Protect your PC

If you don't take proper precautions, hackers can break into your computer and steal restricted information.

Hackers could wipe out information such as your class rosters, grades, projects, lectures, research data, etc. You're responsible, under UCF Policies, for ensuring that your computers and work areas are secure.

Physical Security

Physically protect restricted information and computing resources by following these simple tips:

- Use password-protected screensavers.
- Make sure no one is looking over your shoulder when you enter your password.
- Lock your doors when you leave your office.
- Properly dispose of (e.g., shred, etc.) all documents that contain restricted information when they are no longer needed
- Never leave restricted information (employee or student information) in plain view.
- Store backup copies of important files in a safe location.

Logical Security

- Notify your IT manager if you notice suspicious activity such as the inability to login to your computer, constant computer crashes, abnormally slow programs, new files you did not create, deleted or missing files, or unauthorized persons in your work area. Do not turn off the computer or disconnect it from the network or make any changes before consulting with your IT Manager.
- Keeping your computer up-to-date with the latest patches is one of the best defenses against hackers and the spread of viruses and worms.

Password Security

- If it's a dictionary word - it's a bad password: Don't use it!
- Use a mnemonic, such as the first letter of a song verse or a phrase, while adding in numbers, symbols ($,%,*), and UPPER/lower case letters.
- Change your password often! UCF standard is 60 days.
- Never write down a password and never share accounts.
- Do not give your password to anyone, not even the Service Desk!
- Never use your UCF NID password for non-UCF systems.
- Avoid the "save my password / remember my password" option on web sites.

Acceptable Use Policy

UCF information technology resources shall not be used to…

- Impersonate another individual or misrepresent authorization to act on behalf of other individuals or the university.
- Make unauthorized or illegal use of the intellectual property of others.
- Attempt to read or duplicate electronic information belonging to others, or to decrypt or translate encrypted information
- Send telecommunications messages the content of which is defamatory, or which constitutes a breach of telecommunications security, or is in violation of Federal, State, or local laws or university rules or policies
- Intentionally damage or disable computing or telecommunications equipment or software
- Undermine the security or the integrity of computing systems or telecommunications networks and shall not attempt to gain unauthorized access to these resources.
- A user must report any misuse of computer resources or violations of this policy to their department head, to the Information Security Office, to the Vice Provost or to the Chief Technology Officer at Computer Services & Telecommunications.

Complete policy may be found at www.policies.ucf.edu

Copyright Infringement

A copyright infringement occurs when you download, store, use, copy, or share, something created by someone else without the permission from the person or entity that created it. Violating copyright is against UCF policy and Federal law.

- University security incident response staff regularly investigates reports from copyright owners of file sharing and copyright violations. As a university we understand the philosophy of open communication and sharing of ideas and articles. However, we do not support sharing of ideas or articles that belong to private individuals or organizations.
- Since current peer-to-peer applications are predominantly used for trading copyrighted material, such applications are not permitted anywhere on the UCF network.
- For more information, please check the UCF Golden Rule, Acceptable Use Policy, and the information security website:
  www.policies.ucf.edu
  www.goldenrule.sdes.ucf.edu
  www.infosec.ucf.edu

UCF

Stands For Opportunity

INFORMATION SECURITY FOR FACULTY & STAFF

University of Central Florida
Information Security Office
www.infosec.ucf.edu
infosec@ucf.edu

- The University of Central Florida provides computing resources for the purpose of accomplishing tasks related to the UCF mission.
- Use of UCF computing resources must be limited to justifiable computing support for academic and administrative purposes
- Use of UCF computing resources is subject to review and disclosure in accordance with the Florida Public Information.

Report an Incident

To report an information security incident, such as unauthorized access to a university system or data, unauthorized usage of someone's account or the accidental distribution of restricted data, please contact the Information Security Office using one of the following two ways:

- **Send an email to sirt@ucf.edu**
- **Call Service Desk @ 407-823-5117**

Introduction

As an institution of higher learning, University of Central Florida encourages, supports, protects, and embraces freedom of expression to pursue scholarly inquiry and to share information with the global academic community.
To maintain a secure and reliable network, UCF Information Technology strives to inform all UCF employees and students of the policies which govern the use of UCF computing services and networks.
This brochure is designed with faculty and staff in mind. In it you will find information on where to find policies, information to secure restricted data, your computer and your identity.

