SUBJECT:	Effective Date:	Policy Number:
UCF IT Security Policy	Supersedes:	Page 1 of 11
	Responsible Authority: Computer Services & Telecommunications	

Purpose

The purpose of this policy is to establish guidelines, procedures, and requirements to ensure the appropriate protection of UCF's information systems. In doing so, this policy addresses the need for privacy of personal and university information. The university has at its possession confidential information that must be protected. This policy also addresses the need for integrity of data in the university information.

Scope

This policy applies to all students, faculty, staff, consultants, temporaries, and others not mentioned who access UCF's computer network. This policy also applies to all computer and data communication systems owned by and or administered by UCF.

General Security Policy

Responsibilities

Responsibilities of Every User

All users of the University computer systems and network resources have the responsibility to ensure the overall security of university systems, and to behave in a manner consistent with this security policy. Each user is responsible for understanding and complying with the acceptable use policy (ITR) and the IT Security Policy (ITSP-*this policy*) of the University:

- For the acceptable use policy please refer to Use of Information Technology and Resources Policy (4-002)
- For additional acceptable use policies please refer to the Golden Rule/Computer Use Policy section
- For more clearly defined descriptions of administrative officers with primary information resource security responsibilities please refer to the Security Responsibilities section of the ADICS Guideline.

Responsibilities of System Administrators

System Administrators have the same user responsibilities plus the additional responsibilities and privileges below due to their administrative positions:

- System Administrators are expected to act as local information systems security coordinators

- System Administrators are expected to establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the systems they administer
- System Administrators are expected to be registered with NOC, and be adequately trained to provide network services for their network operating environment
- Backup System Administrators are expected to be identified and registered with NOC
- System Administrators are expected to prepare and maintain security procedures that implement the IT Security Policy in their local environment
- System Administrators are expected to prepare and maintain access control, backup and disaster recovery plans in the event of a disaster
- System Administrators are expected to take reasonable precautions to safeguard against corruption, compromise or destruction of data, computer systems, and network resources
- System Administrators are expected to ensure that user information is treated as private. It is recognized that a system administrator may potentially have contact with user files, email, etc. in the course of his or her duties. The contents of such files must be kept private. Access to system user files is authorized only in the event of a security investigation
- System Administrators are expected to take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully executed on all systems, networks, and servers
- System Administrators are expected to subscribe to appropriate vulnerability lists, based on the network operating system and services they support
- System Administrators are expected to subscribe (or retain their subscription) to the ITRSEC mailing list - please email security@mail.ucf.edu to subscribe or obtain more information
- System Administrators are expected to participate in security training and other activities provided by the Information Security Office (ISO)
- System Administrators are expected to participate on college or school initiated projects (committees) that may impact the Information Technology

Responsibilities of the Departmental Security Coordinators

Departmental Security Coordinators are responsible for ensuring that appropriate computer and communication system security measures are observed in their areas. Departmental Security Coordinators are also responsible for making sure that all users are aware of the UCF's policies related to computer and communication system security.

- Departmental Security Coordinators are expected to communicate and coordinate access to administrative systems for employees in their departments.

- Departmental Security Coordinators are expected to develop and review mechanisms to verify the type of remote access means used by employees and determine whether particular access limitations should be imposed.
- Departmental Security Coordinators are expected to represent university-wide interest in security matters.
- Departmental Security Coordinators are expected to be responsible for coordinating security-related actions enacted by the Information Security Office (ISO) to the university community.

