/SOURCES 13
4.1 THE GC&SU TECHNOLOGY SECURITY INCIDENT RESPONSE PLAN 13

1 Introduction

1.1 Purpose

This document provides a Georgia College & State University (GC&SU) policy framework which should be utilized to assure appropriate and equitable issuance to staff and faculty of basic technology equipment. This policy is a guide for administrators, faculty, and staff for the acquisition, utilization and support of computer and peripheral needs and basic network access, as well as personal responsibilities of the employee and supervisor. Through this policy GC&SU strives to maintain a minimum acceptable level of support allowing faculty and staff to meet their job responsibilities.

1.2 Associated Strategic Planning Items

GC&SU Mission Statement, Vision statement, the 5 strategic goals

(http://info.gcsu.edu/intranet/ippa/plan.htm)

I. Engage the University community in creating a learning environment for accomplishing our liberal arts mission.
II. Develop attitudes among administration, faculty, students and staff that foster trust and respect.
III. Promote intellectual excellence in faculty and students.
IV. Enhance student-centeredness.
V. Link resources to the Mission of the University.

GC&SU Technology Plan Objective 1, 2, 3, & 4

1. Acquire and maintain technology crucial to creating an exemplary learning environment.

2. Establish and maintain reliable, responsive, and competent technology support for faculty, staff, and students.

3. Establish and maintain computer technology laboratories, discipline specific teaching laboratories, electronic classrooms, electronic library resources/services, CEPS in keeping with enhanced learning necessary to achieve the University mission.

4. Engage faculty and students as a "community of learners" able to use technology to create learning experiences that encourage meaningful interaction between faculty and

students, as well as students to students and students to staff, access to information and academic services.

5. Implement a governance structure that accountably promotes the best use of technology resources, and adherence to ethical/ legal uses of technology.

USG IIT Strategic Plan Goal 1, 2, 3, 4 & 5

http://www.usg.edu/usgweb/iitsp/documents/docs/Learning_Without_Limits_4_1_02.pdf

Goal #1 Enhance Student Learning

Goal #2 Expand Reliable and Secure Access to Information and Services

Goal #3 Increase Customer Focus

Goal #4 Ensure Continuous Innovation

Goal #5 Effectively and Efficiently Plan and Manage IIT Operations

1.3 University Rights & Remedies

A violation of this policy may subject the offender to dismissal or other sanctions after compliance with procedural due process requirements. Authorized users, when using the University's computing equipment or personally owned computers (POC) connected to the GC&SU network are required to comply with any related policies set forth by GC&SU and the University System of Georgia (USG). In addition, they are required to abide by any local, state or federal laws. The University reserves the right to amend these conditions and policies at any time without prior notice. In order to protect the integrity of GC&SU's computing resources and authorized users against unauthorized or improper use of those resources the University reserves the right to:

- Limit or restrict any individual's use of; and to inspect, copy, remove or otherwise alter any data, file, or system resource that may undermine the authorized use of any computing resource.
- Disclaim responsibility for loss of data or interference with files resulting from necessary efforts to maintain the privacy and security of those computing facilities.
- Take appropriate legal action necessary to protect GC&SU and its computing resources.

- Enforce the Misuse of State Property policy as stated in Georgia Department of Human Resources, Policy #1205 that can be located at http://www.dhr.state.ga.us/Departments/DHR/1205.pdf

1.4 Definitions

For the purpose of this policy, the following definitions are set forth:

- **University Property:** Any equipment or software secured through the university purchasing process regardless of source of funds.
- **Authorized Use:** Any scholarly activity, University business activity, or personal activity by an authorized user that does not violate any law or University policy.
- **Authorized Users:** Faculty, administrative personnel, staff currently employed by GC&SU, currently enrolled students, or other individuals as approved by GC&SU Chief Information Officer.
- **Computing Resources:** Refers to and includes any and all forms of computer-related equipment, tools and intellectual property. This includes computer systems, personal computers and computer networks and all forms of software, firmware, operating software and application software, owned by the University or under the University's possession, custody or control.
- **Employee:** Any administrative personnel, faculty, or staff member employed by GC&SU.
- **Personally Owned Computer (POC)**: Any computer owned by an employee.
- **Office of Information and Instructional Technology (OIIT)**: The GC&SU department headed by the Chief Information Officer.

