

INFORMATION  
TECHNOLOGY DIVISION

# INFORMATION SECURITY

HANDBOOK FOR STUDENTS, FACULTY AND STAFF

JUNE 2006



Fabiola Rubio, CIO/Vice President  
Information Technology Division  
915.831.6392 p / 831.6418 f  
frubio10@epcc.edu

[WWW.EPCC.EDU/IT/SECURITY](http://WWW.EPCC.EDU/IT/SECURITY)

Richard Buller, Manager  
Information Security Office  
915.831.2722 p / 831.6426 f  
rbuller@epcc.edu

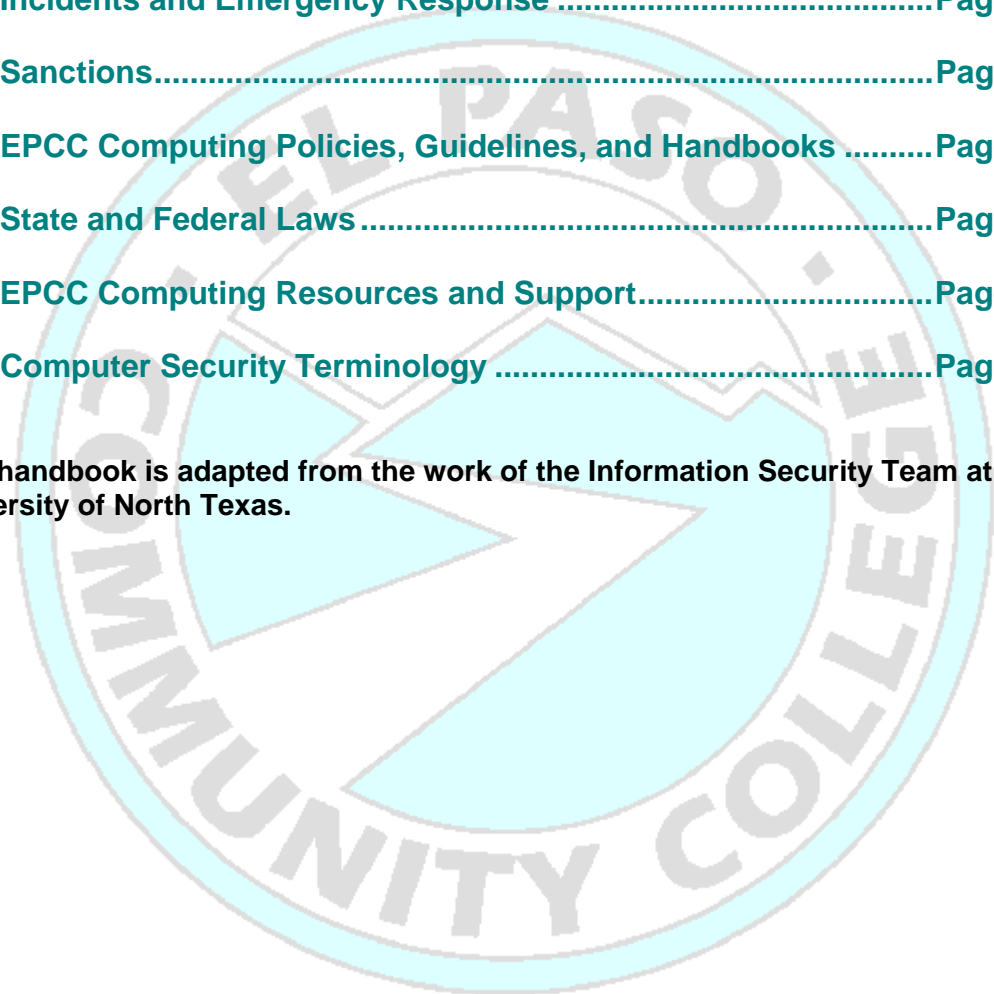
## Table of Contents

<b>1. Overview</b> .....	<b>Page 1</b>
<b>2. Introduction</b> .....	<b>Page 1</b>
<b>3. Security Problems</b> .....	<b>Page 2</b>
<b>3.1 Sharing Computer Accounts and Passwords</b>	
<b>3.2 Failure to Protect Confidential or Sensitive Information</b>	
<b>3.3 Viruses and Worms</b>	
<b>3.4 Hackers</b>	
<b>3.5 People</b>	
<b>3.6 Lack of Contingency (Backup) Plans</b>	
<b>3.7 Copyright and Software License Violations</b>	
<b>4. The Basics of Information Security:</b> <b>Maintaining Confidentiality, Integrity, and Availability</b> .....	<b>Page 5</b>
<b>4.1 Confidentiality and Open (Public Records)</b>	
4.1.1 Protecting Confidential Information about Students	
4.1.2 Protecting Open Directory Information	
4.1.3 Public Information about State of Texas Employees	
4.1.4 How can you help to ensure confidentiality of information?	
<b>4.2 Maintaining the Integrity of Information</b>	
<b>4.3 Ensuring the Availability of Information</b>	
4.3.1 Reacting to a Disaster	
4.3.2 Contingency Plans	
4.3.3 Back-Up Your Files	
4.3.4 Preventing a Disaster	
<b>4.4 Identity Theft</b>	
<b>5. Information Safeguards</b> .....	<b>Page 10</b>
<b>5.1 Password Security</b>	
<b>5.2 Workstation and Computer System Security</b>	
<b>5.3 Physical Security</b>	
<b>6. Responsibilities of EPCC Faculty, Staff, and Students</b> .....	<b>Page 11</b>
<b>6.1 Students</b>	
<b>6.2 Faculty</b>	
<b>6.3 Deans, Department Heads, Managers and Supervisors</b>	
<b>6.4 Owners of Information Resources</b>	
<b>6.5 Custodians of Information Resources</b>	

- 6.6 Processing Managers, Researchers, Persons with Administrative Responsibilities, etc.
- 6.7 Information Security Manager
- 6.8 Auditors
- 6.9 Large Group E-Mail Guidelines
- 6.10 Responsibilities for All Users

- 7. Acceptance of Security Policies and Procedures.....Page 19
- 8. Incidents and Emergency Response .....Page 20
- 9. Sanctions.....Page 21
- 10. EPCC Computing Policies, Guidelines, and Handbooks .....Page 21
- 11. State and Federal Laws .....Page 22
- 12. EPCC Computing Resources and Support.....Page 22
- 13. Computer Security Terminology .....Page 23

This handbook is adapted from the work of the Information Security Team at the University of North Texas.





