	FGCU POLICY 3.022	**Responsible Unit:**
	University Technology Resources	Information Technology Services

A. POLICY STATEMENT

Florida Gulf Coast University's Technology Resources are a vital component of the teaching, research, and business environment of the University. As part of its educational mission, the University acquires, develops, manages, and maintains Technology Resources. These Technology Resources are intended for University-related purposes, including direct and indirect support of the University's instruction, research and service missions, administrative functions, student and campus life activities, and the free exchange of ideas within the University community, and among the University community and the wider local, national, and world communities. Users are to use University Technology Resources in a responsible, legal, and ethical manner.

B. REASON FOR POLICY

The purpose of this Policy is to provide Users with guidance on the appropriate and inappropriate use of Technology Resources.

C. APPLICABILITY AND/OR ACCOUNTABILITY

This Policy applies to all Users of University Technology Resources and to all uses of Technology Resources, whether on campus or from remote locations. Additional policies may govern specific computers, computer systems, or networks provided, or operated by, specific units of the University.

D. DEFINITION OF TERMS

1. *Technology Resources*: All electronic devices and services provided or supported by the University. Electronic devices include the University Network, network servers, desktop computers, workstations, laptop and other portable computers; input devices such as tablets, cellular or satellite phones, modems, scanners, pagers, and telephone systems; output devices such as printers, fax machines, and copiers; storage devices such as servers, portable drives (jump or thumb drives), optical or digital drives, or other external data storage drives or systems; payment point of sale systems and credit card readers; and any other devices that may be connected to the University Network. Electronic services include software mounted on University Technology Resources as well as software services accessed through the University Network, Voice Over Internet Protocol (VoIP) services, and other electronic data or communication services.

2. *University Network*: Systems of personal computers, servers, and other electronic devices

connected in a series of interconnected nodes that can transmit, receive, and exchange data, voice, and video traffic.

The University operates a public wireless network which Technology Resources can access without the requirement of University approval. The University operates a private wired and wireless network accessible only to University-owned Technology Resources and for other Technology Resources that are approved to connect to the private network.

3. *User*: A person who makes use of or accesses University Technology Resources. Users are University employees, students, and faculty, and may include members of the public such as outside patrons of the University Library.

E. PROCEDURES

1. Assignment of Network Account to User

   A network account is assigned to a User upon becoming associated with the University. Users are generally free to use University Technology Resources as necessary to carry out their assigned responsibilities or academic work, subject to the authorized use of Technology Resources as described in this Policy. Users assigned a network account must exercise due care to protect their account information, especially sign-on information, from accidental disclosure and report any potential violations to Information Technology Services (ITS) immediately. Users must also complete the annual required security training to retain access to their network account.

   Users must not connect any devices (e.g., wireless network equipment, computers, printers, etc.) to the network without ITS' approval. Additionally, the University has the right to disconnect or remove University or privately-owned equipment, systems, files, or websites or restrict use thereof at any time as required to maintain the functionality, security, or integrity of University Technology Resources.

2. Use of Network Account by User

   a) Users should also be aware that their use of University Technology Resources is not completely private. While the University does not routinely monitor individual usage of its Technology Resources, the normal operation and maintenance of University's Technology Resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service.

   b) The University may also specifically monitor the activity and accounts of an individual User, including individual login sessions and the content of individual communications, without notice, when:

      1) The User has voluntarily made them accessible to the public, as by posting to a

Web page;

2) It reasonably appears necessary to do so to protect the integrity, security, or functionality of University or other Technology Resources or to protect the University from liability;

3) There is reason to believe that the User has violated or is violating this Policy;

4) An account appears to be engaged in unusual or unusually excessive activity; or

5) It is otherwise required or permitted by law.

c) The monitoring of communications, other than what is made accessible by the User, required by law, or necessary to respond to emergency situations, must be authorized in advance by the appropriate Vice President after consultation with the Office of General Counsel. The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel, agents, or law enforcement agencies, and may use those results in University disciplinary proceedings. Communications made by means of University Technology Resources are subject to Florida Public Records laws.

d) Deleting or erasing information, documents, or messages maintained on University Technology Resources is in most cases, ineffective. Information kept on University Technology Resources may be electronically recalled or recreated regardless of whether it may have been "deleted" or "erased" by a University employee. The University periodically backs-up all files and messages and because of the way in which computers re-use file storage space, files and messages may exist that are thought to have been deleted or erased. Therefore, University employees who delete or erase information or messages should not assume that such information or messages are no longer accessible.

