

Technology Usage Acknowledgement

Before you are issued a User ID and Password to access the SFCC network, you must read this document in its entirety, sign this form, and forward it to the IT Department. Upon receipt of the signed form, the IT Department will issue you a User ID.

I have received, read, understand and will abide by the requirements set forth in the South Florida Community College Technology Usage Guidelines. I will review the guidelines annually for any additions and updates. I understand that the use of technological resources at South Florida Community College is a privilege as opposed to a right or entitlement. I also acknowledge that I will take all necessary steps to ensure the security and safety of the technological resources and data that I may have access to.

Employee Signature

Date

Printed Name

SFCC Employee ID (GID)



SOUTH FLORIDA COMMUNITY COLLEGE

Technology Usage Guidelines

Revised April 2010

South Florida Community College
Technology Usage Guidelines

Table of Contents

Operational Guidelines

User Access and Privileges 1
Acceptable Use for SFCC Employees 3

Security Awareness

Introduction 10
Why is Information Security Awareness Necessary? 10
How Secure Are You?..... 10
Physical Security for Technology Resources 11
Anti-Virus Software 11
Outdated Operating System Software..... 12
File and Folder Sharing..... 12
Backing Up Data Files..... 12
Welcome to the Internet..... 13
E-mail Usage..... 13
Password Protection 14
Why Should I Worry if Someone Has My Password? 15
Privacy of Student and Employee Records..... 16
Copyright or Copywrong?..... 16

South Florida Community College
Technology Usage Guidelines

Definition of Terms

<i>Access</i>	<ol style="list-style-type: none">1. Direct (or local) entry into the SFCC network using a computer or other input device2. Remote entry using communication lines
<i>Application System</i>	Any software that, together, comprises an entire database maintenance system which includes data entry, reports, etc.
<i>Client Application</i>	A program or part of a program that resides and is run from the user's workstation
<i>Network Application</i>	Program or part of a program that resides and is run from the network server
<i>Banner</i>	SFCC's registration, student information, payroll, and etc. application system
<i>Computer System</i>	Any personal computer (PC), workstation, or server on or off the SFCC network
<i>Drive</i>	Storage area either on the local workstation or on a server (appears as a hard disk drive)
<i>Drive Mapping</i>	Assigning a letter (t:, u:, y:, etc.) to network applications or devices.
<i>IT</i>	Information Technology Department
<i>Loading (Software)</i>	Installing software program(s) on a computer for use
<i>Network</i>	A number of connected computers that share information and devices
<i>Network Drive</i>	A drive that resides on a server computer rather than on the local computer
<i>Panther Central Server</i>	Intranet portal used to access information from Banner
<i>Workstation</i>	High capacity PC used to share programs and files
<i>User</i>	Any personal computer (PC) used to access SFCC network
<i>User Profile</i>	Any college employee, vendor, or contractor who has been permitted access to the SFCC network by their User ID and password
<i>User Profile</i>	A configuration for a specific user: rights, permissions, and privileges defined
<i>Panther Den</i>	Desire2Learn (D2L) course management system used for SFCC online classes

South Florida Community College
Technology Usage Guidelines
Operational Guidelines

User Access and Privileges

- 1. New Employee User Access**
- 2. Restrictions**
- 3. Additional Rights**
- 4. Access Hours**

This section is dedicated to User access and privileges. We have provided written instructions for all of the services listed above.

New employee user access is granted after the signed acknowledgement, located at the beginning of this document, has to been returned to IT and Human Resources has notified IT that employment is verified and they have received all required paperwork.

For further clarification of any IT service, contact the Help Desk, and we will be glad to answer any questions you may have. You should also familiarize yourself with the **SFCC Technology Support Manual** for information regarding SFCC technology resources, available support, and request forms.

1. New Employee User Access

As a new employee you will be assigned a User ID by IT. The User ID is typically the first seven characters of your last name and the first character of your first name.

Example: John Community communij
 John Jones jonesj

To avoid duplication of User IDs, there is a possibility that a User ID may deviate from the examples listed above.

It will be your responsibility to follow the IT guidelines in this document when using your assigned User ID.

A temporary password will be given to all newly created User IDs which you will be required to change the first time you log onto the network.

***Note*:** To access your e-mail through the Internet, you must first sign into the network on campus (for more information on e-mail see the section titled "E-mail" in the **SFCC Technology Support Manual**).

As a new employee, you will be permitted to sign onto the SFCC network, use the Internet, use e-mail, and use the college portal Panther Central. This basic access is given without a User Profile. For additional access, your supervisor will need to submit a User Profile: see Additional Rights later in this section.

