USFSP Network Security Guidelines

Table of Contents

I. Access to Data

A. Confidential (or sensitive) information is that information which is confidential by law, including information which requires protection from unauthorized access by virtue of its legal exemption from the Public Records Act, Section 119, Florida Statutes. For example: personally identifiable student data such as grades and test results, and personal medical records.

B. Critical information, networks, applications, systems, or data, are those resources determined by management to be essential to the SUS's critical functions.

C. Personal computers or terminals should not be left unattended when the power is on and confidential or critical information is being accessed. The use of this information is to be restricted to authorized personnel only and only for authorized functions.

II. Workstations and Personal Computers

A. Computer Viruses

a. A computer virus is an unauthorized software program or portion of a program that has been introduced into a computer or computer system, or network. The purpose of a virus is to damage data files, expand to utilize available space, delete data, or other harmful actions. Depending upon the purpose of a particular virus, the reformatting of the infected diskette and/or hard drive may be the only method of eradication. This will result in a loss of ALL the data on the disk or drive.

b. Computer viruses are becoming more common every day and the number of viruses being detected has increased. The loading or copying of unauthorized software onto PC's or other machines is one of the easiest ways for them to invade a computer, system, or network. Just using an infected diskette on your PC can spread the virus.

c. Every diskette containing data coming into or leaving the office should first be checked for viruses to guard against these viruses spreading. Several offices have copies of virus checking software. Ask your supervisor or the Campus Computing Help Desk (ext. 3-4357) for the location of the nearest virus checking software.

B. Software

a. All USF St. Petersburg software for personal computers is licensed. Software agreements specify the terms under which software can be copied. You must comply with these restrictions. Contact Campus Computer Services to find out about these terms and conditions.

b. It is suggested that departments consult with Campus Computer Services before installing or copying any software on personal computers. License software agreements must be honored even if the software is not copy protected.
c. Prior to loading software on the network servers at CCS, the software must be checked by Campus Computer Services for the impact on the server and network.
d. Licensed software purchased by USF St. Petersburg is not to be placed on personal computer equipment (i.e., personal computers not belonging to USF). Special conditions may arise (e.g., testing of non-USF software on a university's machine) in which case you should consult with your supervisor and Campus Computer Services first.
e. Loading of software on personal computers at USF is the responsibility of Campus Computer Services. Only software approved by Campus Computer Services shall be supported.
f. Files which are confidential or sensitive are not to be stored on a hard disk. These files are to be copied (backed up) periodically and kept in locked storage when not in use.

C. Hardware

a. Computer equipment (including monitors, system units, printers, keyboards, external disk drives, scanners, key pads, mouse, cables, etc.) shall be located where they will be as free as reasonably possible from damage by water, fire, or other disasters.
b. Computer equipment should be kept in as secure a place as is reasonably possible.
c. Do not have food, drinks or other foreign objects placed near PC's (this applies to all liquids including plant holders that contain water). Crumbs and liquids can cause damage to monitors, keyboards, and other related equipment.

D. Storage Media & Removable Disks

a. Make frequent back-up copies of important data whether you store it on the hard disk or the removable disks!
b. When not in use, all storage media (3 1/2" diskettes, CDs or Flash drives) are to be stored in locked storage if the data they contain is critical or confidential.

Loss of data can occur if removable disks are stored near magnetic fields (telephones or monitors).

c. Follow instructions provided with your storage media for safe and proper use. As with other computer equipment, foreign objects such as food, liquids and dust can cause damage to diskettes. Excessive heat and direct sunlight may also cause damage to diskettes. Valuable data can be lost if diskettes are not handled safely.

