LAWS & REGULATIONS

Federal and state laws address how confidential information must be handled.

VIOLATION OF THESE LAWS AND REGULATIONS COULD RESULT IN SIGNIFICANT FINES AND PENALTIES TO UF, AND POSSIBLY TO THE INDIVIDUAL RESPONSIBLE FOR THE VIOLATION.

There are multiple federal and state laws governing confidential information that impacts the University of Florida community. To learn more, visit:

https://security.ufl.edu/employee-guide

HIPAA
FERPA
FIPA

REPORT SUSPECTED INFORMATION SECURITY INCIDENTS

If you suspect an information security incident has occurred, even if you had no part in its cause, report it immediately to your ISM or to the UF Computing Help Desk. Signs that could indicate an information security incident include:

- Your GatorLink password no longer works, and you did not institute a change. This could mean someone changed it without your knowledge, a possible result of a phishing incident.
- Your files are suddenly deleted or corrupted, or new files unexpectedly appear.

Other indicators of possible information security incidents are listed at *https://security.ufl.edu/employee-guide.*

LEARN MORE

SECURITY ALERTS

The IT Alerts page is frequently updated with information about campus IT services as well as warnings about cyber scams and viruses. https://alerts.it.ufl.edu

FREE CYBER SELF DEFENSE CLASS

UF's Information Security Office offers a two-hour workshop several times each year. The workshop is designed to raise awareness on topics including safe web browsing, preventing malware infections, recognizing phishing scams, and more. The workshop is part of UF's HR Training & Organizational Development schedule. Register via myTraining.

UF INFORMATION SECURITY OFFICE
Campus P.O. Box 112099, Gainesville, FL 32611-2099
352-273-1344 | *security@ufl.edu* | *https://security.ufl.edu*

The Foundation for The Gator Nation
An Equal Opportunity Institution

EMPLOYEE GUIDE TO INFORMATION SECURITY

PROTECTING UF IS OUR SHARED RESPONSIBILITY

UF | UNIVERSITY of FLORIDA
Information Technology

DON'T FALL FOR ONLINE PHISHING SCAMS
UF Information Technology
UFApps Program Promoted to Full-Time Production Service

COME ON IN, PLEASE USE THE TECHNOLOGY!

The Information Security Office (ISO) protects UF data and personal information from internal and external threats. The university has invested in state-of-the-art intrusion detection software and systems to protect its networks and data, and employs staff to monitor the UF information systems environment 24/7. Still, the best defense against a security or data breach is an informed and involved community:

INFORMATION SECURITY BEGINS WITH YOU!

IT'S A FACT

The number one reason for compromised accounts at UF is when faculty, staff, or a student opens and responds to a *Phishing* email.

Phishing is when someone tries, via email, text, or phone call, to get your personal information by pretending to be a trustworthy company, government entity, or a UF department. Remember:

NO ONE AT UF WILL EVER ASK YOU FOR YOUR GATORLINK PASSWORD OR YOUR SOCIAL SECURITY NUMBER!

If you are in doubt about an email or a phone call you receive at work, check with the UF Computing Help Desk *(352-392-4357/HELP, helpdesk@ufl.edu).*

YOU ARE THE KEY TO INFORMATION SECURITY AT UF!!

LEARN MORE ABOUT PHISHING EMAILS:
https://security.ufl.edu/employee-guide

LEARN MORE ABOUT UF INFORMATION SECURITY POLICIES:
https://security.ufl.edu/employee-guide

MOBILE COMPUTING AND STORAGE DEVICES

All mobile devices (such as smartphones, laptops, and tablets) and storage devices (like USB flash drives or external hard drives) used for university business, regardless of ownership, must be compliant with University of Florida policies and standards. University business includes receiving and answering UF email, processing student assignments and grades, approving time, and research and teaching-related activities.

- All mobile devices must be encrypted and have a strong password or PIN.
- If a university-owned device is lost or stolen, it must be immediately reported to your local IT support group or to the UF Computing Help Desk.

KNOW YOUR DATA!

You are responsible for the data you use, process, and store. Read the Data Classification Policy and Standard: **https://security.ufl.edu/employee-guide.**

PATCH, PATCH, PATCH!

All software has bugs, many of which can allow criminals to exploit your computer to steal or damage data. When new bugs are discovered, software vendors release updates and patches. It is crucial that software updates and patches are installed quickly to prevent security compromises.

- If you use your own computer to do UF work (emails, teaching, learning, and administrative activities) you must install updates and patches as quickly as possible. Failure to do so could leave you responsible legally and financially for any breaches that occur. For information about keeping your personal computer up-to-date, visit the **https://security.ufl.edu/employee-guide.**
- UF's VPN service allows faculty and staff to securely "tunnel" in to campus networks and access services and files. Contact your IT support staff or ISM for assistance setting up a VPN connection.

NEW PROJECT OR GRANT? PURCHASING COMPUTERS OR SOFTWARE?

If you're purchasing a new computer system, service, or software – even if funded by a grant or contract—please check with your Information Security Manager (ISM) or IT support unit before making the purchase. (To find your ISM visit **https://security.ufl.edu/employee-guide**.) Many IT acquisitions must be evaluated with regards to security, privacy, and legal considerations as well as compatibility with existing UF systems. Not taking these steps can cause delays to—and extra costs for—your projects. For information on software and services already evaluated, visit **https://security.ufl.edu/employee-guide.**

CHOOSE STRONG PASSWORDS

UF's GatorLink system requires the use of strong passwords. Creating high-quality passwords can be tricky. Check out the **https://security.ufl.edu/employee-guide** website for tips on creating strong passwords.