Policy & the Law

By using UCF networks, computing services, and other computer resources, you accept and agree to all policies governing their use. The policies for Appropriate Computer Use can be found at www.policies.ucf.edu
Each user is responsible to read, understand and remember computing policy. Users can seek clarification from Information Security Office at infosec@ucf.edu

Computer Use & the Law

Information technology is not only governed by the University itself, but also by state and federal laws; therefore; the policies of all of these organizations may need to be strictly adhered to should a user wish to continue using the network. Find out what applies in your work environment.
FERPA, GLBA, HIPAA, Florida Statutes
Florida Computer Crimes Act
The Digital Millennium Copyright Act

Protect Restricted Information

- Restricted information, as defined by policy 4-008, includes, but not limited to, SSNs, credit card, debit card, ISO, and driver's license numbers, biometric data, medical records (ePHI), computer accounts, access codes, passwords, grades, email addresses, photographs, and other information protected by law or regulation, e.g., FERPA, HIPAA, PCI, etc.
- The UCFID (aka EMPLID) is the designated University identification number that identifies an individual in the UCF computing systems. It is a replacement for the social security number. **You may freely ask for the UCFID on forms and on online applications, include it in communication letters, and communicate within @ucf email system.**
- Do not copy or download restricted information from the University's administrative systems to your PC, Web server, laptop, or any other mobile device.
- Know the protection requirements for each type of data that you come into contact with. For more information please consult with the information custodians (e.g., Registrar, Human Resources, etc.)

Protect Your Identity

- Before purchasing resources on the internet or providing any personal information (bank account number, credit card number, etc.), always make sure that the Webpage is secure. Double check the web address you are going to and look for "https" in the web address (Notice the "s"). This shows the website is encrypted.
- **Email is not appropriate for sending restricted information, as most email providers do not provide encryption.**
- Never collect credit card or bank account information via email. This violates UCF policy on appropriate methods for accepting credit card information. Look for cardholder information security procedures at www.policies.ucf.edu

Watch out for spyware

When you install certain software (such as file sharing or freeware) on your computer, you may unknowingly be installing spyware or adware programs as well. Spyware is a program that gathers information about you and what you do on your computer without your knowledge, sending the information to different sources.

Cloud Computing

Cloud Computing is using services and applications offered through the Internet. This means data and applications may not be held on UCF computer systems. Online email services such as Knights Email, Hotmail and Gmail are examples of cloud computing applications which provide email services and cloud storage through a web browser. There are numerous other applications and services that faculty and staff may be familiar with, such as Instructure Canvas, OneDrive, Apple iCloud, Dropbox, Google Drive, Facebook, Digg, and many more. **Canvas and Knights Email (and its associated applications, such as Office 365, OneDrive, and Skype) are examples of officially recognized cloud service providers for conducting academic work.**
Here are some guidelines to apply in the use of services available in the cloud.
• Internet application and service providers require users to consent to their Terms of Service, frequently via a "click-through" agreement, which is a legal contract. Faculty, staff, and students are not authorized to enter into legal contracts on behalf of UCF and may not consent to click-through agreements for the purposes of University business.
• Storing restricted data in an unauthorized cloud provider system is forbidden.
• Never store or post information or data that the University has classified as "restricted, personal" or Personally Identifiable Information (PII) on the Internet. Examples include social security, credit card, and driver's license numbers, electronic health information (ePHI), etc.
• Be aware of who has access to your online data since file sharing is available with other users.

Watch out for Phishing

Phishing is the act of convincing someone to surrender their private information (e.g., Bank account numbers, Social Security numbers, passwords, etc.) which can then be used to commit identity theft. Often phishing is done through email formatted to look like official communication from banks, eBay, or other legitimate organizations.
• Legitimate businesses do not solicit user account information through email. Delete all phishing emails that you receive.