

Piedmont Virginia Community College

Information Technology Security Policy

2006

Table of Contents

INTRODUCTION	1
PVCC INFORMATION SECURITY OFFICER	2
INFORMATION TECHNOLOGY SECURITY SAFEGUARDS	3
PHYSICAL SECURITY	4
PERSONNEL SECURITY	5
DATA SECURITY	6
AUTHENTICATION, AUTHORIZATION AND ENCRYPTION	10
MONITORING AND CONTROLLING SYSTEM ACTIVITIES	12
THREAT DETECTION	19
INCIDENT HANDLING	20
SYSTEM INTEROPERABILITY	21
SECURITY TOOL KIT.....	22
TECHNICAL COMMUNICATION	24
TECHNICAL TRAINING.....	25
SECURITY AWARENESS TRAINING.....	ATTACHMENT A

I. INTRODUCTION

The objectives of the Piedmont Virginia Community College (PVCC) IT Security Plan are the following:

Acquaint employees with the security procedures required to ensure protection of information technology systems at PVCC.

Clarify employee responsibilities and duties with respect to the protection of information resources.

Enable managers and other workers to make decisions about information security which are in keeping with standard policies and procedures, and which are responsive to prevailing local conditions.

Coordinate the efforts of different groups within PVCC so that information resources are properly and consistently protected, regardless of their location, form, or supporting technologies.

Provide guidance for the performance of information system security audits and reviews.

Demonstrate upper management support for a strong information security program at PVCC.

Establish a basis for disciplinary actions when required to protect PVCC information assets.

PVCC is taking appropriate steps to ensure its information systems are properly protected from all security threats. All PVCC information systems shall be protected, regardless of storage or transmission medium.

Two key concepts form the backbone of the security program at PVCC:

1. All information access is granted on a “need to know” basis only.
2. Information security is the responsibility of the individual employee.

All security procedures in this document are written with these two concepts in mind.

II. PVCC INFORMATION SECURITY OFFICER

The PVCC IT Security Officer is currently Thomas Ruggeri.

The PVCC Information Security Officer has been assigned the following responsibilities:

Maintain and verify network and host security for all college systems.

Develop and maintain formal security policies and procedures.

Maintain and verify Windows group and user ID security databases.

Verify Windows NTFS and Share Level access rights.

Verify Local Area Network switch/router security.

Develop and maintain a formal security awareness and training program.

III. INFORMATION TECHNOLOGY SECURITY SAFEGUARDS

This security plan requires that good management practices be followed to implement information technology security safeguards based on the PVCC IT Risk Assessment. The following is a list of requirements for all information systems maintained at PVCC.

IV. PHYSICAL SECURITY

1. Purpose

Physical Security refers to those practices, technologies and/or services used to ensure that physical security safeguards are applied. Physical security safeguards take into account 1) the physical facility housing the information resources; 2) the general operating location; and 3) the support facilities that underpin the operation of the information systems.

2. Standard

In accordance with the document, COV ITRM Standard SEC2001-01.1 physical security must be an integral part of each agency's security preparedness program. Physical security reduces the risk that key information technology assets will be compromised by physical risks including natural or man-made threats including those that might be caused by nearby activities such as chemical or electromagnetically induced damage.

3. Procedures

PVCC views that safety of employees will always override the security of assets within the college; therefore, key maintenance employees will have access to the network closets as well as access to electrical components of the college.

1. Access to all resources will be controlled by rules of least privilege.
2. Security Cameras are placed throughout the college to provide additional security and monitoring capabilities of IT resources.
3. All network servers and network equipment shall be in a locked room or secured in a locked enclosure.
4. All network server rooms shall be equipped with a fire suppression system located within the room. Network technicians shall be aware of the nearest fire alarm. A smoke detector will be installed in the network server room.
5. The network server room will be monitored for temperature and humidity.
6. All network servers shall be run on an uninterruptible power supply (UPS).