General Administration

- Each user must be made aware of IT Security Policy and Information Technology and Resources Policy of the University
- Individuals aware of any breach of information system or network security, or compromise of computer security safeguards, must report such situations to the systems administrator or the departmental representative responsible for security in that area. The administrator must determine if a security breach has occurred, and if so, must report the incident to the Security Incident Response Team (SIRT) at sirt@mail.ucf.edu
- System Administrators must acquire prior approval, in the form of a work order request, from NOC before making configuration changes or installing network devices, such as switches. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems.
- Each college, school or department should provide Information services for their faculty, staff, and students, thus eliminating the need for them setting up their own services
- Faculty, staff or students must NOT establish their own personal web servers, FTP servers, news servers, electronic bulletin boards, local area networks, modem connections to existing local area networks, or other multi-user systems for communicating information without the specific approval of NOC and Computer Services and Telecommunication (CS&T)
- Enterprise services, such as Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), E-mail, routing, WINS services, firewalls, E-mail relay services, and directory services should be run in cooperation with NOC and Computer Services and Telecommunication (CS&T)
- All servers must be registered with CS&T using the NOC secure server registration page https://newintranet.noc.ucf.edu
- Security protocols, such as SSH and SSL, must be used whenever possible
- Port scanning outside of UCF's LAN is prohibited
- Port scanning within the UCF's LAN is prohibited without the explicit permission of NOC and CS&T
- Packet sniffing is strictly prohibited

Physical Security

- Computing equipment must be placed in an environmentally controlled location (e.g., temperature control, humidity, exposure to water, etc.)
- Computing resources and equipment must be stored in secure locations (server room, wiring closets, etc.) with restricted access
- Printers or faxes used for sensitive data must be stored in a secure location
- Magnetic media such as hard drives, diskettes, or tapes, must be erased before disposal
- A shredder must be used for the disposal of sensitive documents
- UPS is required for networking devices and servers
- Where appropriate security access and authorization documentation must be retained a minimum of three (3) years
- Restricted data, or copy of it, should not be stored on desktops, laptops, handheld, or any portable device (e.g., USB drives, etc.)

System Security

- Only authorized personnel must install applications on a server or workstation
- Administrative access to systems will be determined by the local systems administrator
- System configuration must be done off line. The system must not be connected to the network until it is at an appropriate level of security (see Computer Security Standards and Security Tips for IT for more guidance.)
- Whenever system security has been compromised, or even if there is a convincing reason to believe that it has been compromised, the involved System Administrator must immediately: (a) reassign all relevant passwords, and (b) force every password on the involved system to be changed at the time of the next log-in. If systems software does not provide the latter capability, a broadcast message must be sent to all users telling them to change their passwords
- Operating systems and applications must be kept current. Where appropriate, all the latest operating and application patches must be applied
- Applications must be coded or configured with security in mind
- Security, Account, and System level logging must be turned on when a server is set up
- All unneeded services (e.g., SMTP, Telnet, etc.) must be turned off for network devices, such as printers and computers
- Services not intended for the general user must be protected with a host-based or network-based firewall
- Servers must not be used for general purpose computing, such as web browsing or reading email and must be strictly used for its intended purpose
- The use of fault tolerant system, such as disk mirroring, server duplexing, or RAID is recommended. It is required for servers that store mission or business critical data

- Major applications must be installed on separate servers, e.g., mail on its own server, Web files on a separate server, and in general a database server firewalled from Internet facing servers
- Maintenance and Service agreements with vendors must be kept current

User Account Security

- Each user must have a unique user ID. System administrators must be able to uniquely identify all users, including name, user ID, association, phone number and location. The "Administrator", or "Backup Operator" accounts, for example, are an exception to this rule
- The "Administrator" passwords to mission critical systems must be recorded and saved in a secure location for future reference
- Each user's profile must not be readable, writeable or executable by other users. Access to shared resources should be granted only as needed
- Accounts created for vendors to provide services must only be active during the time the service is carried out
- Accounts must be re-certified annually to ensure that only valid accounts remain active
- All user accounts, where possible, must automatically have the associated privileges revoked after a certain period of inactivity
- Temporary accounts must have expiration dates
- If possible, failed login sessions must be terminated and account locked after three to five unsuccessful tries
- Where possible, concurrent logins must be limited to one
- Additional guidelines regarding Access and Acceptable Use Policy (AUP) may be found in the ADICS Guidelines

Data (restricted)

- Data Classification and Protection Policy #4-006
- when stored in an electronic format, must be protected with strong passwords and stored on secured servers to protect against loss, theft, unauthorized access, and unauthorized disclosure
- when in "hard copy" format or recorded on mobile electronic media, must be stored only in a locked cabinet or drawer in a room or an area where access is controlled by a lock or card reader or that otherwise has sufficient physical access control measures to prevent unauthorized access by members of the public, visitors, or other persons without a need to know
- when transmitted through a data network, must always be protected by using a secure connection method, such as a VPN or SSL
- must not be disclosed to parties without explicit management authorization and then only on a need-to-know basis
- when sent via fax, must be sent only to a previously established and used address or one that has been verified as being in a secured location