## 1. Overview

The purpose of this handbook is to help managers and users of information resources gain an understanding of the basic knowledge necessary to protect these resources. Information resources include the procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information. Gaining knowledge about how to protect these resources can ensure that potential for intrusion, alteration, or loss will be less damaging. This handbook should also be considered a guide for learning best practices for securing information resources- it is a guide to help protect against security breaches, unauthorized or improper access to computing resources, unauthorized disclosure of information, and internal and external threats. The responsibilities of EPCC faculty, staff, and students are listed and links to EPCC Computing Policies, Guidelines, and Handbooks, as well as links to State and Federal laws have been included to provide a basis for the standards that governed the development of these best practices.

## 2. Introduction

El Paso Community College depends upon its computer systems and networks in all aspects of its mission, from scheduling classes and registering students to generating employee paychecks. The continued operation of EPCC information systems depends upon appropriate levels of information security. Maintaining this security depends on all employees doing their part.

The security of our information cannot be maintained only through hardware and software controls. Our behavior as users of the computer hardware, software, and information also affects the confidentiality, the integrity, and availability of that information. This document gives the computer user the basic knowledge needed to protect EPCC information and assets from misuse, abuse, unauthorized access or unauthorized disclosure. College assets include the hardware that you use (your office computer, workstations, servers, etc.,) software (operating systems, desktop software, etc.,) and information that the hardware and software allow you to access. Such information may be sensitive or confidential and may have policies or laws that protect its availability, integrity, and confidentiality.

Federal and state laws, network by-laws, and organizational policies tell us how to behave in accordance with security measures. Several tell us, more specifically, what is appropriate and expected. Relevant EPCC policies can be found in the [EPCC Policies with Associated Procedures](#) file.



## 3. Security Problems

### 3.1 Sharing Computer Accounts and Passwords

One of the most common security problems that users encounter at EPCC is unauthorized use of computer accounts, generally caused by sharing their account with a coworker, a friend or a relative. Account and password sharing is prohibited in almost any circumstance. You should not log in as anyone other than yourself, and you should not allow anyone to log in as you. Passwords should never be shared or disclosed to anyone- not even to your supervisor nor should they ever be sent through e-mail. Perhaps you need to access another person's electronic files, calendar, etc -- ask the IT Help Desk or your Microcomputer Support Unit Technician for alternatives. If your job requires you access student or staff records or you would need a Virtual Private Network client account to work from off-campus locations contact your supervisor to begin the authorization process. If you have questions, contact the Information Technology Help Desk by calling 831-6440.

### 3.2 Failure to Protect Confidential or Sensitive Information

Many of us deal with confidential and/or sensitive information on a daily basis. This information might include passwords, EPCC-IDs and social security numbers, performance reviews, student schedules, grades, student payroll information, confidential memos, medical information, credit card numbers, budgetary/financial information, etc. Do you protect this information? How well do you protect this information? Do you walk away from your computer and leave this type of information displayed on your monitor? Do you leave confidential or sensitive documents on your desk in plain view? Do you leave file cabinets containing this kind of information unlocked? Are sensitive documents locked away after business hours? Do you make comments about confidential information to other employees?

Disclosing information to unauthorized employees, contractors, vendors, parents, etc. prevents the information from being used for its intended purpose and circumvents the controls that have been put in place in order to protect the information. Employees must go through the appropriate training in order to gain access to some types of information. (For example, the federal law requires that knowledge be gained about the kind of information about students that can be made accessible. In order to comply with the law, the Registrar's Office offers FERPA training- Federal Educational Rights and Privacy Act- see <http://www.epcc.edu/banner/catalog/catalog05.pdf#page=5> for more information about FERPA). Or, departments require that those who wish to gain access to information or privileges sign statements that the information will be used appropriately. At EPCC, College procedures require that students, faculty, and staff protect the information with which they are in contact.

### 3.3 Viruses and Worms

Viruses and worms are malicious programs that generally cause damage to the information stored on your computer. A virus attempts to replicate itself to documents



and executables on your local computer and resources such as network drives that are connected to your computer. The most common viruses seen in the world today are Microsoft Office macro viruses. Macro viruses usually arrive attached to a legitimate document and execute as soon as you open the document. Once activated, the virus will replicate itself to all the documents it can find and execute its malicious code such as deleting files or modifying the content of your files. Worms are similar to viruses except that they will attempt to replicate themselves over the network. The most common examples of worms are "email viruses" that arrive as email messages, execute and replicate themselves on the local computer and send copies of the message to people in your address book. Frequently, the viruses and worms don't do their damage right away -- they wait until they have the chance to make copies in other locations before they begin to delete files, etc. Because of this, users may use an infected computer for some time before realizing that a virus is present.

All EPCC microcomputers should employ virus protection software to protect against damage from viruses. EPCC has a site license for virus protection software. This software package must be updated regularly to be effective and can be set to perform that update without your intervention. The IT Help Desk will notify you when major updates are available -- do not hesitate to install these. In addition, you can reduce your risk of virus infection by following these practices:

- Never open or view email attachments you are not expecting without verifying the contents with the sender.
- Configure applications, such as Microsoft Office, to prompt you before executing any macros.
- Disable JavaScript and VBScript (Visual Basic Script) in email clients and web browsers.
- To learn about viruses or for additional information, please refer to the United States Computer Emergency Readiness Team's (CERT) [Virus Information Page](#).
- Note that some College applications (WebCT and Off-campus access to the library's Online Databases) require that session cookies and Java applets be permitted.

### 3.4 Hackers

Computer hackers are people who attack or try to gain control over computer systems. For example, a hacker may steal passwords and other secret information, disrupt systems and networks, threaten or vilify others, invade privacy, break into other systems, vandalize, make political statements, or use your computer to set up servers to distribute copyrighted material or intellectual property belonging to others. Frequently, experienced hackers will attempt to gain access to a number of systems at once so that their activities are harder to trace. They may not be stealing your password to access



your research data; instead, they merely want to use your computer as a launching point for attacking another computer.