7. A list of personnel that have approved access to the server room or LAN/Phone closet shall be maintained. *A logging system shall be set up to document any visitors to the server room or LAN/Phone closet not on the approved access list.* All visitors to the server room or LAN/Phone closet shall be escorted at all times.
8. No food or drink is allowed around computer equipment.
9. Sensitive information shall not be stored on portable computers that are taken outside of secured areas.
10. Do not leave confidential information on desks after working hours or in rooms that are unattended. All media should be clearly classified.
11. When dealing with confidential information, ensure that no one is watching over your shoulder. This precaution should also be taken when typing in passwords.
12. Attended operation is required when printing confidential information to an unsecured location.

V. PERSONNEL SECURITY

Existing state law and regulations impose significant responsibilities on employees for the security of information. If deemed necessary, PVCC will take personnel action based on the following state laws and regulations:

1. The Virginia Employee Standards of Conduct and Performance specifically include unauthorized use or misuse of state records, falsification of records, the willful or negligent damage or defacing of records and records theft as violations.
2. The **Government Data Collection and Dissemination Practices Act** (formerly the Virginia Privacy Protection Act of 1976) specifically requires that State agencies and institutions take affirmative action to establish rules of conduct and inform employees involved in the design, development, operation or maintenance of an information system, that misuse of personal information, or failure to take steps to ensure that information is accurate and reliable, may result in the individual employee being subjected to injunction and assessed the costs of court action.
3. The **Virginia Computer Crimes Act (Code of Virginia § 18.2)** imposes both misdemeanor and felony violations for the unauthorized viewing, copying, alteration or destruction of computer data, software or programs.

Therefore, PVCC has instituted the following personnel security measures:

Prospective new employees applying for positions, which have access to sensitive data, will be screened as to their trustworthiness in handling sensitive data.

All individuals with access to sensitive data must be familiar with PVCC policies and procedures relating to sensitive data.

Technical support personnel will be cross-trained so that procedures can be followed unaffected by the absence of any one key individual.

VI. DATA SECURITY

1. Purpose

Data Security refers to those practices, technologies and/or services used to ensure that security safeguards are applied appropriately to data which is provided, processed, exchanged and/or stored by the State.

2. Standard

In accordance with the document, COV ITRM Standard SEC2001-01.1 data security must be an integral part of each agency's security preparedness documentation and program. Data Security safeguards strive to sustain the level of integrity, availability and confidentiality of this data as stated by the agency's policy.

3. Procedures

Administrative data are essential to Piedmont Virginia Community College's business functions, which include, but are not limited to, financial, personnel, student, alumni, communication, and physical resources. The Data Security Policy defines the security and protection requirements for administrative data. The policy applies to data maintained in the campus file server, PeopleSoft SIS, FRS, and FAIS databases and at other departmental and office level systems, regardless of the media on which they reside. It does not include library holdings or research or instructional material unless they contain information that relates to a business function. The policy also describes the rights and responsibilities of Piedmont personnel in the handling, dissemination, security, and protection of administrative data.

College procedures regarding data security shall comply with all applicable federal and state laws and regulations that govern the privacy and confidentiality of data.

Piedmont Virginia Community College retains ownership of all administrative data created or modified by its employees as part of their job functions.

Classification of Administrative Data

For security purposes, administrative data is of three types, each requiring a different level of protection. Because of the sensitivity of the data maintained at the college, which should be assumed to be confidential or private unless otherwise specified, the college network systems are for authorized users only.

a. Confidential Data

Confidential data requires a high level of protection. Confidential data includes information whose loss, improper use, or disclosure could adversely affect the ability

of the College to accomplish its mission. It also includes records about individuals requiring protection under the Family Educational Rights and Privacy Act of 1974 (FERPA) and data not releasable under the Freedom of Information Act.