- must be accessed using the PID, or similarly secure credential, with a strong password; passwords on systems holding confidential data must be changed every 60 days or less
- must not be posted on any public Web site
- must be destroyed when no longer needed, subject to the records retention schedule. destruction may be accomplished in the following manner:
    - "Hard copy" materials must be destroyed by shredding or another process that destroys the data beyond recognition or reconstruction. After destruction, materials may be disposed of with normal waste
    - Electronic storage media shall be sanitized appropriately by degaussing prior to disposal or by physical destruction of storage media

Mobile Computing

- Security of Mobile Computing, Data Storage, and Communication Devices Policy # 4-007

Terminations and Transfers

- Management must promptly report all significant changes in worker duties or employment status to the System Administrators responsible for user accounts
- Computer access of terminated employees must be deactivated immediately upon notification from the employee's management
- Any files in the terminated or transferred user's home directory should be reviewed
- The user ID's of terminated or transferred employees must not be used by other personnel

Password Administration

- All accounts must have assigned passwords
- Administrators and support staff must never request users to reveal their passwords. If an administrator must sign on to a user's account, the password should be reset to give access to the administrator for support services. The user must be required to change their password after the support service is completed by the administrator
- Network administrators and other support staff are prohibited from disclosing users' ID (e.g., PID) and passwords to anyone
- Users must be forced to change passwords after initial login to a server
- Password history, where possible, must be activated and last six to ten passwords kept
- Minimum password length must be six characters, including special characters and numerals
- Minimum password age, where possible, should be between forty and fifty days

- Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, or in other locations where unauthorized persons might discover them
- Passwords must not be written down and left in a place where unauthorized persons might discover them
- All passwords must be immediately changed if they are suspected of being disclosed, or known to have been disclosed to anyone besides the authorized user
- All vendor-supplied default passwords must be changed before any computer or communications system is used
- Password files must be encrypted
- Additional password standards in ITR must be adhered to
- Additional guidelines regarding Access Control are found in the ADICS Guidelines

Communications

- Encryption should be used when high degree of confidentiality is required for email communication
- Communication software and dialing in through modems attached to a workstation must not be used. UCF provides modem pools and a VPN appliance to connect to UCF's Intranet

Wireless Devices

- Wired Equivalency Protocol (WEP) or WiFi Protected Access (WPA) is not be mandatory on access points
- Sensitive applications must not be hosted on wireless subnets or be transmitted over the wireless network
- No systems on wireless subnets should store or transmit data of a sensitive nature such as credit card numbers, private student information, legal or attorney privileged data
- All users of wireless subnets must acknowledge these policies and agree to abide by them before access is granted to wireless subnets
- All wireless access points will be administered by Computer Services & Telecommunications, Network Operations
- Computer Services must approve any exceptions to the above

Computer Viruses

- To assure continued uninterrupted service for both computers and networks, all desktop systems and servers must have Antivirus software installed and kept current (Unix systems are excluded at this time.)
- Diskettes, flash drives, downloaded files, etc. must be scanned before using them on PCes and servers

Backups

- System Administrators, or backup administrators, must make sure that backups are completed, monitored and tested for effectiveness. Systems should be restorable, after a failure, due to loss of data, or compromise within a short period of time
- Backups should be stored in a secure environment not in the same room as the system
- Backups must be periodically stored in a secure environment offsite
- The number of sets and frequency of backups of a system should be based on the risk analysis of the system, application, or data being backed up
- Backup and restore procedures must be documented
- Backup media must be tested periodically to determine its effectiveness
- Additional guidelines regarding backup procedures are found in the ADICS Guidelines

Disaster Recovery

- Each college, school or department should have a Business Analysis/Risk Assessment plan
- For characterizing risk analysis and sensitivity of data, please refer to the following document: Risk, Sensitivity, and Criticality
- Each college, school or department should have a business resumption plan
- Inventory of hardware, software, service agreements, vendor contacts, personnel information and responsibilities must be maintained
- Business resumption plan should be reviewed regularly
- For disaster recovery and emergency procedures please refer to the following document: Disaster Recovery and Emergency Procedures

