UCF

UNIVERSITY OF CENTRAL FLORIDA

Office of the President

SUBJECT: Use of Information Technologies and Resources	**Effective Date:** 9/16/2022	**Policy Number:** 4-002.5
	Supersedes: 4-002.4	**Page Of** 1 9
	Responsible Authority: Vice President for Information Technology and Chief Information Officer	

DATE OF INITIAL ADOPTION AND EFFECTIVE DATE 5/21/2008

APPLICABILITY/ACCOUNTABILITY

This policy applies to all University of Central Florida (UCF) all persons who use university information technology resources.

BACKGROUND

Computer accounts are provided to students and employees as a privilege associated with membership in the university community and with varying access rights according to institutional role and job duties.

UCF students and employees are generally free to use UCF computing, telecommunications, and electronic information resources as necessary to carry out their assigned responsibilities, subject to the authorized use of those resources as described in this policy and other UCF policies. The university reserves the right to disconnect or remove university or privately-owned equipment or restrict use thereof at any time as required to maintain the functionality, security, or integrity, of university computing and telecommunications resources.

This policy shall not be interpreted or applied to abridge academic freedom or the constitutional guarantees of freedom of speech or freedom of expression.

POLICY STATEMENT

The University of Central Florida's computing and telecommunications resources provide a wide range of capabilities for students and employees to communicate, store, and process information that is essential to the academic, research, and administrative functions of the university. UCF is committed to having a comprehensive information security program that includes a security awareness program to promote and reinforce good security practices, policies and procedures, employee responsibilities, and fulfills the university's legal and contractual obligations.

It is the policy of the University of Central Florida that all students and employees use computing and telecommunications resources ethically, responsibly, and in compliance with all applicable federal and state laws, university policies, and as prescribed by this policy's procedures. The goal of the security awareness program is to promote a strong information security culture at UCF, where users recognize the value and importance of protecting data and the privacy rights of individuals. Users of information systems must complete annual training, other training as appropriate, remain vigilant to the information security threats UCF faces, and report suspected threats immediately to the security incident response team (SIRT) via sirt@ucf.edu or via a call to 407-823-5117.

Any violation of this policy and procedures may result in immediate loss of network and computer access privileges, seizure of equipment, or removal of inappropriate information posted on university-owned computers or university-supported internet sites. In addition to these corrective actions, failure to comply with this policy and procedures may result in disciplinary action up to and including termination for employees or expulsion for students.

DEFINITIONS

Computing Resource. Personal computers, laptops, and portable computing and communication devices, such as tablets, and smartphones, servers, mainframes, data storage systems, and similar equipment capable of processing, accessing, displaying, storing, or communicating electronic information.

Controlled Unclassified Information (CUI). A type of federal data consisting of unclassified information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

Credentials. A combination of username, password, and possibly additional information such as a PIN or biometric scan that together are required to access a computer system or information resource.

Departmental Security Coordinator. A designated employee who serves as the primary contact between the respective department or business unit and the Information Security Office (ISO) for all matters relating to information security.

Electronic Information Resource. Data or information in electronic format and the computing and telecommunications resources through which such resources are accessed or used.

Electronic Messages. For purposes of this policy, electronic messages include electronic mail, text messages, videos, images, or sound files that are sent from a computing resource through a computer network.

Internet Cloud Storage. Data stored in third party data centers, e.g., CrashPlan, Dropbox, iCloud, Google Drive, OneDrive, Box, etc.

Phishing. An attempt to acquire sensitive information such as usernames, passwords, and credit card numbers, often for malicious purposes, through electronic communications, such as email or text messages.

Restricted Data. Any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, both in storage or in transit. Further defined in UCF policy 4-008 *Data Classification and Protection*.

Role-based training. Information security training that is tailored to an employee's specific job function, access, or as dictated by regulatory or contractual requirements. Role-based training may also include training specific to certain types of data sets that require tailored training, such as the Family Educational Rights & Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and certain types of data such as CUI.

System Administrator. A User who has responsibility to manage system updates on behalf of other Users.

Telecommunications Resource. Wired or wireless voice or data communications circuits or networks and associated electronic equipment.

User. A person who makes use of or accesses university computing, telecommunications, or electronic information resources.

A. User Responsibilities

1. Users are responsible for any activity originating from their accounts that they can reasonably be expected to control. Credentials must not be shared with others.

2. Users must comply with all applicable conduct codes and rules, laws, and regulations governing the use of computer and telecommunications resources.