Access to confidential data is restricted and is available only to individuals who require that information to perform their College duties. It should not be discussed with others, except in the course of performing these functions. Confidential data includes, but is not limited to:

- Student data on social security numbers, grades, financial aid, parent's financial status, accounts receivable transactions, biography and academic history.
- Employee data on social security numbers, salaries and benefits, disabilities, evaluations, appointments, and biography.
- Alumni and Friends data on social security number, gifts, pledges, financial status, and biography.

b. Private Data

Private Data is data whose destruction or unauthorized disclosure would not necessarily result in any business, financial or legal loss, but which involves issues of personal privacy. Some private data may be available campus-wide, but will not be available to the public. Private data includes, but is not limited to:

- Student and Alumni data on college address and phone, email address, major field, date and place of birth, dates of attendance, degree, honors and awards received, employment, home address and phone.
- Employee data on email address, home address and phone number.

c. Public Data

Public data is available or distributed to the general public regularly or by special request. It can include names, departments, titles, degrees and majors of graduating seniors, and information in the College catalog.

Data Custodians and Data Owners

Each administrative office shall designate a Data Custodian who is responsible for the day-to-day oversight of administrative data in his or her functional area. The Data Custodian is also referred to in other documents as Application Owner. The Data Custodian usually is the office head. The responsibilities of the Data Custodian include the following:

- Ensuring that his or her office uses of administrative data are consistent with federal and state law, regulatory agency requirements, contractual obligations, and existing College policies.
- Ensuring the quality of data residing in the office's applications.

Although some of the Data Custodian's responsibilities may be delegated to others in his or her functional area, the Data Custodian will continue to have overall accountability for the use and security of the data.

An Owner of a specific set of administrative data is the Data Owner in the office that is designated by the Data Custodian as responsible for the upgrade and maintenance of that data. The Data Owner also may be designated by the Data Custodian as being responsible for the review and approval of all requests for access to and update capability for the data.

It is the responsibility of the Data Owner to ensure that all individuals who are given access to confidential data are instructed about its confidential nature.

Security Committee

The purpose of the College Security Officer is to oversee the on-going operation of the Piedmont Virginia Community College Information systems. Members of the Security Committee will be the Director of Technology, Database Administrator for the system, Security Officer for the system such as eVA, SIS, FRS etc, and the Network Administrator.

The Security Committee will be responsible for:

- Decisions on maintenance, upgrade, and access to specific administrative data, including the assignment of specific ID's, classes or roles of each system.
 - Example: In the SIS system, Classes determine the forms (screens) an individual can see, which in turn determine the information to which that individual has access. Roles determine whether a person only can view the information (read-only access) or also can change the information (read-write access).
- Changes in the Piedmont Virginia Community College Data Standards and Data Security policies.
- Coordination of testing on new procedures, modules, or ensuring that versions of system upgrades are made available.
- Coordination of system training.
- Implementing recommendations of the Systems Users Group.

Routine decisions on maintenance, upgrade, and access to administrative data may be delegated to the Data Custodians. In this case, the Security Committee will be available to resolve disputes, should they arise, among offices about access to data.

Granting Access

1. The employee's supervisor will initiate and sign the written or electronic request (Information Technology Account Request Form) indicating the appropriate level of access that should be granted to any given employee.
2. The employee will then sign and date the request and the VCCS Information Technology Ethics Agreement form at the same time. The fully signed and

dated request forms must be returned to the Human Resources Office for verification before being forwarded to the Information Technology Helpdesk.

3. The Security Officer and the Computer Security Liaison (CSL) will then grant the appropriate access requested. It will be the responsibility of the CSL to contest the Supervisor if the request level is deemed inappropriate.
4. The Computer Security Liaison (CSL) will be responsible for maintaining a folder of requests.

Maintaining of Access

The Data Custodian should review all system accesses and applications specified with the Security Officer each semester or required periods set forth in other system specific policies and send a status report to the CSL.

Termination of Access

1. On the last day of an employee's employment, the employee is required to submit an Account Termination Form sheet to each department and have supervisors sign off for each area of responsibility. The supervisor should check off the computer network access levels that are to be terminated. The form must be signed and returned to the HR office before being routed to the Information Technology Helpdesk. When this form is received by the Information Technology Helpdesk, technical personnel deactivate all computer and network access that is noted and sign off on the form. Information Technology personnel will confirm to the CSL in writing to ensure all other system access is terminated.
2. The completed form will be returned to the employee's supervisor for a final sign-off and returned to Human Resources.
3. Human Resources will place this form in each user's personnel file for audit review.
4. In some conditions, the account termination can be initiated by the HR Manager, the employee's supervisor or the CIO. Reasons for such action must be documented and retained in the employee's personnel file.

