



**INFORMATION SYSTEMS
SECURITY
AWARENESS TRAINING**

Information Systems Security (ISS)

To protect our information and information systems

Information systems security is defined as, "Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats."

A secure information system maintains the principles of confidentiality, integrity, availability, authentication, and non-repudiation.

Confidentiality safeguards information from being accessed by individuals without the proper clearance, access level, and need to know.

Integrity results from the protection of unauthorized modification or destruction of information.

Availability means that information services are accessible when they are needed.

Authentication means the process of verifying a user's identity, or verifying the source and integrity of data.

Non-repudiation means assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Why Information Security Is Your Responsibility

It takes more than anti-virus software to safeguard SFASU computing resources and data. It takes you.

Taking steps to secure your computer not only helps keep your data safe, it demonstrates your commitment to protecting the university network and all data created, stored, and shared over the network by the campus community.

While your department may have staff who provide computer setup and assistance, ultimately you are responsible for taking care of your computer and guarding the information it holds. Following security guidelines and good business practices is part of doing your job. It is the responsibility of everyone who uses a computer at work to protect the University's data. The data on your computer is university property that has been placed in your care. Much of the data we work with is sensitive, such as Social Security numbers, payroll information, grades, and more. **However, all university data needs to be protected.**



Data Classification

Sensitive Information

Information is considered sensitive if the loss of confidentiality, integrity, or availability could be expected to have a serious, severe, or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Types of sensitive information include personnel, financial, payroll, medical, and Privacy Act information, and other information protected by statute.

Non-sensitive Information

Information is non-sensitive if it can be posted internally or externally for all to see, at least with regard to its confidentiality. Note that even non-sensitive information must be cleared before public release. Non-sensitive information usually requires some protection, particularly from unauthorized changes. It is important to note that, in some cases, combining pieces of non-sensitive information could result in a set of information that is sensitive.

Protecting University Data

As an authorized user, you are responsible for contributing to the security of all university-owned computer systems and data. You must abide by the principles of ISS in your daily work routine to protect SFASU information and information systems.

- You are responsible for any SFASU data on your computer.
- You are the custodian of that data.
- This is established in numerous university policies such as :
 - Acceptable Use of Information Resources (F-40),
 - Computer & Network Security (D-8.1),
 - Gramm Leach Bliley Act Required Information Security (D-54),
 - Identity Theft Prevention (C-60)

Your responsibilities

Your responsibilities include:

- Protecting the university property stored on your computer, including information about staff, faculty, students, and alumni.
- Accessing only that information which you are authorized to access in the course of your duties. Your ability to access other information does not imply any right to view, change, or share information.
- Not establishing access privileges for yourself or others outside of formal approval processes.
- Adhering to procedures and business rules governing access and changes to the data for which you are a custodian.
- The university expects all stewards and custodians of its administrative data to manage, access, and utilize this data in a manner that is consistent with the university's need for security and confidentiality.
- SFASU administrative functional areas must develop and maintain clear and consistent procedures for access to university administrative data, as appropriate.

Consequences of Not Practicing Secure Computing

At Stephen F. Austin State University, a wide range of university policies include information relating to computer security and data protection, because of its importance. These policies apply to all faculty, staff, and students. It's your responsibility to know these policies.

- Keeping your computer secure takes vastly less time than recovering from a security problem.
- If your computer is compromised, you will likely lose access to it for at least a few hours, possibly days. You may also lose any work you did since your computer was last backed up.
- If the security problem put sensitive data at risk, or if your computer is lost or stolen, the effects can be far-reaching:
 - You may be held accountable for any negligent action, or inaction, that led to the incident. The individuals whose data is compromised could potentially also suffer financial loss, identity theft, and unwanted public exposure of private information.
 - The university may suffer financial loss as well as loss of reputation.
 - Recovering from a computer compromise or loss of sensitive data, large or small, can take many people many hours and, as a result, is an expensive activity.