III. Local Area Networks (LANs)

A. General Security Guidelines

a. Any office connected to a LAN must accept responsibilities to ensure the proper operation and security of this LAN. The proper operation and security of a LAN is very important when information residing on this LAN is critical to USF St. Petersburg and if the LAN is connected to STPnet (USF St. Petersburg University-wide network). For an office to fully realize the potential of a LAN, it is necessary for members of the office to assume some responsibility for promoting and supporting the LAN.

   i. **Department Responsibilities** - It is required that each office (or the division) designate a permanent staff member to be the LAN Manager/Security Officer to set and enforce local policies and procedures governing the local LAN. A second permanent staff member must be appointed as the LAN Manager/Security officer's backup who will fulfill the positions functions when the Manager is not available. If the existing LAN Manager or backup plans to resign from her/his position in the office or from the University, this person should be made responsible for training a replacement to assume the LAN Manager duties.

   ii. **LAN Manager/Security Officer Responsibilities** - The LAN Manager/Security Officer is responsible for the day-to-day maintenance, security, and support of the office's/division's LAN operation. The LAN Manager must implement appropriate hardware and/or system maintenance schedules that are necessary to ensure the continuous operation of the LAN. Included in the LAN Manager/Security Officer's duties are:

      1. Set-up and administer accounts and passwords on the file server.

2. Set-up and administer network addresses (TCP/IP, AppleTalk).
3. Set-up and administer local mail servers and associated accounts and passwords.
4. Keep system software, virus protection software, etc. for the office LAN up to date.
5. Serve as a resource person for departmental staff, especially for questions related to the management/security of the LAN.
6. Assist office personnel in the set up and maintenance of their computers, and in the installation of new software and software updates.
7. Perform/coordinate backups of LAN computers.
8. Assist St. Petersburg Regional Data Center (SPRDAC) in investigating security breaches.

iii. **Access Security** – Security controls must be provided at three levels of access control: Server, Directory, and File. Each must be strictly enforced. SPRDAC will provide guidance in implementing LAN file server security and in the selection of security products for LAN's.

1. **Server** – Security for log on access to the network and access to file and applications on the server will be implemented via a user ID and password. Each LAN user will be assigned a user ID. Each account must be password protected and password history and password aging must be implemented. Only authorized personnel (students, staff, faculty, and affiliated personnel) shall have accounts assigned. A remote user who does not know a correct ID/password pair should not be able to access the network. User authentication via associated user ID and password might not be possible in some locations, such as computer labs. In such cases, security must be maintained by other mechanisms. Passwords must be chosen by and known only to the individual user responsible for the user ID. Passwords must be non-trivial and users should be given guidelines for choosing strong passwords. The password should not be equal to the user ID or the user's name. Common names, dictionary words, months of the year, etc. should not be used as passwords. Default passwords shipped with

servers, operating system software, or applications must always be changed when the hardware or application is installed or implemented. ID/password files on servers must be encrypted. If possible, passwords should not be transmitted over the network in clear text. It is important to maintain the ID/password directory with current data. LAN access for terminating or transferred employees must be removed immediately.

2. **Directory** – Directory and file security is accomplished via access control rights. These rights should be administered for each LAN user.
3. **File** – There are several levels of file access: Read, Write, Execute, Delete and Add. File access levels should be administered appropriately for users or groups of users depending on what application is being invoked.

iv. **Physical Security** – The LAN Manager/Security Officer has responsibility for the physical security of the LAN hardware. The LAN server should be located in a physically secure area, such as a locked closet or room. The server should not be used as a workstation, except by the LAN Manager for purposes of server administration or in exceptional situations. All cable connections and the cable itself must be in a secure location to lower the risk of inadvertent or mischievous damage to the physical equipment. Standard microcomputer security (such as locking down workstations that are connected to a LAN, and keeping these workstations in secure areas) should be seriously considered. Security awareness should be an important facet in administering a LAN environment. It is important to remember that the most vulnerable security risk in any office could be leaving confidential papers, clearly-named diskettes, and listings in full view in an empty office. Also, walking away from a logged on workstation invites trouble. The use of power-on passwords in workstations where access to the workstation itself requires control is recommended. Where workstations are used by more than one staff member, however, only the manager or supervisor responsible for the area should set or change a power-on password.