Requesting Authorization for Data Extraction

Extraction of data for processing on other systems should only be done for purposes that cannot be accomplished using the existing system. If data extraction is necessary, the confidentiality, integrity, and accuracy of the downloaded data must be ensured. Data extraction is to be done only by individuals who have been granted permission by the Data Custodian or Network Administrator. Requests for permission to extract data are handled in the same way as requests for authorization for granting access to data.

Purging Data from PC and Hard drives

Prior to surplus of all computers and electronic storage devices, including but not limited to hard drives, laptops, servers, or handheld computers, all data MUST be purged utilizing at least a three pass binary overwrite method. A completed "Notice of Computer Equipment Device Cleaning" form MUST be affixed to each unit for surplus. NO unit will be picked up for Surplus Property Collection without this form affixed to it and will not be accepted at the State Surplus Property warehouse. A form must be submitted to the Business Office Procurement Officer for all surplus items, so that a status change can be made in the FAIS system. If an item is to be disposed of, a disposal form must be completed and sent to the Procurement Officer and approval should be granted before the item is discarded.

Sensitive Data Backup and Recovery Policy

Introduction

This Backup policy is the bases of a mechanism to ensure that both data and software are regularly and securely backed up to essentially reduce the impact of systems failures.

I. Policy

Piedmont Virginia Community College requires that computer systems maintained by Information Technology Services be backed up periodically and that the backup media is stored in a secure off-site location. The purpose of the systems backup is to provide a means to: (1) restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster, and (2) provide a measure of protection against human error or the inadvertent deletion of important files. The systems backups will consist of regular full and incremental backups.

Systems backups will be performed on a regular schedule as determined by the Information Technology Network Services. Backups will be stored in a secure off-site location based on the schedule listed below.

II. Procedures

This policy provides guidelines for establishing backup procedures. Exceptions to the standard procedure are permitted when justified. All exceptions must be fully documented.

The standard procedure for systems backup is as follows:

- A. A full systems backup will be performed weekly. Weekly backups will be saved for a full month.
- B. The last weekly backup of the month will be saved as a monthly backup. The other weekly backup media will be recycled for other uses or destroyed.
- C. Monthly backups will be saved for one year, at which time the media will be recycled or destroyed.

- D. Incremental backups will be performed daily. Incremental backups will be retained for two weeks, at which time the media will be recycled or destroyed.
- E. All backups will be stored in a secure, off-site location. All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.
- F. Periodic tests of the backups will be performed to determine if files can be restored.

VII. AUTHENTICATION, AUTHORIZATION AND ENCRYPTION

1. Purpose

Authentication refers to the process of verifying the identity of a user. Authorization refers to the process of establishing and enforcing a user's rights and privileges to access specified resources. Encryption refers to the process of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by an authorized recipient holding the matching key.

2. Standard

In accordance with the document, COV ITRM Standard SEC2001-01.1 authentication, authorization and encryption measures must be an integral part of each agency's security preparedness documentation

3. Procedures

Password Policy:

Computer systems are only as secure as the passwords of the users who access it, particularly users with administrative level permissions. Employees are taught through our Security Awareness presentation the importance of using complex passwords using specialized characters, numbers and characters that are a combination of upper and lower case.

Enforce password history: 2 passwords remembered

This setting enforces how many different passwords must be used before the user can reuse one of them.

Maximum password age: 90 days

This setting controls how long a password is valid before a user is forced to select a new one. Users may change their password sooner, but this is the maximum period allowed.

Minimum password age: 0 days

This setting controls how long a new password must be used before it can be changed. Users are permitted to change their password as often as required.

Minimum password length: 7 characters

As the name implies, this setting controls how many characters must make up the password. 13 would be the complex length according to SANS.