3. Responsibilities of Network Account User

a) A User is responsible for any activity originating from their account.

b) A User's account and password must not be shared with others.

c) A User shall comply with all applicable University Technology Resources regulations, policies, and guidelines, as well as federal and state law and regulations governing the use of Technology Resources.

d) University Technology Resources must be used only for purposes directly related to, or in support of, the academic, research, or administrative activities of the University. University Technology Resources may be used for personal purposes or approved

outside employment activities with permission from the User's supervisor after consultation with ITS.

e) A User shall only connect approved devices and software to the University private network. No personal Technology Resources may be connected to the University private network. Users may connect personal Technology Resources to the University public network and must comply with this Policy when using the University public network.

f) A User shall not attempt to undermine the security or integrity of University Technology Resources and shall not attempt to gain unauthorized access to University Technology Resources. Users shall not employ any computer program or device to intercept or decode passwords or similar access control information. If security breaches are observed or suspected, a User must immediately report to the appropriate system administrator any known, observed, or suspected security breaches.

g) A User shall not use computer or telecommunication systems in such a manner as to degrade or disrupt the normal operation of voice or data networks or to intentionally damage or disable technology or telecommunications equipment or software.

h) All Technology Resources, regardless of funding source, which access the University Network must be approved by ITS prior to use. All software and on-line software services will be reviewed prior to use by ITS for compliance with data and University Network security requirements. All vendor contracts and license agreements for University Technology Resources must be submitted to Procurement for review and execution prior to use.

i) Users shall maintain documentation sufficient to prove that the Technology Resource has been obtained and is installed in conformance with the applicable contract and license(s). Specifically, Users shall ensure that software acquisition and utilization comply with applicable software licenses and U.S. copyright law. A backup copy of software shall be made only if expressly permitted by the applicable license.

j) To maintain proper functioning of computer and networking hardware and software, system administrators and individual Users shall take reasonable care to ensure their computers are free of viruses or other destructive software through installation and frequent updating of antivirus and antimalware software as directed by ITS.

k) Users of University Technology Resources shall use these resources prudently and avoid making excessive demands on these facilities in a manner that would knowingly impair access to, or use of, these resources by others.

l) The User shall not take University Technology Resources out of the country without University approval. Contact the Travel Desk for information regarding traveling

with University or personal Technology Resources.

4. Remote Access of Network

   Users must use the University virtual private network (VPN) to remotely connect to University Technology Resources.

5. Technology Resources for Taking Payments (Credit Cards, etc.) for University Activities

   A University unit must obtain written authorization from Finance & Accounting prior to collecting or processing payments. This includes approval of Technology Resources used for FGCU's approved payment application or new installations of payment applications and Technology Resources. No payments for University activities may be done through unapproved means, such as mobile payment solutions or third-party payment solutions.

6. Use and Misuse of Technology Resources

   a) Occasional personal use of University Technology Resources is permitted when it does not consume a significant amount of time or University resources, does not interfere with the performance of the User's job or other University responsibilities, and is otherwise in compliance with this Policy.

   b) University Technology Resources shall not be used to impersonate another individual or misrepresent authorization to act on behalf of other individuals or the University. All messages transmitted through University computers and telecommunications networks must correctly identify the sender.

   c) University Technology Resources shall not be used to make unauthorized or illegal use of the intellectual property of others, including copyrighted music, videos, films, and software.

   d) University Technology Resources shall not be used for unapproved commercial purposes or for personal financial gain without express written approval from the President, or designee.

   e) The University provides telephone and long distances services for official University business. University employees are allowed to make incidental use of the telephone system for personal calls. However, charges accruing from the incidental minimal use may be reimbursed to the University at the Vice President's discretion.

   f) A User shall not transmit to others or intentionally display in the workplace images, sounds, or messages that inhibit the ability of others to perform their job functions or violate FGCU Regulation 1.003, Non-Discrimination, Anti-Harassment, and Sexual Misconduct.

g) Users assigned Network accounts must comply with all applicable laws when using University Technology Resources. Applicable laws include but are not limited to the Florida Computer Crimes Act (Chapter 815, Florida Statutes), the Florida Communications Fraud Act (section 817.034, Florida Statutes), the Computer Fraud and Abuse Act (18 U.S.C. 1030), and laws relating to child protection, privacy, copyright, and trademark.

7. Enforcement

A User who violates this Policy may be denied access to University Technology Resources. The University may suspend, block, or restrict access by a User's account, independent of such procedures, when necessary to protect the integrity, security, or functionality of University Technology Resources. Alleged violations will be addressed through the University disciplinary procedures applicable to the User. Users who are not associated with the University may be denied access to University Technology Resources. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Authority

Florida Computer Crimes Act (Chapter 815, Florida Statutes)
Florida Communications Fraud Act (section 817.034, Florida Statutes)
Computer Fraud and Abuse Act (18 U.S.C. 1030)
BOG Regulation 3.0075, Security of Data and Related Information Technology Resources.

History of Policy

New 03/02/88; Amended 01/30/06, Amended 09/03/09, Amended 05/16/22

APPROVED:

*s/Michael V. Martin	May 16, 2022
Michael V. Martin, President	Date