Especially challenging is the fact that hackers invent programs that do their dirty work automatically, and they share these programs with other hackers. A hacker might start a program that searches every system on the Internet for a particular security hole. When the program discovers a machine with that hole, it compromises the machine, installs "backdoors" for future access, and then it proceeds to check other machines. Fortunately, there are several groups of "good guys" who publish information about these activities and how to "patch" the holes. The [Computer Emergency Readiness Team](#) at Carnegie-Mellon is probably the most famous of these.

### 3.5 People

More common than not, people are more of a threat to security than any other source. People can make mistakes which cause the integrity of data to be questioned, weaken the physical security of computer systems, or even cause systems to crash. Some people intentionally cause security problems. These kinds of people are called hackers, but they could just as well be disgruntled employees.

Other kinds of people weaken security through negligence. These kinds of people share their computer accounts, share their computer passwords, choose weak, bad passwords, don't back-up their files, don't lock their office doors, don't log out when away from their computers, etc.

Then there's the "missing person." This person is unavailable for extended periods due to illness, termination or even death. Can you find important files if your assistant is unavailable? Contingency plans should be made available and kept up-to-date for these kinds of events.

### 3.6 Lack of Contingency Plans

Disasters can strike at any given moment. Can you confirm that you have adequate plans in place to address how your department (or the areas which you are responsible for) would operate in the event of a fire, flood, tornado, earthquake, loss or unavailability of computer resources, missing personnel, telecommunications outage, etc.? It's important to have contingency plans in place that address how critical operations would continue in the event that one or more important services become unavailable. The plan should provide for short and extended periods when these services are not available. See "Basics of Information Security: Maintaining the Confidentiality, Integrity, and Availability of Information" for more details about contingency plans.

### 3.7 Copyright and Software License Violations

The majority of software and other copyrighted documentation or works have usage restrictions included in either their copyright or license agreements. It's important for all users to make certain that they comply with the regulations stated in these agreements. Some licenses or copyrights strictly prohibit software, media, works or documentation



from being reproduced or distributed inappropriately. Some agreements require permission from the owner of the copyright before the item can be reproduced, while some software licenses strictly prohibit duplication at all. Some software copyrights limit usage to a single computer, while other types of software may be copied or downloaded onto more than one computer.

Since it's unreasonable to be able to guess what the copyright or license requirements are, you should find out what the copyright laws actually state and make certain that license agreement regulations are strictly followed. It's also important to make certain that software license agreements are kept on hand- near the computer on which the software resides.

## 4. The Basics of Information Security: Maintaining Confidentiality, Integrity and Availability

### 4.1.1 Confidentiality and Open (Public) Records

Most types of college information (records) are defined as either "Confidential" or "Open" (public) within [EPCC Policy 3.03.03, Records Retention](#); [EPCC Procedure 7.01.00.10, Admission Criteria](#); and [EPCC Procedure 7.01.00.14, Admission and Enrollment Requirements for Non-U.S. Citizens](#). Information that is classified as confidential cannot be disclosed or disseminated to the public (people who aren't employees of the college with a need to know this information). Much of the information about our students (grades, financial aid status, Social Security numbers, EPCC-ID number, etc.) is confidential.

### 4.1.2 Protecting Confidential Information about Students

All of us--faculty members, custodians, secretaries, computer support staff, vice presidents--have a responsibility to protect information about our students from public disclosure. It doesn't matter whether this information is on the central computer, on a printout, a computer screen, a diskette, a CD-ROM, etc. The Family Education Rights and Privacy Act (FERPA) of 1974, guarantees students the right to protect all information that is not classified as "open directory" information. Some of the records, other than student records, which are designated as confidential include:

- Apprenticeship Records (Internships)
- Application Records
- Client Records (From Institutes)
- Counseling Notes
- Employee Insurance Files
- Employee Security Records
- Federal Tax Records
- Fines Records, Paid and Unpaid
- Fingerprint Cards
- First Report of Alleged or Occupational Disease
- Investigation Records



- Legal Case Records
- Library Circulation Records
- Medical Records
- Reports- Laboratory
- Request for Name Change- Employee
- Request for Student Transcripts
- Request for Tuition Assistance
- Research Data
- Statement of Truth-in-Lending
- Veterans Administration Records

### 4.1.3 Protecting Open Directory Information

Open Directory Information about Students (this information may or may not be flagged to be "withheld from the public"--check with the Registrar's Office to be certain):

- Student's full name
- Address (local, permanent, and e-mail)
- Telephone listing (local, permanent)
- Birth date, birth place
- Major field of study
- Dates of attendance
- Degrees and awards received
- Most recent/previous school attended
- Classification
- Participation in officially recognized activities and sports
- Weight and height of athletic team members
- Photograph

Some students request that open directory information also be withheld from the public. These students are identified within the Student module of the EPCC Banner Administrative Information and Management System (AIMS). Please see [FERPA Compliance at EPCC](#) or contact the Registrar's Office for additional information. All EPCC employees who regularly deal with student information should attend FERPA training, available through the Registrar's Office. Open directory information includes general information (as listed) but ALL OTHER STUDENT INFORMATION IS CONFIDENTIAL!

### 4.1.4 Public Information about State of Texas Employees

Unless otherwise restricted, the Texas Public Information Act (also known as the Texas Open Records Act) does not prohibit the disclosure of the records of Texas state agencies- this includes colleges and universities. Information about employees who work for Texas state agencies (including EPCC) can be disseminated to the public. This information includes (but is not limited to):



- Name
- Sex
- Ethnicity
- Salary
- Dates of employment

Employees may restrict disclosure of their social security number, home address, and home telephone number, by filling out an Employee Biographical Data form (available from The Personnel Office). Requests for information from the public should be referred to the Office of the President. Visit the Texas Attorney General's web site at: [http://www.oag.state.tx.us/AG\\_Publications/txts/2004publicinfohb\\_toc.shtml](http://www.oag.state.tx.us/AG_Publications/txts/2004publicinfohb_toc.shtml) for more information about the act.

#### 4.1.5 How can you help to ensure confidentiality of information?

- When in doubt don't give it out!
- Identify confidential information as "CONFIDENTIAL" on the print-out pages, diskette, screen, etc.
- Choose good passwords, and keep them secret. Passwords are confidential too!
- Log out and/or lock the office when you're away from your desk.
- Don't permit another person to use your computer account.
- Use special care when posting grades (assign random numbers, don't use part of Social Security numbers).
- Secure print-outs and other documents. Retrieve your print-outs as soon as possible.
- Don't leave confidential or sensitive documents laying out in plain view.
- Use CONFIDENTIAL paper recycling bins. Make sure discarded diskettes and tapes are unreadable.
- Attend FERPA training- send your student workers too!