Password must meet complexity requirements: Enabled

In order to meet complexity requirements a password must contain characters from at least three of the following four categories:

- Upper case letters
- Lower case letters
- Numbers
- Special characters (\$,#, or punctuation marks)
- Note: complex passwords may not be made up of the username or any part of the user's full name.

Store passwords using reversible encryption for all users in the domain: enabled

This setting is required to be enabled for using the Challenge Handshake Authentication Protocol (CHAP), among other things, and can also be set for individual users (IIS 5.0 Digest Authentication).

Account lockout policy:

The account lockout policy backs up the Password Policy. Even a good password can be guessed or discovered, given enough time, and/or computing resources.

Account lockout duration: 3 minutes

Once an account becomes locked out, when too many incorrectly entered passwords are attempted, this setting specifies the amount of time before the account automatically becomes available again.

Account lockout threshold: 4 failed attempts

This setting specifies the number of tries that a user may attempt to enter in an incorrect password before the account becomes locked out for a specified amount of time (see account lockout duration).

Reset account lockout counter after: 120 minutes

Each time an incorrect password is entered for an account, the account lockout counter increments by one. The Reset Account Lockout Counter decrements the threshold counter after a specified amount of time has passed.

VIII. MONITORING AND CONTROLLING SYSTEM ACTIVITIES

1. Purpose

Monitoring and Controlling System Activities refers to those practices, technologies and/or services used to ensure that the implementation and maintenance of security safeguards and system changes are adequately documented and managed, such that accountability can be established.

2. Standard

In accordance with the document, COV ITRM Standard SEC2001-01.1 Monitoring and Controlling System Activities must be an integral part of each agency's security preparedness documentation and program.

Inspect system activities for unexpected behavior.

System activities include those associated with system performance, processes, and users.

Programs executed on your networked systems typically include a variety of operating system and network services, user-initiated programs, and special-purpose applications such as database services. Every program executing on a system is represented by one or more processes. Each process executes with specific privileges that govern what system resources, programs, and data files it can access, and what it is permitted to do with them.

The execution behavior of a process is represented by the operations it performs while running, the manner in which those operations execute, and the system resources it uses while executing. Operations include computations, transactions with files, devices, and other processes, and communications with processes on other systems via your network.

User activities include login/logout, authentication and other identification transactions, the processes they execute, and the files they access.

If you permit third party (vendor, contractor, supplier, partner, customer, etc.) access to your systems and networks, you must monitor access to ensure all actions are authentic and authorized. This includes monitoring and inspecting of system activities.

Why this is important

You need to verify that your systems are behaving as expected and that the processes executing on your systems are attributed only to authorized activities of users, administrators, and system functions.

Unexpected or anomalous system performance may indicate that an intruder is using the system covertly for unauthorized purposes. They may be attempting to attack other systems within (or external to) your network or they may be running network sniffer programs.

A process that exhibits unexpected behavior may indicate that an intrusion has occurred. Intruders may have disrupted the execution of a program or service, causing it to fail or to operate in a way other than the user or administrator intended. For example, if intruders successfully disrupt the execution of access-control processes running on a firewall system, they may access your organization's internal network in ways that would normally be blocked by the firewall.

3. Procedures

Network Administrators are required to monitor college servers on a daily basis. This monitoring would include monitoring the servers' event logs, services, processes, system configuration data and performance counters, file activity, registry activity and printer activity.

1. Notify users that monitoring of process and user activities is being done.

Users are informed through the College Security Awareness Program of authorized use of your systems. Piedmont Virginia Community College's computers, networks and information systems exist to promote shared access to computing, communication and information systems necessary to support the College's mission of teaching, research and community service. Thus, all account holders of College information facilities have responsibility to use these systems in a respectful, ethical, professional and legal manner.

Piedmont's Responsible Computing Policy applies to any individual using PVCC-owned or leased computers, networks, Internet connections, and communications systems transmitting either data, voice or video information. Activities involving these systems shall be in accordance with the VCCS Computer Ethics Agreement, Policy on Use of the PVCC Web Server, PVCC Technology Security Plan, the College's Standards of Conduct for students, other related policies in the PVCC Faculty and Student Handbooks and relevant state, federal and international laws.