2 Purchasing

2.1 Pre-purchase Review Requirements

The purchase of all GC&SU technology equipment and software, regardless of the source of funds, shall be reviewed by the GC&SU Office of Information and Instructional Technology. The Vice Chancellor/CIO of the University System of Georgia has delegated “approval authorization” to the GC&SU Chief Information Officer (CIO) for purchases not on State of Georgia Contract that do not exceed $50,000 and for those on State of Georgia Contract that do not exceed $100,000. Items exceeding those levels must be submitted to the Vice Chancellor’s office for approval. To assure sound purchasing, supportability, appropriate pricing and assure for security of the University’s resources, GC&SU requires that all items be reviewed. Thus there is no minimum allowable independent purchase. Under these guidelines, technology equipment, software, maintenance or licenses shall not be purchased with departmental Purchasing Cards. The GC&SU OIIT staff can help expedite critical items by using the University’s Purchasing Card and billing purchases to departmental accounts.

2.2 Receiving and Inventory

All technology purchases shall be delivered to the Office of Information and Instructional Technology for examination, inventory and scheduled deployment except where financial or scheduling consideration would dictate another approach.

2.3 Software

GC&SU abides by the guidelines and policies of the Business Software Alliance.

http://www.bsa.org

The University considers software piracy a serious offense. Only licensed, genuine software will be installed on University owned equipment. Waivers may be granted by the CIO for public domain and faculty developed software. In addition, individuals using personal owned computers on the campus shall be able to provide license documentation if needed. In order to be able to comply with annual audits, OIIT shall maintain the licensing documentation and original media of purchases. OIIT will be responsible for purchasing campus licenses for applications that are universally appropriate and included as part of the standard configuration. Funding for individual and small group licenses shall be the responsibility of the purchasing entity. Software purchased through university purchasing shall not be installed on personally owned computers without approval by the OIIT. If a license agreement is not renewed, the application, if required by the agreement, shall be removed from the computer on the expiration date of the license.

2.4 Hardware

The University, through the OIIT, shall provide each faculty and staff member with a standard configuration of equipment and software. The current standard configuration describing the adopted platform and software is available on the GC&SU Technology Resources WEB page.

http://technology.gcsu.edu

The standard configuration details are subject to change without notice based on system upgrades, licensing agreements and USG activities.

Additional equipment, upgrades, and deviations from the standard load may be proposed for review. If endorsed, any additional funds necessary to cover price differences or support will be the responsibility of the purchasing entity.

2.5 Replacement Cycle

The University has established a computer replacement cycle with an exchange of each university supplied machine (2.4) on a three (3) year average based on sufficient USG budget allocations. The replacement initiatives will follow the Replacement Cycle Schedule by departments/units available on the GC&SU Technology Resources WEB page.

http://technology.gcsu.edu

The cycle is based on an average of three (3) years. Depending on equipment condition, budgeting and job requirements, replacement may occur in two (2) years or be delayed until four (4) years.

3 Operational Practices

3.1 Deployment Procedures

All purchase requests must include the name and location of the individual that will be the user of the equipment. Upon deployment, equipment will be installed for the identified individual. In the event that the equipment is an upgrade or replacement, the current equipment shall be returned to the University's general inventory after the successful deployment of the new computer as confirmed by the user. In the event of a replacement/upgrade, all efforts will be made to protect the user's data. However, the user shall be responsible for having back-up copies of all critical files.

3.2 New Faculty

Each new fulltime, tenure track faculty member shall receive one (1) new standard configuration upon arriving on campus.

3.3 Redeployment

The redeployment of equipment for specialized uses shall be requested through the OIIT. The deployment decision shall be based on overall campus needs, requested activity and availability of inventory. Any equipment removed from the possession of an employee will have a "secure" wipe of the hard drives before reissue or salvage to assure removal of sensitive data.

3.4 Security

Security is major concern of the University and the University System of Georgia. Audits by the USG Auditors and State of Georgia Auditors have a technology component. To assure the safety of the university resources, faculty and staff should be familiar with all the security policies and guidelines. The following items pertain to the university's security procedures concerning hardware and software.

- The President of the University, through the university's Technology Security Incident Response Plan has delegated the responsibility and necessary authority to the CIO, to assure that critical data and the network infrastructure of the University are secure.