v. **Data Security** – It is the LAN Manager/Security Officer's responsibility to monitor access to the data on the network, based on the relative risk and the user's "need to know". Authorization ("who" can see and use "what") requires careful thought. LAN network passwords and the resources to which they provide access may be adequate for sharing documents and data collections, such as mailing lists; however, for more complex databases with confidential contents, more definition is required. In such cases, the application programs should provide the appropriate level of security. This is an application and/or database administration function.

vi. **Backups** –Servers with software, data files, and/or backup data for workstations on the LAN need to be backed up on a regularly scheduled basis. The office LAN Manager/Security Officer is responsible for backing up each LAN and is required to implement a tested and auditable process. This is crucial for recovery from power or hardware failure, data and/or network problems, and physical disasters. If possible, procedures for backup should not require operator intervention. They should be automatic. Backups should be stored on site for quick recovery from data or network problems. LAN backups for critical business functions should also be stored off site. Recovery procedures must be documented and tested. Software installation and upgrade must be done by the LAN Manager/Security Officer or the backup LAN Manager/Security Officer.

vii. **Viruses** – The LAN Manager/Security Officer is responsible for regular scans of each server and computers with hard disks for viruses and security violations.

B. **Security Guidelines for Microsoft Windows Local Area Networks**:

a. **System Login Security Administration** – All accounts must be created by the system administration group. Accounts should be set up with passwords, with the possible exception of lab accounts, or special usage accounts which can be station restricted for security. Passwords must have a minimum of nine (9) characters, be unique and non-repeatable, with periodic expiration. All password accounts should be set up with an expiration date parameter in addition to having several other security options enabled, such as intruder lockout and change password at next login.

b. **Restriction of Sensitive Utilities** – Only the system administration group has rights to implement any of the security policies that are part of the User Manager for Domains utility. The ability to administer users and groups in other domains is controlled by trust relationships which are set up by the administrator. Access rights should be set up on Windows server so that only the administration group has rights to other sensitive areas, such as the registration database, Server Manager and all other management utilities.

c. **Password and File Access Control** – Passwords are established during user account creation and should be created following the secure options available in the creation utility. Access to the file system and other resources is controlled through a security token granted after login authentication and depends on the rights granted via the Access Control List, which is established and controlled by the administration group. Domains are created to administer and control security.

d. **Coordination of Network Problems** – In a Windows enterprise network, there would need to be a central administration group to administer trust relationships and file permissions across domains, in addition to managing other enterprise operations. SPRDAC has implemented a central administration group to administer the NT enterprise network at USF St. Petersburg. A disaster recovery plan should be formulated that includes a definition of what constitutes a disaster and a set of procedures to deal with recovering from various failures.

C. **Security Guidelines for UNIX-based operating systems, such as Linux, Mac OS and Solaris.**

a. **Unix Hosts**: The following are standards and guidelines for securing and protecting UNIX host systems that are connected to STPnet.

i. **Physical Security** – The following vulnerabilities need to be prevented: Unrestricted access to the system, including the power switch/key, the reset button, boot media, and console commands. Unrestricted access to diskette, tape and CD drives. Unattended root login sessions.

ii. **Inter-system Permissions** – The files /.rhosts, /etc/hosts.equiv, /etc/hosts.lpd and local.rhosts files can create vulnerabilities. Care should be taken so that "less secure" hosts are not given access to "secure" hosts. This even applies to system administrators who have personal accounts on multiple systems. File systems for NFS export must not be exported indiscriminately; i.e., a file system must only be exported to an enumerated list of hosts.

iii. **File Permissions** – Permissions on sensitive commands, directories and configuration files should be set so that only authorized personnel have access.

iv. **/etc/services, anonymous ftp, ...** – Configuration of network services should only allow access to services which are needed, and should associate services with secure ports. Services such as anonymous ftp should be set up according to the vendor's instructions.