#### 4.2 Maintaining the Integrity of Information

Is the information accurate? Is it complete? How do we know?

Unless our information is accurate and complete, it's pretty much useless and it may even be dangerous. Almost all of our data is sensitive in this respect. Grades, salaries, research data, and most other records and documents must be protected from unauthorized modification or destruction. How?

- Check your work for accuracy and completeness.
- Choose good passwords, and keep them secret.
- Log out and/or lock the office when you're away from your desk.
- Don't permit another person to use your computer account.
- Use virus detection/protection software.
- Make sure you have backups (on paper, diskettes, tape, or file server).
- Control (specify, understand, document) who has access to the data that you manage.



- Control what kind of access they have. Can they update some or all records? Can they update only some parts of a record or all parts of a record?
- Check references when hiring.

## 4.3 Ensuring the Availability of Information

### 4.3.1 Reacting to a Disaster

Every office should have a contingency plan to address possibilities such as fire, theft, water damage, vandalism (including data loss from virus or hackers), loss of a key employee, hardware failure, network unavailability, etc. Information Technology must plan for the loss of the main computer servers and other central systems. Other departments must plan how they will cope if their own systems are damaged, or if central systems are unavailable for an extended period (perhaps weeks or a month or more). Plans should address the most critical functions, such as registering students, paying employees and vendors, disbursing financial aid, email services, etc.

### 4.3.2 Contingency Plans

Contingency plans are basically made up of procedures and lists. Sometimes simple plans are the best and they're certainly better than no plan at all. Procedures should address how to accomplish basic tasks without computers/networks: who does what, what should be done first/second/..., how do you restore files from backup, etc.

Lists should include:

- Key personnel contact information (telephone/cell number, pager numbers, etc.)
- Critical data, hardware, and software
- Critical documentation
- Critical supplies and equipment
- Vendor contact information (telephone number, address, contact name, etc.)
- Emergency procedures (evacuation plans based on type of disaster, test dates, etc.)
- Storage location of critical back-up data
- Date of the last review of the contingency plan

A contingency plan is never really "finalized." Some of the information in the lists change frequently and should be updated and disseminated. Departments should test their plans periodically to ensure that the contingency procedures are still practical, files can be restored, etc. Plans should provide alternatives for short term as well as extended periods when critical resources may be unavailable. See the [Checklist Criteria For Business Recovery](#) (sponsored by FEMA) guide for general assistance in developing a contingency plan.

### 4.3.3 Backup (Make a duplicate of) Your Critical Files

In the event of a disaster, will you be able to recover the files that have been lost? Your files (electronic data, e-mail correspondence, etc.) should always be backed up (copied)



and placed in a secure location- especially those files that you do not use on a daily basis, yet may be critical to your office operations. Here are a few ideas to help you with the Backup process:

- Add "Backup Files" to your weekly or monthly "to-do" list.
- Know how often the files on your department's file server are backed-up.
- Backup what you can't replace on your hard drive.
- Backup, or "archive" your important e-mail messages (see your computer support person if you need assistance).
- Keep a Backup in a secure location- somewhere other than your office.
- Make use of folders or directories to simplify the Backup chore.
- Use version numbers in filenames, keep several recent versions.

If you need assistance, contact the Microcomputer Support Technician for your campus.

#### 4.3.4 Preventing a Disaster

Several measures may actually help to prevent a disaster. These could include:

- Perform periodic risk assessments to determine what is vulnerable.
- Have an up-to-date contingency plan in place.
- Make sure your critical files are backed-up up at least once a week.
- Ensure the physical security of your office/computer areas.
- Choose good passwords and keep them secret.
- Log out and/or lock the office when you're away from your desk.
- Do not allow any other person to use your computer account.
- Use virus detection/protection software.

#### 4.4 Identity Theft

Your personal identity information exists in EPCC databases and is protected by technology tools in the form of hardware and software, physical security protective measures, passwords to control access and procedures and standards to guide the routine operations that use and maintain this information. However, complete security protection is never achieved and we must all be aware of the threats to college and personal information. Theft of personal information has become a daily occurrence around the world and will, eventually, involve every one of us through incidents at home, at work, the financial institutions we use, the public utilities to which we subscribe for services, and many other possibilities. Identity theft is a federal crime. It occurs when one person's personally identifiable information (PII) (which can include name, social security number, or any account number) is used or transferred by another person for unlawful activities. Numerous identity theft resources are available at <http://www.privacyrights.org/identity.htm#ITRC>. For a list of personal data breaches, visit <http://www.privacyrights.org/ar/ChronDataBreaches.htm>. The Federal Trade Commission provides clear instructions on the proper actions to take if you believe your personal information has been compromised. This site has information in both English and Spanish. Visit <http://www.consumer.gov/idtheft/>.



## 5. Information Safeguards

### 5.1 Password Security

#### Select a good password:

- Don't use a common word, a friend's name, a pet's name, your nickname, the name of your favorite team, etc. Co-workers, friends, and even casual acquaintances, may know this information.
- Use a combination of letters, numbers and special characters (\$, \*, !, etc.).
- Use the first (or second, or last) letter of each word in a phrase.
- Use UPPER and lower case characters.
- Select something that you can remember. A good way of doing this is to use a mnemonic to remember your password, such as the name of your first grade teacher plus your mother's age at your birth plus a tilde ("hoLlins23~")
- Use a different password for each system.
- Choose passwords that are a minimum of eight characters in length.

#### Change your password:

- When you first receive your computer user-ID. Remember to destroy any paperwork that lists the account user-ID and password.
- When you suspect that someone else may know it. (Keep your password secret!).
- Periodically (EPCC production systems should be changed every 120 days).
- Never re-use an old password.
- Try not to write down your passwords, but if you must, keep the written password in a secure location and be sure to change all passwords if you suspect your passwords were viewed by anyone else.
- Do not identify a password as being a password or reference the system to which it links.
- Do not attach the password to a terminal, keyboard, or any part of a computer.
- Never record a password on-line and never send a password to another person via electronic mail.
- Destroy any paperwork that lists your account, user-ID or user names and passwords.

