Policy on Reporting Security Incidents

With Resources on Computer Security

All college employees are responsible for maintaining the confidentiality, integrity, and availability of data and computer systems.

Security incidents should be reported as soon as possible, but within one business day to the unit head and the college's director of Information Technology (Don Harper, help@eecs.ucf.edu), as well as UCF's Security Response Information Team (srit@ucf.edu or 407-823-5117).

UCF's Data Classification and Protection Policy (4-008, see http://policies.ucf.edu/documents/4-008DataClassificationFINAL.pdf) defines several classes of data:

- *Restricted Data*, which is considered sensitive and protected, including:
    - *Personal Restricted Data*, including personally identifiable information, from which a person may be uniquely and reliably identified and contacted,
    - *Non-personal Restricted Data*, which is non-personal information whose release could adversely affect the university, including computer passwords and "student academic records as defined by the Family Educational Rights and Privacy Act of 1974."
- *Unrestricted Data*, which is all data not considered sensitive and protected.

To maintain *confidentiality*, all restricted data must be protected at rest and in transmission, and must not be disclosed "without explicit management authorization."

To maintain *integrity*, computer accounts should be protected by strong passwords, and measures should be taken to prevent access by unauthorized personnel.

Availability is violated when a computer system cannot be properly used for its intended purpose.

A security incident occurs when restricted data is disclosed without proper authorization, when integrity is compromised, or when availability is violated.

According to UCF's policy, "The UCF Information Security Officer must be notified immediately if data classified as restricted is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the university's information systems is occurring or is suspected of having occurred."

In addition to contacting the security response information team (srit@ucf.edu or 407-823-5117), all security incidents involving people (faculty, students, and staff) and/or CECS data or equipment must also be reported to the unit chair affiliated with the person reporting the incident and the college's Director of IT (Don Harper, help@eecs.ucf.edu). The unit chair names and e-mails can be found by accessing the CECS web-site www.cecs.ucf.edu. The SRIT team, the unit chair and the CECS IT Director will then work together to resolve the reported incident. When a security incident is reported, the unit chair and the CECS IT Director should immediately isolate the computer system(s) in question.

Informational Resources

General information about security resources at UCF can be found at www.infosec.ucf.edu.

Information about incident reports can be found at the following URL:
https://www.cst.ucf.edu/about/information-security-office/incident-response/

Student related information security pages can be found at:
https://www.cst.ucf.edu/about/information-security-office/iso-resources-rewrite/iso-resources-students/

An information security brochure (antimalware software, watch out of spyware, email tips, protecting your identity, common sense and the internet, report an incident) that is of help to students can be found at:
https://www.cst.ucf.edu/wp-content/uploads/infosec/Student_InfoSec_Brochure.pdf

An information security brochure (protect your PC, physical security, logical security, password security, acceptable use policy, copyright infringement, report an incident) that is of help to faculty can be found at:
http://www.cst.ucf.edu/wp-content/uploads/InfoSec_Brochure.pdf