Examples include laws regarding libel, privacy, copyright, trademark, obscenity, and child pornography; the Florida Computer Crimes Act; the Electronic Communications Privacy Act; and the Computer Fraud and Abuse Act.

3. Except in isolated or occasional circumstances, the computing and telecommunications resources of the university must be used only for purposes directly related to or in support of the academic, research, service, or administrative activities of the university. In accordance with university regulation UCF-3.018 Conflict of Interest or Commitment; Outside Activity or Employment if a university employee wishes to use university facilities, equipment, materials, or software in connection with an outside activity or employment, permission must be obtained in advance using the appropriate form outlined in the regulation.

4. Users must not attempt to undermine the security or the integrity of computing systems or telecommunications networks and must not attempt to gain unauthorized access to these resources. Users must not employ any computer program or device to intercept or decode passwords or similar access control information. If security breaches are observed or suspected, they must be immediately reported to the security incident response team (SIRT) via sirt@ucf.edu or via a call to 407-823-5117.

5. Users must not use computer or telecommunication systems in such a manner as to degrade or disrupt the normal operation of voice or data networks or university computer systems or to intentionally damage or disable computing or telecommunications equipment or software.

6. Users must ensure that software acquisition and utilization adhere to the applicable software licenses and U.S. copyright laws. Users must maintain sufficient documentation to prove that all software installed on any computing resource assigned to them was legally obtained and is installed in conformance with the applicable license(s). Backup copies of software may be made only if expressly permitted by the applicable license(s).

7. Users of university computing facilities and telecommunications networks must 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.

8. Employees with access to university information systems must complete an online Security Awareness Training course every 12 months. Newly hired employees are required to complete the information security training course within the 30 days from date of hire or start date and every 12 months thereafter.

9. Employees with access to university information systems may be required to complete supplemental role-based training based upon policy, regulatory, or

contractual requirements, depending on job role and/or prior to gaining access to information systems containing certain types of data such as FERPA, HIPAA, CUI, etc., that require additional training.

10. Users may receive simulated phishing messages as part of authorized internal simulated phishing campaigns.

11. Employees with access to university information systems may be required to complete additional supplemental training provided on an as-needed basis depending upon results from authorized internal simulated phishing campaigns.

12. Users with access to university information systems may be required to sign an "Acceptable Use Policy" and "Confidentiality Agreement" prior to receiving access to the university's information systems and data.

13. Users may lose access to university systems if they do not complete annual training, or any other assigned training as required.

14. System Administrator, or where appropriate, users, must take reasonable care to ensure their computing resources are not compromised by viruses or other malicious software. Additionally, any vulnerabilities classified as exploitable, critical, high, or medium must be resolved in a timely manner as described in 105 Patch Management Standards or when directed by the Information Security Office (ISO). It is the responsibility of the User or System Administrator to contact the UCF IT Service Desk for technical support if they are unable to address a vulnerability or compromised system.

15. Failure to address these vulnerabilities or maintain a secure system may result in the vulnerable or compromised systems being isolated from the UCF network until the issues are properly mitigated.

B. Use and Misuse of Computing and Telecommunications Resources

1. The university's computing and telecommunications resources must 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 computing resources and telecommunications networks must correctly identify the sender.

2. The computing and telecommunications resources of the university must not be used to make unauthorized or illegal use of the intellectual property of others, including copyrighted music, videos, films, texts, images, and software.

3. The computing and telecommunications resources of the university must not be used for unapproved commercial purposes, or for personal financial gain, without express written approval from the provost and executive vice president or his or her designee.

4. Users are reminded of the university's commitment to a civil and non-discriminatory environment. Employees, including student employees, must not transmit to others or intentionally display in the workplace materials or messages that could reasonably be perceived as invasive of another's privacy; pornographic; unlawfully harassing; or disruptive to the operations of the university or any part thereof.

5. Users must not use university computer or telecommunications resources to download, intentionally view, store, or transmit images that could reasonably be regarded as obscene or pornographic.

6. The university provides email and other electronic messaging systems in support of official university business and functions. University employees are allowed to make incidental use of such systems for necessary personal messaging. University students may use university information technology resources for personal and recreational purposes, in addition to educational endeavors, but must do so in conformance with university policies.