#### Don't be a victim of "social engineering:"

A frequent cause of loss of password security is "social engineering" - a deliberate attempt by someone to obtain your password through deception. To prevent such loss of your password:

- Never reveal your password to anyone else.
- Help desk personnel, network managers, or computer support personnel should never have occasion to need your password to diagnose problems.



- Don't reveal your password over the telephone, via e-mail, etc.
- Make sure that no one is peering over your shoulder when you type in your password.

## 5.2 Workstation and Computer System Security

You can increase the chances that your computer will not be attacked by an intruder by learning how a computer can become vulnerable to attack. To learn more about the attacks on computers and how to avoid them, read "[Top Ten Cybersecurity Tips](#)". Take the quiz at <http://www.staysafeonline.info/home-quiz.html>. Faculty and staff members should contact their network manager or system administrator for assistance in implementing the suggested recommendations. Visit this [Microsoft](#) site to learn about the latest threats and protective measures for the Windows desktop environment.

## 5.3 Physical Security

The physical security of computing resources (computers, equipment, files, etc.) is actually the first principle of good security, because as long as someone can get to your computer he/she can gain control over it. By instituting a few simple safeguards, we can greatly limit security breaches and other unauthorized access to our computing resources. You may be held financially responsible for property assigned to you and lost or damaged. This property includes (but is not limited to) computers, pagers, cell phones, etc. Here are a few helpful hints to safeguard the physical security of items that are your responsibility:

- Log out when leaving your computer.
- Close and lock your office door every time you leave.
- Don't leave your office keys in easily accessible locations-secure them.
- Restrict the number of keys to your office.
- Know who accesses your office. (It may be necessary to maintain an attendance log for high security areas.)
- Use a screen-saver, and one that requires a password to get back into your computer after the screen saver activates.
- Keep your passwords and computer user-ids or user name a secret.
- Report suspicious looking persons or activity to the EPCC Police Department.
- Express any concerns about physical security in writing.
- The EPCC Police Department provides courtesy physical security inspections by request. Tell your supervisor.

## 6. Responsibilities of EPCC Students, Faculty, and Staff

### 6.1 Special Responsibilities for Students

Many computing services are available to EPCC students, including:



- Use of Academic Computing Services computer laboratories.
- Online registration.
- E-mail account.
- Access to the EPCC Library's online databases from off-campus.
- Assistance from Help Desk personnel.
- Use of these services is a privilege granted to the members of the College community. In turn, users agree to abide by the applicable policies and procedures of EPCC, as well as federal, state and local laws.

Here are some general guidelines to help students comply with these policies and laws, and to keep these valuable resources functioning and available to all who need them:

- Be aware of the thousands of others who depend on the College's computer systems, network, and the Internet to do their work. Consider how your computer behavior will affect them and choose what you know is right.
- Understand that College policies address academic dishonesty, including theft, disruptive conduct, and misuse of materials and property. These policies apply to computing activities as well as activities in the classroom, residence halls, or elsewhere on campus.
- Don't copy software unless specifically authorized.
- Don't let other students, relatives, or any other person use your computer account(s). You will be held accountable for any abuse of computing resources by persons you allow to use your account.
- Protect your password -- keep it secret and change it regularly. Choose your password wisely. It is not uncommon for students to steal other students' passwords for the purposes of performing prohibited acts.
- Understand what you are authorized to do. Know that your computer accounts are provided so you can send and receive mail, read and post notices to new groups, and access library and other information resources. Academic Computing Services computers, networks, and printers are available to you so that you can do word processing, make spreadsheets, and access College computer services and the Internet.
- In some cases, your professors will authorize access to additional resources so that you can do class assignments. You can use EPCC computers as long as your activities add no additional cost to EPCC and as long as you continue to obey the procedures, standards and laws.
- In general, you cannot use EPCC computers for commercial purposes.
- Understand that the privacy of messages you receive and files you create is limited. Although your use of College computers is not generally monitored, there may be circumstances (hardware failure, hacker attacks, etc.) in which



computer system administrators may need to look at information and files to solve problems and protect systems. (System administrators should treat any information they might see that turns out to be unrelated to the problem as strictly confidential).

- Comply with reasonable requests and instructions from the computer system operator/administrator. (A system operator/administrator should NEVER ask for your password. If a request seems unreasonable, verify the identity of the person claiming to be a system operator or administrator).
- Don't "hack" (disrupt computers systems and networks, send forged electronic messages, invade the privacy of others, steal other people's passwords, etc).
- Report security problems immediately to your instructor, system administrator, the Information Security Program, or other appropriate College authority.

## 6.2 Special Responsibilities for Faculty

Take a minute to talk to your students about information security:

- Ask them to refrain from sharing EPCC computer accounts.
- Teach them how to select good passwords.
- Remind them to periodically back up their files and scan for viruses or worms.
- Direct them to other relevant sources of information, such as the Student Code of Conduct.
- Remember to protect student information when posting grades, etc.
- How to properly use and protect notebooks from the mobile cart.

## 6.3 Special Responsibilities for Deans, Department Heads, Managers and Supervisors

Management should restrict the number of persons granted privileged access to a minimal practicable number, then tell the person who is responsible for overall administration of a system the names of those persons and what functions those persons have been assigned. Persons who are to be given privileged access to a EPCC computer system should be selected (or approved) by the head of the department that owns or manages the operation of the computer system or by another member of management to whom this responsibility has been delegated.

Granting privileged access to EPCC computer systems represents an investment of trust. Persons who are to be given such trust by management should be selected carefully, based on personal characteristics of honesty, integrity, and dependable work habits. The manager should clearly define the job responsibilities of each person selected for privileged access to avoid ambiguity over what the privileged user should or should not be doing.



Final responsibility for the security of computer resources rests with the management of the organizations that own or control them. It is the responsibility of management to comply with all computer security standards in force at EPCC and to conduct themselves in a manner that will foster security awareness and understanding among users.

Ensure adequate training opportunities for your staff. Remember, some staff may need more instruction than others, especially when it comes to scanning for viruses, organizing files into directories or folders, backing up files to diskette or tape, etc. Document, in the EPCC Classification and Compensation Job Description, any special security responsibilities for a particular position. Responsibilities should be commensurate with position's authority.