South Florida Community College
Technology Usage Guidelines
Operational Guidelines

2. Restrictions

Some restrictions are applied to the workstations and User IDs such as:

- Programs cannot be loaded without the assistance or prior approval of IT. This prevents conflicts with standard SFCC installed applications as well as copyright infringements. Rest assured, you will always have the access and privileges that you need to perform your job.
- No network changes or drive mappings (assigning drive letters to a network server or printer) are allowed without IT intervention. This prevents users from mapping drives that can conflict with the standard drive letters that the college uses to run various applications.

3. Additional Rights

If you need more privileges and access than what is given with basic access, such as access to department drives on the network, Banner, etc., your department head must fill out a “**User Profile**” form, which is located in the All Public Folders \ Forms section in the e-mail system. The User Profile form is used to grant rights in the Banner system (view, edit, create information).

If you are granted additional rights, you will be given a home folder on the network (U: drive). This folder will be limited to a size of 50 MB. You may also be granted rights to the R: drive which is for temporary storage only. It can be used to share information with others. **Warning: this is a non-secure drive open to everyone. Information is not backed up by IT and can be deleted by anyone with access to the drive.**

On occasion, “Power User” rights will be given to an employee if specific tasks cannot be executed with standard rights. If you need “Power User” rights you must fill out a “SFCC Computer Self-Administration Policy” form to be considered for these rights (a copy of this form can be found in the **SFCC Technology Support Manual**). You must demonstrate that you have the knowledge to work with the additional rights and privileges. Power User rights can be revoked for misuse. If a Power User needs IT assistance, the service call will follow the normal service call procedure and schedule.

If you need access to the imaging system (OTG), a request form must be completed and forwarded to IT.

Faculty may also receive access to the Desire2Learn (D2L) course management system. For more information, faculty should contact their department chair or the eLearning Department.

4. Access Hours

The network shall be available to college staff seven days a week, generally from 6 a.m. to 10 p.m. Panther Central self-service applications are available 4 a.m – 1a.m. The only exceptions to this would be when maintenance is required for the online servers. Normally, server backups and maintenance software shall run 8 p.m. – 6 a.m. E-mail will be available 6 a.m. – 10 p.m.

South Florida Community College
Technology Usage Guidelines
Operational Guidelines

Acceptable Use of Technology for SFCC Employees

Introduction

SFCC provides computer access and network capabilities through IT. The college relies heavily upon these systems to meet operational, financial, educational, and informational needs. It is essential that these systems and machines be protected from misuse and unauthorized access. It is also essential that SFCC's computers, computer systems, and computer networks, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner.

This policy applies to **ALL** SFCC computer systems and refers to **ALL** hardware, data, software, and communications networks associated with these computers. This policy covers all computers ranging from single user personal computers to those connected to the college's network. In addition to this policy, users of these computer systems are subject to applicable state and federal laws.

Computing resources are valuable, and their abuse can have a far reaching negative impact. Computer abuse affects everyone who uses computing facilities. The SFCC community should exercise high moral and ethical behavior in the computing environment.

SFCC's IT staff will not look at private information, unless authorized by an individual to perform work on his or her behalf or under extraordinary circumstances that may require maintaining the functionality of the system. Extraordinary circumstances include, but are not limited to the following: reading the header of an incorrectly addressed e-mail message to try to send it to the intended recipient, investigations of suspected violations of the college's policies, medical or need-to-know emergencies, financial or legal audits, or when required to comply with law enforcement authorities.

SFCC will only monitor the activities of those that use the campus network or the Internet as it relates to optimizing network performance, unless allegations of improper behavior are brought to our attention by others, or we discover inappropriate activities in the course of investigating problems with network performance. We do routinely monitor traffic levels on the network, to maintain optimal performance, and take note of which individual machines may be generating large volumes of traffic. Routine monitoring is concerned only with load on the network resources and does not seek to eavesdrop on the nature of the information being transmitted.

Policy on the Public Records Law and E-mail

Florida's Public Records Law

Chapter 119 of the Florida Statutes defines public records as:

“All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software or other materials, regardless of physical form or characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official by any agency.”

South Florida Community College
Technology Usage Guidelines
Operational Guidelines

How the Law Affects College Employees

E-mail created or received by college employees in connection with official business, which perpetuates, communicates or formalizes knowledge, is subject to the public records law and open for inspection unless specifically exempted by the Legislature.