Review and investigate notifications from system-specific alert mechanisms (such as email, voice mail, or pager messages).

This includes notifications from:

- users and other administrators via email or in person
- operating system alert mechanisms
- system management software traps
- intrusion detection systems
- custom alert mechanisms from service or application programs (including tools)

Review and investigate system error reports.

Network administrators and Computer Network Technicians review various system logs to check for errors and investigate their cause.

Event logs are recorded daily on each server.

Syslogs are stored on the TACACS servers located at the VCCS and reviewed by VCCS personnel. Notifications are sent to the college if a problem is detected.

Our Asset management software allows us to check for CPU usage and report when a user is running out of disk space.

Review system performance statistics and investigate anything that appears anomalous.

Using performance monitors, the Network Administrator or Computer Network Technicians can monitor the total resource use overtime for CPU, memory, and disk space. Disk counters (input/output, queue lengths) over time and at specific times are also monitored.

Status reports for Print queues are reported back to the users.

When there are plans to change the system status for shutdown or re-starts the Network Administrator or Computer Network Technicians notify users ahead of time. If it is a planned outage for more than an hour, this is communicated at least 2 days in advance.

If the systems shutdown on their own then we would check for presence of a Trojan horse program that requires a shutdown or restart of a system or service.

Continuously monitor process activity (to the extent that you can).

The examination of processes is complex, time consuming, and resource intensive. The degree to which we are able to identify suspicious processes depends on our knowledge of what processes you normally expect to be executing on a given system and how they should behave.

Due to the large number of processes and their rapidly changing natures, it is impractical to monitor them continually. We can identify any unexpected, unusual, or suspicious process behavior and the possible implications by looking for:

- missing processes
- extra processes
- unusual process behavior or resource utilization
- processes that have unusual user identification associated with them
-

Data from log files and other data collection mechanisms help to analyze the process behavior. These include:

- User executing the process.
- Process start-up time, arguments, file names.
- Process exit status, time duration, resources consumed.
- Amount of resources used (CPU, memory, disk, time) by specific processes over time; top "x" resource-consuming processes.
- System and user processes and services executing at any given time.
- Processes running at unexpected times.
- Processes terminating prematurely.
- Processes consuming excessive resources (wall clock time, CPU time, memory, disk) may warn you of an impending denial-of-service condition or the use of a network sniffer.
- Unusual processes, such as password cracking, network packet sniffing or any other processes not due to normal, authorized activities.
- Processes with unusually formatted output or arguments (for example, on UNIX systems, a process running as ". /telnetd" instead of "/usr/sbin/telnetd").

- New, unexpected, or previously disabled processes or services. These can indicate that an intruder has installed their own version of a process or service or, for example, are running IRC services, web services, FTP services, and so forth to allow them to distribute tools and files they have stolen (such as password files) to other compromised hosts.
- Inactive user accounts that are spawning processes and using CPU resources.
- a terminal exhibiting abnormal input/output behavior.
- Processes without a controlling terminal that is executing unusual programs.
- An unusually large number of processes.

Identify any unexpected, unusual, or suspicious user behaviors and the possible implications.

Data from log files and other data collection mechanisms will help you to analyze user behavior. These include:

- Login/logout information (location, time): successful, failed attempts, attempted logins to privileged accounts.
- Login/logout information on remote access servers that appears in logs.
- Changes in user identity.
- Changes in authentication status, such as enabling privileges.
- Failed attempts to access restricted information (such as password files).
- Keystroke monitoring logs.
- Violations of user quotas.

Look for:

- Repeated failed login attempts including those to privileged accounts.
- Logins from unusual locations or at unusual times including unusual or unauthorized attempts to login via a remote access server.
- Unusual attempts to change user identity.
- Unusual processes run by users.
- Unusual file accesses, including unauthorized attempts to access restricted files.
- Users logged in for an abnormal length of time (both short and long).
- A user executing an unexpected command.
- A user working from an unusual terminal.