Glossary

BNA: Backup Network Administrator

Cisco ACS: The Cisco Secure ACS product line consists of access control servers used to determine who may access the network and what services they are authorized to use

DCE: Distributed Computing Environment. This network security architecture incorporates a version of Kerberos, as well as other facilities such as a directory service

DEN: Directory-Enabled Networks, an initiative formed by Microsoft and Cisco to define a directory schema foundation for common network objects as well as for the use of LDAP as a query protocol

Encryption: A process involving data coding to achieve confidentiality, anonymity, time stamping, and other security objectives

Kerberos: Technology, developed at MIT, which uses encryption to avoid transmitting passwords in clear text over the network

ISO: Information Security Office

LAN: Local Area Network

Mission Critical Data: Data which is vital for an organization to function harmoniously. The unavailability of such data would prevent an organization from functioning

NA: Network Administrator

NOC: Network Operations Center – Responsible for the daily operation of the interconnected networking devices

NSC: Network Security Committee – comprised of members from the UCF community. Deals with assisting, enforcing, propagandizing, etc. of the security policy

NST: Network Security Team – Responsible for network security and the implementation of network security devices

One-Time Passwords (OTP): A System in which a user is provided a new password at regular intervals, usually every sixty seconds. This is one approach to blocking password sniffers. That is to say, never using the same password twice

PGP: Pretty Good Privacy. A public key/private key encryption scheme used to digitally sign messages, encrypt files, or both

Restricted data: Data that are considered sensitive and protected. There are two sub classifications of restricted data: personal and non-personal

> Personal restricted data includes personally identifiable information: a) information from which an individual may be uniquely and reliably identified or contacted, including an individual's social security number, account relationships, account numbers, account balances, account histories, and passwords; b) information concerning an individual that is considered "nonpublic personal information" within the meaning of Title V of the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 11 Stat. 1338) (as amended) and its implementing regulations, and; c) information concerning an individual that is considered "protected health information" within the meaning of the Health Insurance Portability and Accountability Act of 1996 (as amended), and its implementing regulations. Protection for such data may also be subject to additional operating regulations in accordance with vendor or partner agreements, such as the Payment Card Industry Data Security Standards.
>
> Personal restricted data also include the home addresses, telephone numbers, social

security numbers, and photographs of certain university employees, such as police officers and their spouses, as specified in F.S. 119.07(4)(d)1-7.

Non-personal restricted data includes electronic information whose unauthorized access, modification, or loss could adversely affect the university; e.g., cause financial loss or loss of confidence or public standing in the community, adversely affect a partner; e.g., a business or agency working with the university, or adversely affect the public.

Non-personal restricted data also includes security-related information, such as computer passwords and student academic records as defined by the Family Educational Rights and Privacy Act of 1974.

Server: Any computer that provides services to any other computer over a network e.g., Microsoft Internet Information Server, Apache HTTP Server, telnet and ftp server, Norton PC Anywhere, Virtual Network Computing (VNC), Napster, Audio Galaxy Satellite, etc.

SIRT: Security Incident Response Team

SSH: The Secure Shell, being used to protect Unix systems and users. It creates an encrypted channel so the data is not visible as clear text. SSH can use certificates as well

SSL: Provides a "secure" (i.e. encrypted connection) between a web-browser and a web-server so that the data cannot be sniffed

References

Administrative Data, Information, and Computer Security Policy and Guidelines, IT Resource Policy, Data Classification and Protection Policy #4-006, Security of Mobile Computing, Data Storage, and Communication Devices Policy # 4-007

Acknowledgements

I wish to acknowledge the contributions of the following staff members for their assistance in the creation of this document:

Robert Scott, Tim Christopher, Jim Ennis, David Collantes, Matthew Hathaway, Chris Rank, Tony Travaglini, Greg McCoy, Aaron Steimish

Effective Date: 10/16/03

History – New 9/10/01, Amended 10/10/03, Amended 7/11/06, Amended 8/13/07