If your e-mail falls within the definition of a public record, you may not delete it except as provided by the State General Records Schedule for Community Colleges (Schedule GS5). Furthermore, unless your e-mail is specifically exempt as described by the public records statute, you must produce that e-mail to any person upon request.

Retention Periods for Public Records

Retention periods for public records, including e-mail can be found in the State General Records Schedule for Community Colleges (Schedule GS5). Retention for most e-mail records falls within the following two categories:

1. Retain Until Administrative Purpose is Served:

- Routine announcements and information including notices of seminars and workshops, queries regarding processes or ideas and general information regarding programs;
- Reference files that are general-information files used in daily functions of the administrative area; and
- Meeting notices, minutes, statistical records, reading files and recipient's inter-departmental memoranda.

Retention schedules are based on a record's informational content, not its format. E-mail that falls into the category of "retain until administrative purpose is served" may be deleted on a daily basis. E-mail that has a longer retention period – such as correspondence or sender's memoranda – must be kept through the three-year retention period.

2. Retain for Three Fiscal Years:

- General correspondence, sender's inter-departmental memoranda, and most fiscal and budget records.

It is the user's responsibility to know which category e-mail falls. When in doubt whether to delete or archive your e-mail messages, contact your department chair or administrator.

Guidelines

It is a general policy that technology resources are to be used in a responsible, efficient, ethical, and legal manner in accordance with the mission of SFCC.

Failure to adhere to the policy and guidelines may result in suspension or revocation of the offender's privilege of access to technology resources.

Access to technology resources is coordinated through a complex association of local hardware and software as well as external government agencies, and regional and state networks. In

South Florida Community College
Technology Usage Guidelines
Operational Guidelines

addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines.

1. **Acceptable Use** – The use of your account must be in support of education and research that is consistent with the educational goals and policies of SFCC. Use of other networks or computer resources must comply with the rules appropriate for that network. Transmission of any material in violation of any U.S. or state regulation is prohibited. This includes but is not limited to: violating the conditions of the Educational Code dealing with the student’s rights to privacy, copyrighted material, threatening or obscene material, or material protected by trade secret. Use for product advertisement, political lobbying, personal or private business, commercial, or for-profit purposes are also prohibited.
2. **Privileges** – The use of technology resources and the Internet at SFCC is not a right but a privilege and inappropriate use will result in a cancellation of that privilege. Each individual who receives an account will receive information pertaining to the proper use of the network. SFCC administrators will decide what inappropriate use is and their decision is final. An account may be closed by the administration at any time deemed necessary or recommendation of the faculty or staff.
3. **E-mail “Netiquette”** – You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to):
 - a. Be polite. Do not use vulgar or abusive language.
 - b. Exercise caution revealing personal information over the Internet. E-mail is not guaranteed to be private.
4. **Warranties** – Since Internet connectivity is provided by a third party, SFCC cannot control certain service interruptions. Use of any information obtained through this Internet connection is at your own risk. SFCC specifically denies any responsibility for the accuracy or quality of information obtained through its services.
5. **Authorization and Security** – Security on any computer system is a high priority. If you can identify a security problem, you must notify the security administrator immediately. Do not show or identify the problem to others. Do not allow your account to be used by another individual. Do not use another individual’s account. Attempts to log on as another user may result in cancellation of your privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access. All individuals should not reveal their private address, or phone number or those of others over the Internet. Each user (student, faculty, staff, or authorized others):
 - a. must have a valid, authorized account in areas required, and computer resources which are specifically authorized;
 - b. may only use his/her account in accordance with its authorized purpose;
 - c. may not allow other persons to use his/her account unless authorized by the system administrator for a specific purpose;
 - d. is responsible for safeguarding his/her own computer accounts; and
 - e. should change passwords often to ensure privacy and security.

South Florida Community College
Technology Usage Guidelines
Operational Guidelines

6. **Vandalism** – Vandalism will result in cancellation of your privileges. Vandalism is defined as malicious attempt to disrupt network services, harm or destroy data of another user, or disrupt Internet services. This includes (but is not limited to):
 - a. the creation of, or the uploading of, computer viruses on the network or Internet;
 - b. the installation of software products that monitor network activity
 - c. the installation of software products that monitor and/or record computer activity.
 - d. violation of copyright or patent laws concerning computer software, documentation, or other tangible assets.

7. **Exceptions of Terms and Conditions** – All terms and conditions stated in this document are applicable to all users of the network. These terms and conditions reflect an agreement of the parties and shall be governed and interpreted in accordance with the laws of the state of Florida and United States of America.