Additional Requirements for Computers Storing Confidential Data

If your computer holds confidential data, it must be kept in a secure university location, or it must be physically locked down, or the confidential data must be encrypted. This means that if confidential data is on a computer that ever leaves your office, it must be encrypted. If you are in a location where people could possibly walk up to your computer, your computer needs to be physically secured with a locking cable, or the data must be encrypted.

The same requirements apply to mobile devices, such as smart phones and PDAs and to portable media such as external hard drives, USB thumb drives, CDs, DVDs, tapes, and diskettes. Since mobile devices are fairly small and easy to lose, they can pose a significant risk. If they ever leave a secure location, any confidential data must be encrypted. In addition, only authorized individuals should have accounts on a computer that contains confidential data. If you need to encrypt data, check with your department's technical support staff.



How to protect your identity

Identity theft is a rapidly growing threat, and it thrives on poor security practices. Your best defense is to build good security habits and encourage everyone you know to do the same. If you believe you may be the victim of identity theft, contact your local community law enforcement or the University Police to file a report.

MySFA ID

At universities all across the country, theft of the electronic IDs assigned to faculty, staff, and students, such as mySFA IDs, is a rapidly growing problem.

- Your mySFA ID is your online identity at SFA.
- Used with your mySFA password, it provides access to your personal information and is the key to using a variety of campus services, such as email.
- It may also provides access to other people's university data.
- Keeping your mySFA ID password safe is one way you can help protect everyone's data on campus.
- Part of being a good network citizen is protecting other people's data.



How to Recognize Security Incidents – mySFA ID & Computer Theft

Security problem: mySFA ID Theft

The following are some possible signs that someone has stolen your mySFA password and may be using it, without your knowledge, to commit fraud or other crimes.

- You receive many notifications of undeliverable email messages.
- Your password stops working. This may indicate that whoever stole your mySFA password has changed it.
- You notice changes to how your email is working, or changes to your personal information on university systems.

If you have any reason to suspect your mySFA password has been stolen, you should change it immediately.

Security problem: Computer Theft

Both laptop and desktop computers are subject to theft off and on campus. If your work computer is stolen, immediately report it to your supervisor. They will file a report with the University Police. Do the same if you have lost any portable media, such as external hard drives, USB thumb drives, CDs, DVDs, tapes, or diskettes.

Never leave your computer alone in a public area. Any computer in a public area needs to be physically secured.



How to Recognize Security Incidents – Computer compromise

Sometimes, security issues aren't recognized right away, because it's difficult to tell the difference between your computer's everyday quirks and things caused by a security problem.

The following are some potential signs that your computer may be infected with malware, such as a virus, worm, or other software that allows someone to control your computer remotely. Be aware, if this is the case, the only solution may be to reinstall all of your computer's software.

Your computer may have been compromised if:

- It seems slower than usual, or crashes more often.
- When browsing the web, you see lots of popup windows, or your web browser takes you to a different site than you expected.
- Your anti-virus software, anti-spyware software, or personal firewall reports a problem.
- You receive an email from Information Technology Services alerting you that your network usage has increased significantly, even though you have not been using the Internet more than usual.
- It runs out of disk space unexpectedly

How to Respond to Security Incidents

If you suspect that your computer has been compromised, do the following:

1. If possible, disconnect the computer from the network.
2. Do NOT run anti-virus software on the computer, because it could destroy information necessary to investigate the compromise.
3. Your department's technical support staff. You should always start with your department's technical support staff. They are in the best position to offer immediate help and guidance in determining if you do, in fact, have a security problem on your computer.



Knowledge Check

What can happen if someone breaks into my computer?

- a. Files may get deleted
- b. My personal communications exposed
- c. My computer may be used to gain access to other systems
- d. My computer may be used to commit a crime
- e. All of the above

Knowledge Check

Periodically backing up the contents of your computer in case it's damaged, lost or stolen is good security practice.

- A. True
- B. False

Select all applicable: Confidential information must be encrypted only when:

- A. transmitted through the internet
- B. copied or stored on a mobile device
- C. copied or stored on a removable media
- D. copied or stored on a non-SFA owned device