If you notice unusual activity associated with particular users, initiate supplemental data collection mechanisms to gather detailed information about their activities. Many multi-user systems provide mechanisms to audit all processes associated with a particular user. Since process accounting logs tend to generate a great deal of information rapidly, you will need to allocate sufficient resources to store the data collected. Similarly, detailed network logging of all activity associated with all the systems accessed by a specific user can be voluminous, and you will need to allocate resources accordingly. Review the newly collected data often (at least daily) and rotate files regularly to minimize the amount of information that you must analyze at any given time.

Identify other unexpected, unusual, or suspicious behaviors and the possible implications.

If your network interface card is in promiscuous mode, an intruder may be using this mode to run network sniffers for capturing passwords and other sensitive information. However, keep in mind that legitimate network monitors and protocol analyzers will set a network interface in promiscuous mode as well.

Logging information produced by vulnerability patches (updated software that corrects or closes vulnerability), if provided by the vendor and if turned on, can aid in identifying a pattern where an intruder exploits more than one vulnerability before gaining access. For example, a failed logged attempt to probe for an old vulnerability (produced by the vulnerability patch) could be followed by a successful probe for a new vulnerability that is not logged. The presence of the vulnerability patch logging information along with other mechanisms such as integrity checking could alert you to this type of intruder action.

Periodically execute network mapping and scanning tools to understand what intruders who use such tools can learn about your networks and systems.

We recommend running mapping and scanning tools during non-business hours and when you are physically present because mapping tools can sometimes affect systems in unexpected ways.

Eliminate or make invisible (if possible) any aspect of your network topology and system characteristics that you do not want to be known by intruders who use mapping tools.

Periodically execute vulnerability-scanning tools on all systems to check for the presence of known vulnerabilities.

We recommend running such tools during non-business hours and when you are physically present because scanning tools can sometimes affect systems in unexpected ways.

Eliminate all vulnerabilities identified by these tools wherever possible. Many of these can be dealt with by updating configuration file settings and installing vendor-provided patches.

Consider using scanning tools that include password analysis as part of the vulnerability assessment. Such analysis may include the identification of weak, non-existent, or otherwise flawed passwords such as those that can be determined as using brute force or dictionary-based attacks.

IX. THREAT DETECTION

1. Purpose

Threat detection refers to those practices, technologies and/or services used to:

- 1) detect that a suspicious activity may be occurring on systems/networks.
- 2) alert security administrators and security staff accordingly.

2. Standard

In accordance with the document, COV ITRM Standard SEC2001-01.1 threat detection must be an integral part of each agency's security preparedness program. Threat detection enables and agency to respond in a timely fashion to new or sudden risks against the agency's systems, and to improve the security of those systems over time.

3. Procedures

The College has deployed a Cisco Pix firewall on campus. The firewall has been set up to separate data traffic of students from faculty and staff. This separation is done through the set-up of students on separate switches from faculty and staff and having separate VLANs on each switch ports. De- Militarized Zones (DMZ) are also set up for control of students versus faculty and staff. Cisco Firewall logging will be turned on and monitored.

A VPN Concentrator is used to authenticate all remote access users.

An Access Control System (ACS) is used for issuing access controls for the LAN and the VPN system.

Once a threat has been detected the following steps that were recommended by SANS (SysAdmin, Audit, Network, and Security) Institute will be taken:

1. Identify where and what the threat may be:
 - a. The College uses a number of methods to identify and evaluate suspicious activity that may be occurring on the College's computing resources. These include, but are not limited to, Intrusion Detection Systems (IDS), network monitors, LAN packet sniffers, reports from employees through incident reports and reports from other agencies.
 - b. Suspicious activity detected by the IDS and LAN packet sniffer and suspicious activity reported by employees that warrant investigation will be logged.

2. Preparation will be made on how to isolate the threat.
3. Establish containment of the threat and isolate systems entirely from the network until the threat has been eradicated.
4. Eradicate the threat.
5. Recover any lost or damaged files.
6. Document lessons learned.

X. INCIDENT HANDLING

1. Purpose

Incident Handling refers to those practices, technologies and/or services used to respond to suspected or known breaches of security safeguards.