The above Acceptable Use Policy and Guidelines have been established by SFCC. If any user violates any of these provisions, his or her access to the network may be terminated and all future access could possibly be denied.

Acceptable Use of Cloud Computing at SFCC

The *Acceptable Use of Cloud Computing* section of this policy provides guidance to members of the SFCC community who wish to use applications and services available on the Web, including social networking applications and content hosting. These tools, which often reside on complex, dynamic networks, are collectively referred to as “cloud computing.”

Internet Applications at SFCC

Internet application and service providers may require users to consent to their Terms of Service, frequently via a “click-through” agreement, which is a legal contract. Faculty, staff, and students are not authorized to enter into legal contracts on behalf of SFCC and may not consent to click-through agreements for the purposes of college business. If individuals approve these agreements, they would be personally responsible in any legal actions related to the services.

College information **must not be stored, shared, or otherwise processed** by a cloud computing service unless the service enters into a legally binding agreement with SFCC (e.g. D2L/Panther Den) which is considered a private cloud computing service that requires the provider to protect and manage the data according to standards and procedures acceptable to the college.

SFCC provides a variety of applications and services that support instructional, administrative and academic research activities by faculty, staff and students while meeting the college’s guidelines. SFCC may have agreements with specific vendors or offer college-hosted solutions that meet your needs. Check with IT for a list of existing campus agreements and services.

South Florida Community College
Technology Usage Guidelines
Operational Guidelines

Challenges with Cloud Computing

Applications and services that are not purchased or licensed by SFCC – including those freely available on the Internet, such as popular social media sites – may not meet college standards for user privacy, security, intellectual property protection, and records retention.

Potential problems with non-SFCC approved applications include:

Intellectual Property and Copyright

Terms of Service from many providers include provisions about who owns intellectual property rights when content is created or uploaded to the application or service that may confuse intellectual property ownership claims.

Note, also, that cloud computing providers may reserve the right to change their Terms of Service at will.

Privacy and Data Security

Security of data uploaded to Internet services is rarely guaranteed. “Free” services frequently depend on data aggregation and data mining about users to attract advertising revenue. The privacy and/or security of that data is then potentially at risk. State and federal law mandate protection of sensitive information such as student data, social security numbers and credit card information.

The college has specific policies and procedures to protect the confidentiality and privacy of student and employee records. SFCC Procedure 2152 deals directly with maintaining the integrity and security of electronic student records including the Family Educational Rights and Privacy Act ([FERPA](#)) and [Florida Statute 1006.52](#). You are required, as a college representative, to abide by these laws.

Data Availability, Accessibility and Records Retention

All SFCC business and educational records are subject to public records law, regardless of where they are stored. However, many providers assume no responsibility for archiving content or ensuring availability, which places the burden on the user to ensure availability.

Additionally, SFCC is committed to ensuring that information, including any materials provided through Internet applications and services, meet reasonable standards of accessibility for all.

SFCC also requires that instructional and administrative records be retained according to the retention periods for public records, as published in the [State General Records Schedule for Community Colleges \(Schedule GS5\)](#).

Best Practices for Using Cloud Computing

Sensible practices apply when using any Internet application.

South Florida Community College
Technology Usage Guidelines
Operational Guidelines

Intellectual Property and Copyright

- Remember that many SFCC images and symbols are owned by the college and not freely available for reproduction. Contact Community Relations and Marketing for more information.
- Remember that students, except in a limited number of circumstances, own their work.
- Ensure that students understand appropriate use of copyrighted materials, particularly when content is publicly available.

Privacy and Data Security

- Never divulge information that the college has classified as “restricted” on the Internet. Examples include social security numbers, credit card information, and driver’s license numbers. Do not place college data on a **public** cloud computing site.
- Comply with FERPA requirements to protect student privacy. Do not place grades or evaluative comments on Internet sites other than Panther Den (D2L). Contact the Office of the Registrar for assistance interpreting FERPA
- Never use personally identifying information without explicit permission, unless the college has classified the information to be “public,” for example, in the college directory (“People Directory”).

Data Availability and Records Retention

- Do not place college data on a **public** cloud computing site.
- Ensure that all data – whether instructional, administrative, or academic research – are retained according to the records retention schedule.
- Ensure that applications or services are accessible to all.
- Back up materials regularly to ensure that records are available when needed, as many providers assume no responsibility for data-recovery of content.