- All computers shall be deployed with administrative and user password configurations. Administrative passwords will be restricted to OIIT personnel. Installation of software, changes of configurations or operating systems will be made by the OIIT staff. Requests for adjustments or installations shall be made through the SERVE help desk. Waivers allowing administrative rights in unique circumstances may be granted by the CIO to faculty or staff members who require administrative access to computer systems in order to perform tasks within the scope of their employment. Abuse of waiver or failure to follow this equipment and software policy may result in waiver revocation. Denials of waivers or waiver revocations may be appealed to the University Technology Committee. In the event that a waiver is granted, the user may be personally responsible for costs for damage to the university's resources or losses resulting from user negligence.

- All computers shall have the university's approved virus protection application installed. The user shall not disable that application or in anyway hinder the functionality or upgrade capabilities. Hindering functionality includes disabling download features or failing to comply with directives that assure the virus .dat signatures are kept current.

- Computer configurations shall incorporate a domain authentication procedure for logging on to the GC&SU network. Allowing non-authorized users access to passwords or sharing of accounts is prohibited. This does not include individuals who produce an OIIT ID authorizing them to perform system and computer maintenance. Employees with Red security clearance are authorized to work on any university equipment. Yellow security clearance is provided to employees authorized to work on general faculty and staff machines not associated with enterprise level applications. Green ID badges identify lab and general non technical support personnel.

- Any personally owned computer that is connected to the university's wired or wireless network or is used to physically exchange files with university owned resources shall have a legal, approved current virus scanning application. Virus scanning applications for personally owned computers may be purchased through the SERVE help desk. These applications are licensed for faculty use only on machines used for university activities.

3.5 SERVE Helpdesk

The official SERVE help desk is designed to receive all technology inquires. The SERVE representatives will attempt, through a series of questions, to resolve the problem by phone. If the representative is unable to resolve the problem, a service request will be placed. A trouble call number will be issued to the caller. A support technician will respond to all requests as soon as possible. Critical software installs will be completed within 48 hours. If there is a unique or critical need, the user should be sure to identify and fully explain the need. If possible, priority consideration will be given.

3.6 Acceptable Use

The user shall be aware of all GC&SU and USG acceptable use policies. The following items pertain to the university's procedures concerning hardware and software use.

- Some electronically-received information may be found to be offensive and perhaps pornographic by some members of the GC&SU community. Individuals may be particularly offended if they are exposed to the material unwittingly. Exposing other persons to offensive materials may constitute prohibited harassment.
    - Except as permitted by Georgia law in connection with teaching and research, users in offices or public areas while alone or in the presence of others shall NOT:
        - Create, display, or transmit threatening, racist, obscene or harassing language and/or materials.
        - Transmit to others in any location inappropriate images, sounds or messages that might create an atmosphere of harassment for others.
        - Display, store or transmit sexually explicit images, messages, or cartoons.

- Employees shall not willfully disseminate computer viruses. Authorized users should be sensitive to the ease of spreading viruses and should take steps to insure computer files are virus free.

- Employees of GC&SU may use the University's computing resources including transmission over the University network, for scholarly purposes, for official University business, and for personal purposes so long as such use (a) does not violate any law or University policy, (b) does not involve significant use of University resources or direct costs, (c) does not substantially interfere with the performance of University duties, work, or data communications networks, and/or (d) does not conflict with the State policy on Misuse of State Property.

- Any attempt by any person or group to circumvent system security, guess other passwords, or in any way gain unauthorized access to local or network resources is prohibited. Employees may not use another person's computing account, attempt to forge an account, or use a false account or E-mail address.

- Transferring copyrighted materials to or from any system or via the University network without express consent of the owner may be a violation of Federal and/or State Law.

- Using the GC&SU network to share copyrighted audio and/or video materials except as provided by federal, state, USG and/or GC&SU policy is prohibited.

Authorized users of GC&SU's resources are encouraged to report violations of University policies to unit representatives or the OIIT personnel.

4 Related Documentation/Sources

4.1 The GC&SU Technology Security Incident Response Plan

SENSITIVTY NOTICE

University System of Georgia (USG) and Georgia College & State University (GC&SU) – Sensitive

The GC&SU Office of Information and Instructional Technology - Technology Security Incident Response Plan is classified as USG sensitive. It contains sensitive system security information relating to the security services, processes, and operations of the USG and GC&SU enterprise information networks. Unrestricted public disclosure of this information would assist unauthorized persons to breach the USG and GC&SU educational network systems and place ‘privacy’ and other sensitive categories of information at risk.

The Technology Security Incident Response Plan is available for review from the Chief Information Officer or Chair of the University’s Homeland Security Committee upon demonstration of appropriate need.