Try to carefully assess applicant's trustworthiness before hiring. Notify the appropriate system administrators to disable user-IDs when an employee terminates employment at EPCC. If the termination might be hostile, request that the user ID(s) be disabled immediately. See the EPCC Procedure 2.05.01.66, "Access Management: Employee Separations and Absences." This procedure requires the IT Help Desk be notified so all granted access can be withdrawn and accounts disabled.

If you supervise a system administrator (network/file server manager, other multi-user system manager), review the EPCC Information Security Handbook for Students, Faculty, and Staff with that person.

Promptly report ongoing or serious problems regarding computer use.

## **6.4 Special Responsibilities for Owners of Information Resources**

Most of the administrative information stored on EPCC computing systems is owned by the El Paso Community College. Various administrative units are assigned to own and control the College's data files that are primarily created and processed within their program areas. For example, the Registrar's Office controls student records; the Personnel Office manages employee records; and the Comptroller's Office oversees the College's financial data. These "owner designees" are responsible for specifying and approving appropriate security controls for the administrative data. Owners of information resources assign custody of EPCC data assets to data custodians (programmers, system administrators, etc.) who implement the controls based on values that they (owners of information resources) have determined. Controls may be specified at various levels (by owners), including:

- Whether records may be viewed only, or viewed and updated
- Whether all records may be viewed, or only a portion of all records
- Whether the entire record may be viewed, or only certain fields (such as name, Social Security number, birth date, etc.).



For many of the larger databases, such as employee or student records, a feature of the Banner Administrative Information and Management System enables the owner designees to manage these complex security specifications. For further information, contact Information Technology for an overview of the security features of the system.

## **6.5 Special Responsibilities for Custodians of Information Resources (System Administrators, Data Processing Managers, Researchers, Persons with Administrative Responsibilities, etc.)**

The "custodian of an information resource" is the unit charged with the physical possession of certain data. Custodians are normally technical managers, such as the operators or managers of a multi-user, central or departmental computer system, server, or network of microcomputer workstations. However, persons who maintain internal departmental data about faculty, staff/student employees, or students (i.e. personnel/payroll information, etc.) using departmental resources (databases, spreadsheets, documents, etc.) are also custodians of the information they manage, and, the end user is the custodian of his or her individual workstation.

Certain designated persons are given broader access to the resources of computer systems because their job responsibilities require such access. Typically, such persons are responsible for providing administrative services on the designated computer(s), services such as system maintenance, data management, and user support. The term "broader access" covers a range -- from wider access than given to an ordinary system user, up to and including complete access to all resources on the computer system.

Responsibilities include:

- Control physical and login access to College computer resources under its possession. Security controls for these resources shall take into account local, state and federal reporting and auditing requirements, as well as provisions to eliminate, as far as is feasible, the incidence of theft, fraud, destruction, or other abuses of College computer resources.
- Take appropriate measures to protect the data from loss due to natural disaster, hardware failure, user error, and system contamination (e.g. computer virus) or other malicious activities. The custodian should archive the data located on the EPCC computer system in accordance with operational and data archival procedures.
- Ensure that, if possible, the process by which a user accesses the resources of their computer resources of their installation displays a message regarding a user's responsibility to comply with the provisions of this policy.
- Enforce compliance with provisions of software licensing agreements and other computer resource contracts for the computer installation. Reasonable steps should be taken to not permit unauthorized copies of computer software and manuals to be obtained.



- Report security problems to the Office of the Vice President for Information Technology/Chief Information Officer or the Information Security Manager.

Persons given broader-than-normal access privileges on EPCC computer systems agree:

- Not to "browse" through the computer information of system users while using the powers of privileged access unless such browsing: is a specific part of their job description (e.g., an auditor); is required during file system repair, management, or restoration; is necessary to investigate suspicious or system-impairing behavior; or is specifically requested by, or has the approval of, the person who authorized their privileged access. Browsing should never be done unless it is in the best interest of EPCC.
- Not to disclose, to any unauthorized person, computer information observed while operating with privileged access.
- Not to copy any computer information for any purpose other than those authorized under their defined job responsibilities.
- Not to intentionally or recklessly damage or destroy any EPCC computing resources.
- Not to accept favors or gifts from any user or other person potentially interested in gaining access to EPCC computer systems.
- Not to do any special favors for any user, member of management, friend, or any other person regarding access to EPCC computers. Such a favor would be anything that circumvents prevailing security protections or standards.
- Not to tell or disclose to any unauthorized person the information required to gain privileged access, or to engage in careless practices that would reveal that information to unauthorized persons.
- Not to attempt to gain or use privileged access outside of assigned responsibility (e.g., on other machines) or beyond the time when such access is no longer required in assigned job functions.
- Not to change or develop any computer software in a way that would (a) disclose computer information to persons not authorized to have it, or (b) make it possible to retain any special access privilege once that authorized privilege has been terminated by management.
- Not to make arrangements on computer system(s) under their charge that will impair the security of other systems. In order to comply with this restriction, a system administrator setting up authorized networking connections should make use of available controls and protections as fully as reasonably possible.



- Report all suspicious requests, incidents, and situations regarding a EPCC computer to an appropriate member of local management, Internal Audit, EPCC Police, and/or to EPCC FIRST (Forum for Incident Response and Security Teams).
- Use all available software protections to safeguard computer system(s) under their charge from unauthorized access by any person or another computer.
- Take steps to the best of their ability to comply with all computer security standards and policies in force at EPCC and furthermore, advise management and/or designated computer security representatives at EPCC of deficiencies in these standards.
- Conduct themselves in a manner that will foster security awareness and understanding among users.

## 6.6 Special Responsibilities for the Information Security Manager

- Ensure that adequate security procedures, including backup, disaster recovery, and contingency planning, have been formulated for the centrally administered computer systems.
- Coordinate the implementation of security procedures, including backup, disaster recovery, and contingency planning, for the departmental computer systems and personal computers.
- Establish mechanisms for monitoring compliance with and violations of EPCC computer resource security policies and standards.
- Establish procedures for investigation, logging, and management reporting and follow-up of access violations.
- Perform periodic risk assessments and security audits of existing and proposed systems.
- Oversee the development and maintenance of a comprehensive handbook and individual information security standards to implement College computer resource security procedure and standards.
- Oversee the development of training courses for training employees in EPCC computer resource security policies, standards, and procedures.
- Gather information from the Information Resource Custodians and report as necessary and appropriate.