Tips for Faculty

- Communicate the issues, conditions, and risks associated with any tool you choose at the beginning of the academic term, preferably in the syllabus. This allows students who object to withdraw from the course or to request alternate assignments or other solutions. However, be sensitive to the fact that withdrawal may not be possible if the course is required, the course is offered in a sequence, the course is not offered regularly, or the course is only offered by one instructor.
- Restrict online access to student content as much as possible within the context of your instructional goals. In general, course work conducted online should always be restricted to members of the course.

South Florida Community College
Technology Usage Guidelines
Operational Guidelines

- Always require students to use aliases when creating accounts, particularly if access to student work is public. Also, prohibit use of the SFCC Internet name and password as an alias.
- Never include personally identifying information about yourself or your students in content or in profile information online.
- Remember that faculty, students and staff may not speak for the college.
- Manage your social media presence strategically and review it regularly.

South Florida Community College
Technology Usage Guidelines
Security Awareness

Introduction

Although it may sometimes appear that security was designed to make our lives difficult, it is in all actuality designed to protect us. Security is implemented to protect not only you and your data, but also to protect the information resources and student, employee, and financial data of SFCC.

The chief information officer (CIO) of Information Technology is designated as the IT security administrator for SFCC. What this means is that the CIO is responsible for making sure that our network, servers, and computers are safe from viruses, hackers, and any other risks that may be prevalent in this technological age. If you can identify a security problem, it is your responsibility to notify the security administrator immediately. Do not show or identify the problem to others.

This document is designed to help you understand the intricacies, dangers, and best practices of technology security.

Why is Information Security Awareness Necessary?

The mission of the SFCC's Information Technology Department (IT) is to deliver and maintain an information security program that safeguards information assets against unauthorized use, disclosure, modification, damage, or loss.

This is done by educating the college and non-college people about technology security related issues, assisting in strengthening technical measures to protect campus resources, and developing mechanisms to react to incidents and events that endanger the college's information assets.

With the Internet came the free and unimpeded flow of information and ideas. But, that capability comes with high risk from breaches, hacker attacks, and viruses that can take down the network on which administration, instruction, and communication depend. Our passwords, our e-mail, business data, student data, our reputation, and everything we do on a computer, are at the mercy of viruses and hackers if they break into our network.

One thing is clear: While the availability of computing resources is critical to the day-to-day operation of the college, network and data security is everyone's responsibility. It would be convenient if the solution was a piece of technology, and it's tempting to rely on the IT staff to ensure cyber security, but the reality is more complex. A successful security strategy involves technology, policy, and people.

How Secure Are You?

If you were going to take down the FBI Web site, would you do it from your computer using your Internet account? Of course not. People who perform computer crime often use innocent victims' computers as go-betweens in their activities. It's like using a stolen car to commit a crime...guess whose license plate gets turned in.

Indiscriminant vandalism of vulnerable computers is common. Automated worms and viruses don't care whose computer they infect. Many times neither do vandals who deface Web pages and access personnel and personal files. They'll take whatever they can get. More and more often, an automated code installs secret back doors allowing other people to control our computers.

South Florida Community College
Technology Usage Guidelines
Security Awareness

Any computer on our college network is an attractive target. Our high speed Internet connection, lack of restrictive communications barriers, and the large number of lightly monitored computers could make our network an attractive storage and dissemination point for pirated software, illegal copies of movies, and various types of inappropriate material.

Physical Security for Technology Resources

Physical security of technology resources is something that can be easily put in place by each and every department and each individual as well. Take the time to be sure physical security is a priority.

You may think that because a computer (or other technology resource) is on your desk, in an office environment, or located in a lab, that it's secure. This is not necessarily correct. Thus, everyone should take precautions to protect against casual theft and unauthorized access. There are a few simple things that can be done to secure such resources:

- Make sure external and internal doors to offices and/or labs are locked at appropriate times -- especially when unattended.
- Follow IT procedures for moving or repairing equipment so it is not taken under false pretenses. Be sure you know who is taking the equipment. See the "Hardware" topic in the *Operational Guidelines* in the **SFCC Technology Support Manual** for information on these procedures.
- Either log off or lock the computer if you are going to be away from your area for any length of time: don't give someone the opportunity to misrepresent you on the network by using your ID. Encourage others to do the same.
- Students and/or guests should not be left unsupervised in an area where there are computers.
- When using a laptop computer outside the office, be conscious not to leave it unattended. Confidential information could be stored on the hard drive.

Anti-Virus Software

Every year, people who want to be protected from the latest flu virus get a new flu shot. This is because, every year, new flu viruses appear making the old flu shots ineffective.