7. The following uses of university messaging systems by students, employees, or any other user of the messaging system are prohibited under this policy:

   a. unlawful harassment as prohibited by university policy
   b. threatening messages sent to individuals or organizations
   c. messages that include malware, phishing, or hoaxes
   d. spamming or high-volume email transmission other than those specifically allowed by the Broadcast Distribution of Electronic Mail Policy (4-006)
   e. for commercial use or personal financial gain
   f. false identification (any messages that misrepresent or fail to accurately identify the true originator)
   g. messages that contain or direct users to computer viruses, worms, or other harmful software
   h. any illegal activity or crime

8. The university and its employees are prohibited from using any university resources in support of a political campaign or for campaign fund raising, even under a reimbursement arrangement. An example of prohibited use would be a university employee using university electronic messaging, internet, or telephone resources to solicit support of a political candidate or to raise funds for a candidate.

C. Access to and Disclosure of Electronic Information

1. Users should be aware that their uses of university computing and telecommunications resources are not completely private. The university does not routinely or without cause monitor individual use of these resources; however, the normal operation and maintenance of these resources require the backup and caching of data and communications, logging of activity, monitoring of general usage patterns, and other such activities. In addition, information

stored on university computing resources or passed through university telecommunications networks may be accessible to the public through public record laws, subpoenas, interception, or other means.

2. The university may specifically monitor the activity or accounts of individual users of university computing and telecommunications resources, including individual login sessions and the content of individual communications, without advance notice when:

   a. the user has voluntarily made such information accessible to the public, as by posting to a listserv, blog, or webpage
   b. it reasonably appears necessary to do so to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability
   c. there is reasonable cause to believe that the user has violated or is violating a university policy, a regulation, or a law
   d. an account appears to be engaged in unusual or excessive activity
   e. it is otherwise required by subpoena or court order

3. Access to and disclosure of electronic information is governed by the following provisions.
   a. Professional ethics dictate that any person having access to proprietary or restricted information must:

      1) use that access only to the extent required to discharge the assigned responsibilities of that person's position
      2) not disclose any such information except to the extent authorized or required under this policy or applicable rules or laws
      3) not use, in any manner, such information or knowledge for personal financial gain

   b. A university employee may not read, view, listen to, or otherwise access electronic messages or the contents of computer systems of another user without the knowledge or consent of that user, except: (i) under the limited circumstances provided for in this policy or (ii) upon express prior authorization from the provost and executive vice president, his or her designee, the general counsel, or the UCF Police Chief or designee. Such prior authorization must be given in writing and must clearly state the purpose of granting such access. Information accessed in authorized instances must not be disclosed except as provided in this policy or with prior written authorization from the university's provost and executive vice president, his or her designee, the general counsel, or the UCF Police. Such prior authorization to disclose must be given only in cases involving an actual or possible breach of system security, a violation of law, a violation of university regulation or policy, or dereliction of duty or responsibility on the part of a university user.

c. Any suspected abuse or misuse of university computing and telecommunications resources should be reported to the Information Security Office (407-823-3863 or infosec@ucf.edu). Proper pursuit of such cases may require that person to disclose relevant information to supervisors or designated investigators.

d. Employees who access restricted data are expected to sign the UCF Confidentiality Agreement.

RELATED DOCUMENTS

The following related policies are available online at: http://www.policies.ucf.edu/

Policy 2-004 *Prohibition of Discrimination, Harassment and Related Interpersonal Violence*
Policy 2-100 *Florida Public Records Act: Scope and Compliance*
Policy 2-103 *Use of Copyrighted Material*
Policy 4-001 *Retention Requirements for Electronic Mail*
Policy 4-003 *Telecommunications Services*
Policy 4-006 *Broadcast Distribution of Electronic Mail*
Policy 4-007 *Security of Mobile Computing, Data Storage, and Communication Devices*
Policy 4-008 *Data Classification and Protection*
Potential Outside Activity, Employment, and Conflict of Interest and Commitment Disclosure (AA-21)
http://compliance.ucf.edu/conflict-of-interest/

A&P and USPS Permission to Use UCF Personnel, Equipment, Facilities, Students, or Services
http://hr.ucf.edu/files/HR12_PermissionToUseServices.pdf

INITIATING AUTHORITY Vice President for Information Technology and Chief Information Officer

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 4-002.5

Initiating Authority: Matthew Jett Hall Date: 9/13/2022

University Policies and Procedures Committee Chair: Rhonda L Bishop Date: 8/30/22

President or Designee: Alexander Cartwright Digitally signed by Alexander Cartwright Date: 2022.09.16 09:11:38 -06'00' Date: 9/16/2022

History 4-002 5/21/2008, 4-002.1 5/13/2014; 4-002.2 9/1/2016; 4-002.3 4/29/2021