v. **Installation of Software** – Public domain and user contributed software should not be installed unless it can be complied from source code which can be reviewed.

vi. **Assignment of UID numbers and groups** – Care must be taken so that UID and GID numbers are unique, and that non-administrative users do not have unintended authority. This also applies to software that requires its own userID and/or group.

vii. **Account Usage** – Do not su from another user's account (unless su -) because root would inherit the user's environment. If using vi as root in a user's directory, be sure that you are not vulnerable to any .exrc file in the user's directory. The handling of this varies according to vendor and operating system. Root should not have the current directory in its path.

viii. **Continuing Audit** – Recommend creating a job to run on the system at regular intervals to check various permissions, and UID/GID numbers. Recommend regular review of physical security. Monitor CERT for security advisories. Critical CERT advisories that must be implemented shall be posted on CERT Web pages. Security programs can be obtained from CERT and used to expose security weaknesses via the network. The tripwire program (which checksums system files) should be run periodically to check for unauthorized modifications of system files.

D. **Security Investigations**:

a. At the request of the office/departmental LAN Manager/Security Officer, SPRDAC will assist in the investigation of any security violation. To aid SPRDAC in their investigation, the office/departmental manager/security officer must provide SPRDAC with the following:

i. Timely notice of the violation.
ii. Super user privileges on the machines involved.
iii. Pertinent logs documenting the violation, if available.
iv. Written logs of the installations/updates of system and application software.

IV. Documentation

A. Individual users are the custodians (persons responsible for the care and usage) of software manuals and reference manuals for hardware and related equipment. It is each person's responsibility to take reasonable precautions so that these are not lost, stolen, or damaged. Lost, missing, or damaged manuals should be reported to Campus Computer Services.

B. Printouts that contain confidential or critical information should be handled at all times with security procedures equivalent to the confidentiality level of the information they contain and kept in locked storage when not in use.

V. Contingency Plans

Contingency plans are alternative steps to take when information technology support is interrupted. Contingency plans assure that you can continue to perform essential functions in the event that you lose access to data and equipment resulting from a number of reasons (theft, equipment failure, fire/water damage, unauthorized access, etc).

A. You must contact Campus Computer Services for assistance in obtaining alternate means of computing in case of an emergency. Campus Computer Services has established a minimum arrangement for hardware usage in the event that an interruption occurs at USF St. Petersburg offices.

B. Establish a routine whereby backup copies of removable media are made on a regular basis and stored in a location other than the computer workstation or files are copied to the permanent storage network drive (P:).

C. Server files shall be backed up on a regular basis.

VI. Usernames and Passwords

A. As part of USFSP's personnel procedures, Campus Computer Services must be notified as soon as possible when an employee is terminated or transferred. This should be done by notifying Campus Computing, helpdesk@usfsp.edu or (ext. 3-4357).

B. Passwords must not be posted in public access areas or on the computer itself. Keep them in a secured place. DO NOT SHARE PASSWORDS.

C. Establish a routine whereby security passwords for mainframe access, Banner applications, and functions are changed periodically. Personal computer passwords should also be changed periodically.

D. Employees who access external computer resources (e.g. other Regional Data Centers, SAMAS, FIRN, INTERNET...) are required to follow the security rules and procedures required by those data centers, networks, etc.

VII. Data Integrity

A. Only authorized information shall be entered into USF computers. The input of sensitive or critical information must be accurate and complete and shall be subject to error checking.

B. The input of sensitive or critical information shall be verified for accuracy by comparing what was actually processed against what was supposed to have been processed.

C. The source of data and the "as of" date should be included on all reports.

VIII. Electronic Mail

A. All electronic messages are the property of the State of Florida, unless otherwise protected by statute, as State property is used to send, store and receive this form of communication.

B. In the performance of its duties to the state, USF St. Petersburg may monitor or spot check the contents of electronic messages or methods used by employees. This may include a check on production, efficiency or signs of misconduct.

C. Electronic mail is to be restricted to official use only.