Similarly, because new computer viruses are released almost daily, our computers need to get new "shots" almost daily to provide continued protection. This is done by updating our anti-virus software.

However, viruses are getting more sophisticated every day. They can open secret doors allowing strangers into our network. They can send out private information. They can delete files on computers. They get better and better at infecting computers and convincing us to help them do it. They increasingly make a mess of the computers and servers that they infect.

No anti-virus software can protect us from all viruses. Anti-virus software is out of date as soon as a new virus is released. During the hours or days after a new virus is released, all the computers in the world are vulnerable until new anti-virus signatures can be created, distributed, and installed. Thus,

South Florida Community College
Technology Usage Guidelines
Security Awareness

even though we're running anti-virus software, it is necessary to use care when opening e-mail attachments or downloading unknown files.

The anti-virus software that SFCC provides to all of its computers will update itself automatically if the computer is connected to the SFCC network. However, not all computers at SFCC, such as laptops, are always connected to the network and, therefore, must be updated manually and frequently.

Outdated Operating System Software

Have you ever had a computer do something it wasn't supposed to do? Crash or hang up or display something oddly? Ever hear of the term "computer bug"? These are all examples of software defects.

Some software defects can enable thieves, vandals, or automated code to take control of computers. Even brand new computers and software often have defects that are discovered after they were shipped.

Software makers regularly release defect fixes. To protect ourselves, all of the computers connected to the SFCC network are updated automatically. Again, computers that are not always connected to the network, such as laptops, must be updated manually and frequently.

File and Folder Sharing

Current operating systems allow us to share folders on our computers should we wish to do so. Unfortunately, a computer can be unintentionally configured to share files and folders that can give away personal information, passwords, or control of the computer. Make sure you don't give away more than you intend. Here are a few tips.

- Never share an entire hard drive.
- Create specific folders to share rather than sharing existing ones.
- Be careful what you put in shared folders.
- Be careful about letting others store files in your folders without a password. Some folks may put objectionable material there. Also, many viruses can use your folders to spread.
- Never store college documents on systems other than college servers.

Backing Up and Storing Data Files

IT operates a set schedule to backup network servers and the data files contained on them (except the R drive). We maintain several backup copies and store them in a safe place. You will, most likely, have files on your computer's local hard drive. If you do, you have an important responsibility to safeguard it, especially if that data contains sensitive or confidential information. Here are some simple practices to follow to ensure that the data you use on a daily basis is safe.

- Back up your data regularly (at least once a week) to your network drive.
- Know how to restore the backed-up data.

South Florida Community College
Technology Usage Guidelines
Security Awareness

- If you have data on removable media (such as CDs or DVDs), shred CDs and DVDs that may contain outdated sensitive information.
- If you have important and/or sensitive information stored on CD or DVD, lock your backup media in an accessible but secure location such as a filing cabinet (a locked, fire-resistant cabinet if possible). Unless otherwise specified, backups should be accessible to an employee's supervisor, and should be stored in a location that can be available in the event of a disaster.

Welcome to the Internet

We all see reports of theft, vandalism, or fraud on television and in the newspaper.

How often do you think such things would occur if there was little or no risk of getting caught or punished, or if the crime could be performed from halfway around the world using someone else's name - in seconds?

Here are some things to keep in mind about the Internet.

- The Internet is made up of more than 300 million people. There are people out there who will take advantage of you.
- Anyone can put anything they want on a Web page. It doesn't make it true.
- If you put up your own Web page, be careful of the type of personal information you make available to everyone on the Internet.
- When you type passwords or personal information into a Web site, the information is available to the owner of the Web site. Only type your SFCC password into official SFCC Web sites. Doing otherwise gives the owner of the Web site instant access to all your SFCC accounts.
- If you have access to Web publishing, be careful how you use it. Today's computers make it easy to publish files to the Web with a couple mouse clicks or a simple drag and drop. It is easy to make a mistake. It is very easy to mistakenly publish your "My Documents" folder to the World Wide Web.

E-mail Usage

Although e-mail is typically only viewed by you and the recipients of your e-mail, there should be no expectation that your e-mail is private. Your e-mail can be printed, forwarded to other users, etc. by its recipients. E-mail is to be used in a responsible, efficient, ethical, and legal manner. Your e-mail should consist of appropriate topics and language that would appear in a formal memorandum or a telephone conversation. As with all other institutional resources, the use of e-mail must be consistent with the educational mission, goals, and policies of SFCC.