## 6.7 Special Access for Auditors

There will be occasions when auditors require access to EPCC computer resources and data files. The access should be permitted in accordance with these guidelines.

Auditors from the El Paso Community College:

- Shall be allowed access to all College activities, records, property, and employees in the performance of their duties.
- Shall notify the Vice President for Information Technology/Chief Information Officer prior to accessing individual data files.

State and Federal Auditors: Will be granted access to College computer resources and data files on an as needed basis, as approved by the President.

## 6.8 Large Group E-Mail Guidelines [see El Paso Community College Policy 2.05.01.34 – EPCC E-mail Policy for more detailed specification]

All Vice Presidents and the Chief Information Officer recommend the following guidelines for using large E-mail groups:

- Departments and individuals should be judicious in sending E-mail to all faculty and staff. Many recipients may consider the message to be annoying "junk mail" or "spam," especially if the broadcast messages are not relative to the conduct of official College business and continues to proliferate. Persons may decide a particular broadcast message that is not official business as harassment and request the sender remove them from their mailing list or address book. As a general guideline, the message should be of sufficient general value that it would justify being sent as a memorandum if E-mail were not available. In other words, is the message important enough to justify sending to virtually every EPCC employee? Campus-wide discussions should use Usenet news groups, not E-mail.
- All large group mailings should use appropriate mail groups. The Microsoft Exchange and Outlook software allow groups of 100 members. Public Groups can be built for a department, program or work group. Offices or individuals that make frequent or regular large group mailings that are not official notifications to all faculty and staff are encouraged to maintain their own groups. Messages to these groups should have an introduction indicating willingness to remove an individual from the group if requested by return E-mail.
- See EPCC Procedure 2.05.01.34, "Electronic Mail Services, Personal and Broadcast Email, and Email Restrictions" for District Announcements and Community Affairs broadcast message services.



## 6.9 General Responsibilities for All Users

- Know the basics of Information Security.
- Learn about possible security problems.
- Review and comply with the EPCC computing policies and guidelines.
- Review state and federal laws governing computing standards and crimes.
- Follow guidance in EPCC Procedure 2.05.01.38, "Acceptable Use of Information Technology Resources."
- Report security incidents immediately.
- Use EPCC information resources responsibly, respecting the needs of other computer users.
- Follow these tips:
  1. Do not share passwords.
  2. Do not open e-mail attachment from unknown people.
  3. Lock up diskettes when you leave your work area.
  4. Log off or disconnect from all network systems. Do not leave your computer unattended.
  5. Make periodic backup copies of work from your hard drive or floppy disks that are essential to your business function.
  6. Install anti-virus software, keeping its virus patterns current.
  7. Do not propagate virus hoax or chain mail.
  8. Information that is no longer needed should be destroyed.
  9. Beware of shareware; it may contain a virus.
  10. Keep patches current, especially the security related ones.

## 7. Acceptance of Security Policies & Procedures

The EPCC Information Security Handbook for Faculty, Staff, and Students is published in partial fulfillment of the requirements of Texas Administrative Code Title 1, Chapter 202, "Information Security Standards", Rule §202.77(a), "User Security Practices": All authorized users (including, but not limited to, institution of higher education personnel, temporary employees, and employees of independent contractors) of the institution of higher education's information resources, shall formally acknowledge that they will comply with the security policies and procedures of the institution of higher education or they shall not be granted access to information resources. The institution of higher education head or his or her designated representative will determine the method of acknowledgment and how often this acknowledgment must be re-executed by the user to maintain access to institution of higher education information resources.



EPCC's Information Security Program maintains this Information Security Handbook for Faculty, Staff, and Students on its website. It contains links to relevant policies and procedures and is updated as needed by the Information Security Program and Office of the Chief Information Officer personnel. All official EPCC policies and procedures should be available in paper form and circulated for review within each departmental area as well as at this link: <http://www.epcc.edu/it/security>.

Acceptance of EPCC's security policies and practices includes acknowledgement that certain information is confidential and intended for use only at EPCC. Students, faculty, and staff will agree to abide by the policies and procedures that govern the use of the College's automated information systems, and will accept the responsibility to protect information as described within the Family Education Rights and Privacy Act, the Texas Public Information Act, and security policies, procedures, and standards of EPCC.

Training opportunities will always be exploited as training is necessary to fully understand and fulfill these information security and proper use responsibilities. A notice and an acknowledgment procedure will be established at EPCC and work like this:

- (To be developed) All current employees will be asked to review EPCC Information Security Procedure and the EPCC Information Security Handbook for Students, Faculty, and Staff. At least once annually, all current employees will see a confidentiality and compliance statement when they begin to log on to their account. They will be asked to read and, by key or mouse-click acknowledgement, agree to comply with all described conditions.
- New employees, when they access their newly-created account for the first time, will have the opportunity to read about the confidentiality of information and acknowledge compliance with EPCC policy, procedure and Information Security standards.

## 8. Incidents and Emergency Response

Incident reporting and response is governed by the EPCC procedure (being developed). Security violations, suspected or confirmed, should be reported right away. EPCC faculty, staff, and students can report problems in several ways:

- Contact the [Information Security Manager](#) (send e-mail to [infosec@epcc.edu](mailto:infosec@epcc.edu) or call 831-6312).
- Call the Computing and IT Helpdesk, 831-6440, and ask the operator for assistance with a security problem.
- Contact your campus Microcomputer Support Technician.



- Notify your department head.
- Contact the EPCC Police Department, 831-2200, if criminal activity is suspected.

Information needed by the security contact:

- Your name, department, telephone number, email address, etc.
- The name of the person who discovered the incident/crime and their contact information.
- Description of what happened.
- Date and time of the incident.
- Location where the incident occurred (department, building/room number).
- Names of individuals involved in incident (if known).
- Name of witnesses (if known).
- Documentation or logs of the incident (if available).

## 9. Sanctions

Violations of Colleges policies and applicable state or federal laws are cited in applicable documents. A general overview of those sanctions is listed below. This list is not intended to usurp punishments for violations of policy or law.

Penalties for violations range from loss of computer resource usage privileges to dismissal from the College, prosecution, and/or civil action. Each case will be determined separately on its merits.

