
PRIVACY:
TIPS, TRICKS, AND WAR STORIES

Who We Are

Dan LoPresto

Director, Privacy Compliance

Delainey Strickland

Information Security Professional

UCF

Data protection is the process of safeguarding important information from corruption, compromise or loss. The importance of **data protection** increases as the amount of **data** created and stored continues to grow at unprecedented rates.

privacy

Pronunciation: /ˈpr I vəsi, ˈprʌ I -/

noun

[*mass noun*]

a state in which one is not observed or disturbed by other people

the state of being free from public attention

UCF

Social Engineering Defined

— an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he/she needs to gain access to the system or otherwise extract confidential information, money, etc.

Clever manipulation of the natural human tendency to trust.

UCF

Social Engineering Defined

Clever manipulation of the natural human tendency to trust.

Methods:

- Phone
- Email
- In Person
- Instant Messaging
- Online (Social Media, etc.).

Reconnaissance:

- Dumpster Diving
- Association Observation
- Online & In-Person Research

UCF

Social Engineering Summarized

- Social Engineering involves the manipulation, or 'hacking,' of people using partial knowledge and clever ruses.
- Social engineers rely on reconnaissance, password disclosure, low security awareness and motivation to breach security mechanisms.
- We use a combination of e-mail and online articles, posters, and information security and protection training to raise awareness and protect ourselves from Social Engineering, Phishing and similar attacks.

UCF

Social Engineering Defense

- Never! Never! Never! Give your password to anyone for any reason!
- Verify the identity of all callers.
- Exercise caution when sharing information about other employees
- Never type things into the computer when someone tells you to unless you know exactly what the results of the commands are!
- Don't give out technical details of the university's software, systems, or similar except to valid users.
- Never answer questions from telephone surveys. Tell the caller that UCF employees do not participate in telephone surveys. If they need information, they should submit it in writing.

UCF

Protecting Yourself

- **Phishing email is often disguised** to look like it's from a legitimate source. If it's asking for information or directing you to take action that's unexpected, check carefully before responding. If you are uncertain about an e-mail from someone you know, call them on a known phone number to verify. If an e-mail is from another company or organization, call the organization on a publicly available number to verify the person's identity and intent.
- **Do not reveal any personal or confidential company information** in email, online, or on the telephone unless you know who you are dealing with and why.
- **Don't ever share your passwords** with anyone.
- **Don't reuse passwords** when going online for business or personal matters. Use different passwords and rotate your personal passwords so they are not the same as your business passwords.
- **Don't have confidential conversations in public settings.**
- If you find a CD or USB flash (thumb) drive, **do not place it into your computer** to see what is on it - turn it in to IT.
- **Don't respond to or forward unsolicited email** advertisements, chain letters, and hoaxes.
- **Log out** of sensitive programs when you walk away from your computer.
- If you receive telephone calls looking for someone or asking for company or personal information about you or other associates, be very cautious. **Unless you can confirm their identity, be safe and don't share the information.**
- **Consider using two-factor authentication** or two-step verification for your personal email account .

UCF

How To Handle Requests Involving Personal Data

Students and others' requests for:

- a copy of their personal information
- to delete their personal information

Direct them to email privacy@ucf.edu

- If they hand you a request in writing: send a fax or email, scan and/or forward it to privacy@ucf.edu immediately

Advise the individual that Privacy Compliance will initiate a Data Subject Access Request (DSAR) and communicate from that point forward.

UCF

Remote working employees are required to ensure the protection of all restricted and highly-restricted data, which includes personal and university confidential information accessible from or maintained within their home office. Below are some important tips and reminders for remote working employees:

Handling Restricted Information:

Take extra precautions to physically secure university assets while working remotely.

- Where possible, set up your at-home work area away from any windows where passers-by can see them.
- When you put computer equipment in your vehicle, use the trunk when possible and make sure items cannot be seen from outside the vehicle.
- Never leave computer equipment in an unlocked vehicle.
- Immediately notify the Security Incident Response Team (SIRT), via sirt@ucf.edu, if a university asset is lost or stolen.

Handling Personal Information:

Paper materials containing any Personal or otherwise Restricted Information belonging to students, faculty, staff, donors, etc. associated with the university, when no longer needed, should be cross-cut shred or destroyed so they cannot be reconstructed. If you do not have a cross-cut shredder at home, please place all documents of this nature in a secure bag or box. Once you return to campus, bring the documents and place them in the shredder bins on-site.