South Florida Community College
Technology Usage Guidelines
Security Awareness

Some things to keep in mind about e-mail:

- The name on an e-mail message is about as useful as the return address on an envelope. It can easily be forged by a virus or individual. Keep this in mind when you take action based on e-mail messages. In particular, be cautious about opening attachments, giving out personal information, or altering your computer based on information in the message.
- A newly released e-mail virus can travel around the world and infect thousands of computers before anyone knows what is happening. Anti-virus software may not protect against new viruses and may even be disabled by them. Be cautious about opening e-mail attachments.

E-mail offers many opportunities for security problems. E-mail can easily be forged and does not necessarily afford the privacy one might expect. Here are some things to keep in mind when using e-mail.

- Don't give out confidential information in response to an e-mail. For example, someone may try and persuade you to give out your password or a credit card number. You may not know whom you are dealing with. No reputable organization will send you an unsolicited e-mail message with a program like a patch or software update as an attachment. They will always reference an official Web site where you can download it. Before doing so, make sure it is an official Web site and not something that just looks like one. If you are not sure, contact IT.
- Be wary of unsolicited technical advice. Strangers may suggest certain things that could easily expose your computer to another environment.
- Be wary of mail attachments that you don't know anything about. This also applies to Web downloads. It's very easy for a computer virus to be present in e-mail from people you know and people you don't know. **Although the college uses anti-virus software that checks all e-mail, new viruses are created at an alarming rate, and there is no guarantee that the anti-virus software will catch all of them.**
- If you receive abusive e-mail, it should be reported to your supervisor so action can be taken. It is suggested you do not delete the message, as it can often be useful in tracking down the incident.
- As has been stated before, don't share your e-mail password or keep it written down where it can be easily discovered.

Password Protection

Guidelines for Generating a Strong Password:

- Create a password that contains upper and lower case letters. Put the mixed-case within the password; a single change of case at either or both ends may not be sufficient.
- Create a password that mixes letters with digits. Again, place the digits throughout the password, not simply at the beginning and end.
- Create a password that is easy to remember so you don't have to write it down.

South Florida Community College
Technology Usage Guidelines
Security Awareness

- Create a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.
- Choose a line or two from a song, a poem, a literary title, or use an affirmation. Create a password by using the first letter of each word in the title, etc. For example:
 - Title: "I can do anything I set my mind to" becomes **lcDAismMt**.
 - Choose two short words and connect them. For example: "dogboat," "shockvalve," or "candydown."

Be creative and have fun with it.

WARNING: Do not use these examples!

Guidelines on What to Avoid:

- Avoid using personal information. For example, your name, your user ID, the name of a spouse, child, friend, or pet.
- Avoid using information easily obtained about you, such as license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Avoid using a password made of all digits or repeating the same letter to create a password.
- Avoid using a word contained in any dictionary, spelling list, or other word list in any language.
- Avoid using simple transformations of a word such as reversing the spelling, changing upper case to lower case or vice versa, or using all capitalization. To increase the number of possible password combinations a cracker/hacker would have to guess, be sure to use a password that is at least eight characters long.

Here are some things to remember about passwords:

- **DO NOT** sign on to a computer so that another person may gain access to the network or application systems.
- **DO NOT** write your password on a piece of paper and place it in clear view or under the keyboard or mouse pad. These would be the first places someone would look!
- **DO NOT** disclose your password to any other person.
- **DO NOT** use your SFCC User ID and password on any Web site other than a SFCC Web site or page.

Any of the above actions constitutes a security breach and may, if considered serious enough, subject you to disciplinary action.

Why Should I Worry if Someone Has My Password?

Your user ID and password identify you as you to the server. If someone has your password, that person could pretend to be you while doing unauthorized or illegal things online. For example, you may not care if someone reads all of your e-mail, but you would care if someone were using your account to send e-mail to organize a crime, send a virus, or send e-mail with inappropriate material to someone else. You may not care if someone viewed student data, but you would care if someone used your account to change student data or even corrupt student data (your account name would be "attached" to those actions). Also, someone with your password may be able to make your account

South Florida Community College
Technology Usage Guidelines
Security Awareness

unusable to you. To protect yourself from unnecessary investigation and frustration, it is a good idea to protect your password.

If there is any indication an account has been accessed illegally or if strange things appear to be happening, **immediately** report it to IT, and **immediately** change your password. Protecting your password is one way you can protect yourself from unauthorized use of your computing accounts and files.