If the offender is a faculty member, his or her supervisor (usually the department chair) shall initially recommend to the dean and thereafter to the Vice President for Instruction the appropriate sanction. When termination is recommended, the faculty member may appeal to the College Review Committee or to the College Tenure Committee, whichever is appropriate in accordance with the El Paso Community College Faculty Handbook.

If the offender is a staff member, the procedures to be followed are those specified in the "Discipline and Discharge Policy" of the El Paso Community College Employee Handbook.

If the offender is a student, the procedures to be followed are those specified in the "Code of Student Conduct and Discipline" as printed in the El Paso Community College



Student Handbook. If the student in violation of this policy is also an employee of the College, sanctions may include termination of employment. Other State and Federal Laws may be applied.

## 10. EPCC Computing Policies, Guidelines, and Handbooks

### 10.1 Computing Policies

- [EPCC Policy 2.05.01.xx Information Technology General Policies](#) – At this link, select “Policies with Associated Procedures”; then go to Page 162 where the IT area begins.
- EPCC Procedure 2.05.01.58 [Information Security Procedure](#)
- EPCC Policy 3.9 [Web Publishing Policy](#)
- EPCC Procedure 2.05.01.54 Acceptable Use of Information Technology Resources

### 10.2 Computing Guidelines

- EPCC Procedure 2.05.01.34 Electronic Mail Guidelines – to be linked
- System Administrator Code of Ethics – to be published
- Desktop Applications Software Guidelines – to be published
- Web Publishing Guidelines – to be published

### 10.3 Handbooks and the EPCC Policy Manual

- [Staff Information](#)
- Employee Handbook (download from <http://www.epcc.edu/erd/> see "Resources/Publications")
- [College Policy Manual](#)
- [Student Code of Conduct](#)

## 11. State and Federal Laws

- Information Security Standards - [Texas Administrative Code Part Title 1, Chapter 10, Section 202](#)
- Computer Crimes - [Texas Penal Code, Chapter 33](#)
- Telecommunications Crimes – [Texas Penal Code, Chapter 33\(a\)](#)
- Tampering with a Governmental Record- [Texas Penal Code, Chapter 37](#)
- Computer Fraud and Abuse Act of 1986- [U.S. Penal Code, Title 18, Section 1030](#)
- Fraud and related activity in connection with computers- [U. S. Penal Code, Title 18, Chapter 47 - Fraud and False Statements, Section 1030](#)
- [Federal Copyright Law](#)
- [Digital Millennium Copyright Act](#)
- [Computer Software Rental Amendments Act of 1990](#)



- [Texas Open Records Act](#)

## 12. EPCC Computing Resources and Support

- [EPCC Information Technology](#) (Main Page)
- [EPCC Information Technology Helpdesk](#)
- [Information Security Program](#)
- [Virus Information Page](#)
- [EPCC Police Department](#)
- [Frequently Asked Questions](#)

## 13. Computer Security Terminology

Access- to approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of information resources.

Access Administrators - The individual or group that connects information users to information as authorized by the information owner.

Access Control- the enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

Accountability - An audit trail(s) at the user, application and/or system level that verifies use of any computerized system (network, Personal Computer [PC], or host computer) that will depict the time and date of an individual event.

Availability- ability to be present or ready for immediate use.

Breach or Incident- an event which results in unauthorized access, loss, disclosure, modification, or destruction of information resources whether accidental or deliberate.

Computer-an electronic, magnetic, optical, electromechanical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

Computer Security- those measures, procedures, or controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure.

Confidential Information- information that is excepted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal law.



Contingency- intended for use in circumstances not completely foreseen.

Control- a protective action, device, policy, procedure, technique, or other measure that reduces exposure.

Critical Application - An application that is so important that its loss or unavailability would have a significant impact on the continued operation of county program(s). This is usually an automated programming tool but may also be a manual process.

Critical Information- information that is defined by the agency to be essential to the agency's function(s).

Custodian of an Information Resource- a person responsible for implementing owner-defined controls and access to an information resource.

Data- a representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means. Data includes all files, regardless of size or storage media, including e-mail messages, system logs, and software (commercial or locally developed).

Data Security- those measures, procedures, or controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure.

Department Head - An employee of the College with budgetary authority over users of an information resource.

Disaster- a condition in which an information resource is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.

Disclosure- unauthorized access to confidential or sensitive information.

Hacker- a person who illegally gains access to and sometimes tampers with information in a computer system.

Harm- includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

Incident or Breach- an event which results in unauthorized access, loss, disclosure, modification, or destruction of information resources whether accidental or deliberate.

Information- that which is extracted from a compilation of data in response to a specific need.

Information Integrity - The accuracy and completeness of information systems and the data contained therein.



**Information Resource-** the procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

**Information Security -** The protection of information from unauthorized access modification, destruction or disclosure.

**Integrity-** the state that exists when computerized information is predictably related to its source and has been subjected to only those processes which have been authorized by the appropriate personnel.

**Owner of an Information Resource-** a person responsible for a business function and for implementing controls and access to information resources supporting that business function.

**Password-** a protected word or string of characters which serves as authentication of a person's identity (personal password), or which may be used to grant or deny access to private or shared data (access password).

**Physical Security -** The protection of information processing equipment, facilities and personnel from potentially harmful situations.

**Public Information -** Any information prepared, owned, used or retained by the county which is not specifically exempted from the disclosure requirements of the California Public Records Act or other local, state or federal laws.

**Risk-** the likelihood or probability that a loss of information resources or breach of security will occur.

**Risk Management -** The process of taking actions to avoid risks or reduce risk to acceptable levels approved by management.

**Security Controls-** hardware, programs, procedures, policies, and physical safeguards which are put in place to assure the integrity and protection of information and the means of protecting it.

**Sensitive Information-** information maintained by state agencies that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. It is information that requires higher than normal assurance of accuracy and completeness. The controlling factor for sensitive information is that of integrity.

**User of an Information Resource-** an individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.

**Virus-** an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by



---

attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

Worm- A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

---

[EPCC IT Home](#) | [Help Desk](#) | [Training](#) | [EPCC/IT Events](#) | [About Us](#) | [Our Mission](#)

Questions, comments and corrections for this site: [ITHelpDesk@epcc.edu](mailto:ITHelpDesk@epcc.edu)

[Go to the EPCC home page](#)