Unplug Virtual Assistants Before Audio/Video Conversations:

Before engaging in phone, Skype, Teams, Zoom, or other audible conversations with other employees, students, faculty, etc. regarding university business, cease using any/all virtual assistant services like Google Assistant, Siri, Alexa, Bixby, Cortana, and others as they are known to record conversations while activated, even when not commanded to do so. Unplugging these devices is preferred, otherwise power them off or close applications that perform virtual assistant-type functions.

UCF

Remote working employees are required to ensure the protection of all restricted and highly-restricted data, which includes personal and university confidential information accessible from or maintained within their home office. Below are some important tips and reminders for remote working employees:

Physically Secure Company Assets:

Restricted information on screen or paper should be handled in a way that avoids disclosure. Care should be taken in handling, discussing, or reviewing such information in public places where Restricted Information might be seen, overheard or electronically intercepted. Restricted information should not be left in open areas and should instead be kept in a secure location, such as a locked file cabinet or desk drawer. If you do not have a locked location for storage, they should be kept in one specific place within your home, such as a laptop bag, box, or storage container away from non-employees.

Avoid Sharing Personal and Confidential Information with Family, Friends, and Others:

- To respect the privacy of our faculty, staff, students, guests, and others associated with the university, avoid sharing personal or otherwise restricted information with family, friends, and others who reside with you. Lock your computer when you step away from it.
- Unlocked computers are not only subject to the eyes of non-employees, but to the hands of children who may innocently want to “play” on your (work) computer. Please remember that only employees are permitted to use university-owned equipment.

Keep All Data on University-Owned Computers:

If you’re using a university-owned computer, keep all data on that machine. Personal devices generally do not maintain an equivalent level of security monitoring and detection capabilities or encryption and therefore increase the risk of potential exposure.

UCF

Remote working employees are required to ensure the protection of all restricted and highly-restricted data, which includes personal and university confidential information accessible from or maintained within their home office. Below are some important tips and reminders for remote working employees:

Be wary of phishing e-mails:

Phishing e-mails use a lure – typically a message about an urgent or inviting issue – to trick individuals into taking some detrimental action. That action may be to open a malicious e-mail attachment, click a malicious link within an email, or take some other step that may reveal sensitive credentials or information. Phishing e-mails tied to disasters and crises are common, and the pandemic has been no exception. Avoid clicking links from sources you do not recognize and otherwise looks suspicious. Do not open untrusted attachments. Report phishing e-mails via Outlook and/or contact sirt@ucf.edu If you need assistance, contact IT Support.

Only Use Secured Wireless Networks (Wi-Fi):

Most employees are working from their home where they can secure their residential wireless network (Wi-Fi). However, employees who do not have secure Wi-Fi at their homes must not use unsecured, public Wi-Fi, as they are prime spots for malicious parties to spy on internet traffic and collect Confidential Information. Instead, use personal hotspots or another way to encrypt your web connection, such as Virtual Private Network (VPN).

Only Use Approved Online File Storage Sites:

Only use approved online file storage sites, such OneDrive, Teams, university shared network folders, etc., as necessary. Do not use any other file storage sites, such as Box.com, Google Docs, or Dropbox, etc.

Exercise Caution Hosting and Attending Meetings / Conference Calls:

For university-hosted meetings involving online collaboration applications, associates should only use approved UCF tools, such as Teams and Zoom.

UCF

Thanks for your time today!!!

Dan LoPresto, Privacy Compliance Officer

Delainey Strickland, Information Security Professional

UCF

Dan LoPresto, Privacy Compliance Officer

- Provide guidance around protecting Restricted Data stored, processed, and transmitted into, within, and outside the university.
- In accordance with university policies, state and federal laws, international regulations, and best practices, work with nearly every department to help secure digital assets and the data they contain.
- Serve as the university's GDPR Data Protection Officer (DPO), HIPAA Privacy Officer, and helps maintain compliance while investigating potential violations.
- Investigates FERPA violations and other data related concerns.
- Consistently collaborate with Information Security, General Council, and is a member of the Security Incident Response Team (SIRT).
- Coordinate with university departments and units to ensure privacy-related audit findings are addressed.
- Review contracts and negotiate language that promotes the protection of university data.
- Develop privacy training materials and other communications to train employees on university privacy policies, data handling practices, and procedures.
- Conduct privacy risk assessments and ongoing privacy compliance monitoring activities.

Privacy Compliance Officer

Contract Review

- Capture privacy obligations in writing

Ad Hoc Guidance

- Provide guidance to efforts involving student and employee data

Meetings

- Offer insight to internal projects & processes

Research

- Exploring new laws / best practices, attending conferences and webinars

Audit Response

- Ensure that requirements are met, and policies are followed

Data Governance

- Participate in committees centered around the organization security and appropriate treatment of data throughout the university