Privacy of Student and Employee Records

In March 2005, a thief stole a laptop computer from a major California university office. That laptop contained personal information of about nearly 100,000 alumni, students, and applicants. The university had to notify almost 100,000 people that social security numbers or other sensitive data had been compromised. You may be thinking about our administrative software system as the sole repository of student and employee information. Not so. Sensitive information may reside on your computer's local hard drive in the form of documents, spreadsheets, and databases. Storing these types of documents in your home or departmental directories on the network instead of your local computer's hard drive may lessen the impact if someone were to abscond with a computer from your office. **DO NOT** store files that may contain sensitive information on the "Everyone" drive (drive R:) or on any server other than those located at SFCC or under contract with SFCC as these locations are not considered secure.

The college has specific policies and procedures to protect the confidentiality and privacy of student and employee records. South Florida Community College Procedure 2152 deals directly with the Family Educational Rights and Privacy Act ([FERPA](#)) and [Florida Statute 1002.22](#). You are required, as a college representative, to abide by these laws.

Copyright or Copywrong?

Copyright law states that the owner of any tangible creative work has the *sole* right to reproduce, distribute, perform, display, transmit, or transform that work. Therefore, unless you have the permission of the copyright owner or owners, your use or reproduction of the materials constitutes copyright infringement.

Nearly every original, tangible expression is copyrighted immediately upon creation. An author does not have to register the work, announce that the work is copyright protected, or display the copyright symbol to copyright the work. All he or she must do is create an original work in tangible form.

In fact, very little is not copyright protected. Some things that are not included: works that are not in tangible form, titles, names, symbols or designs, ideas, procedures, methods, concepts, and works that are entirely comprised of common property that has no original authorship such as tape measures and rulers, standard calendars, height and weight charts, and so forth. The only other works that are not covered under copyright are works in the public domain.

When in doubt, assume that a work is copyrighted, and you need permission to use it.

South Florida Community College
Technology Usage Guidelines
Security Awareness

The Internet, most software, including freeware, is NOT in the public domain. All software is copyrighted on creation. The only public domain software available is software that the owner has specifically relinquished to the public domain. Other software covered by copyright is:

- commercial software,
- shareware, and
- freeware.

For commercial software and shareware, you may make an archival copy of the software for backup; however, you cannot use the backup unless you need to recover the original. You may not modify or reverse engineer (decompile) the software. You may not develop new software built on these software packages without the permission of the copyright holder.

For freeware, you may make copies for backup and distribution, but not distribute it for profit. You may modify and/or reverse engineer (decompile) the software. You may develop new software built on these software packages provided the new software is also designated as freeware. You cannot modify or further develop freeware and then sell it.

There are specific penalties for violating the copyright law that you and the college could be held accountable for if you were to violate that law. The following is an excerpt of the law with information that applies to copyrights and the penalties for violations:

“Software is automatically protected by federal copyright law from the moment of its creation. The rights granted to the owner of a copyright are clearly stated in the Copyright Act, Title 17 of the US Code. The Act gives the owner of the copyright “the exclusive rights” to “reproduce the copyrighted work” and “to distribute copies...of the copyrighted work” (Section 106). It also states that “anyone who violates any of the exclusive rights of the copyright owner...is an infringer of the copyright” (Section 501), and sets forth several penalties for such conduct.

“Those who purchase a license for a copy of software do not have the right to make additional copies without the permission of the copyright owner, except (i) copy the software onto a single computer and (ii) make “another copy for archival purposes only,” which are specifically provided in the Copyright Act (Section 117). The license accompanying the product may allow additional copies to be made; be sure to review the license carefully.

“Software creates unique problems for copyright owners because it is so easy to duplicate, and the copy is usually as good as the original. This fact, however, does not make it legal to violate the rights of the copyright owner. Although software is a new medium of intellectual property, its protection is grounded in the long-established copyright rules that govern other more familiar media, such as records, books, and files.

“The unauthorized duplication of software constitutes copyright infringement regardless of whether it is done for sale, for free distribution, or for the copier’s own use. Moreover, copies are liable for the resulting copyright infringement whether or not they knew their conduct violated federal law. Penalties include liability for damages suffered by the statutory damages of up to \$100,000 for each work infringed.

South Florida Community College
Technology Usage Guidelines
Security Awareness

“The unauthorized duplication of software is also a Federal crime if done “willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b).” Criminal penalties include fines of as much as \$250,000 and jail terms of up to 5 years.”

For more information on copyright issues, please refer to the “Software” topic of the *Operational Guidelines* section of the **SFCC Technology Support Manual**.

NOTE: If you have any questions or concerns regarding technology security, call IT at once at ext. 7462.

Adopted: August 2005
Revised: September 2007
Revised: April 2010