2. Standard

In accordance with the document, COV ITRM Standard SEC2001-01.1 incident handling must be an integral part of each agency's security preparedness program. Incident handling reduces the risk that key information technology assets will be compromised by an intrusion or other breach of security.

3. Procedures

All computer related and non-computer related incidents are reported to the College by submitting an Incident Report to the Business Office. These report forms may be obtained from the Business Office. If it is a facilities security incident, the Incident Form is submitted to the Facilities Manager. If this is a System security incident it is submitted to the Information Systems Security Office.

Once a system threat has been detected, the following steps that were recommended by SANS (SysAdmin, Audit, Network, and Security) Institute will be taken:

1. Identify where and what the threat may be:
 - a. The College uses a number of methods to identify and evaluate suspicious activity that may be occurring on the College's computing resources. These include, but are not limited to, Intrusion Detection Systems (IDS), network monitors, LAN packet sniffers, reports from employees through incident reports and reports from other agencies.

Suspicious activity detected by the IDS and LAN packet sniffer and suspicious activity reported by employees that warrant investigation will be logged.
 - b. If this incident is related to pornography, the content will be checked to see if perhaps it does relate to a classroom project such as Biology or Nursing. If not, it will be documented and reported to outside

authorities, if necessary. All child-related pornography will be reported to Federal authorities.

2. Preparations will be made to isolate the threat.
3. Establish containment of the threat and isolate systems entirely from the network until the threat has been eradicated.
4. Eradicate the threat.
5. Recover any lost or damaged files.
6. Document lessons learned.

XI. SYSTEM INTEROPERABILITY

1. Purpose

Systems interoperability refers to those practices, technologies and/or services used to ensure that security safeguards are applied consistently and appropriately to mechanisms that allow diverse systems and networks to interoperate.

2. Standard

In accordance with the document, COV ITRM Standard SEC2001-01.1 systems interoperability security measures must be an integral part of each agency's security preparedness documentation. The interdependence of control procedures in regard to system interoperability security is a concern when the issues of authentication, authorization and data security are fundamental in safeguarding network resources.

The Office of Information Technology at Piedmont Virginia Community College provides shared information technology resources and services to all PVCC staff, faculty, and students as well as select visitors for activities supporting the College's mission. The purpose of this standard is to protect the integrity of PVCC's technology resources and the users thereof against unauthorized or improper use of those resources. All individuals (PVCC employees and otherwise) granted access to PVCC's IT facilities and resources will be required to follow the guidance documented in this standard.

The required components are addressed below:

- Each agency must ensure that authentication, authorization and data security, as established by the data owner, are not compromised during data sharing and systems interoperability.
- Auditable user agreements must be established between the agencies sharing data, which clearly state the degree of authentication and levels of protection required.
- Web-enabled transactions that require user authentication, or transfer of sensitive data, or involve the transfer of funds, must use encryption (e.g. SSLv3).

3. Procedures

Currently PVCC does not have any interoperable automated systems with other agencies or outside entities. In the future, if PVCC does have an interoperable automated system with other agencies or outside entities, PVCC will ensure that appropriate security is established with the other agencies or outside entities. Auditable user agreements will be established between the agencies or outside entities.

All web-enable systems that involve sensitive data currently utilize encryption based on SSLv3. Any future web-enable system that involves the transfer of money will also use encryption based on SSLv3 or better.

XII. SECURITY TOOL KIT

1. Purpose

Best practices requires that each agency or ITS personnel have available a diverse array of analytical tools for the proper maintenance and troubleshooting functions that may occur during the course of performing periodic network security safeguards. For example, firewall technology can provide a mechanism through which authentication, authorization, filtering and routing of remote users to an internal system can be accommodated. Typically an agency's security tool kit will be comprised of a combination of commercial off-the shelf products, industry proven free shareware, and agency developed software tools. Examples of common technologies within an organization's security tool kit include firewall technology vulnerability scanners or Intrusion Detection System (IDS) and network sniffers.

2. Standard

In accordance with the document, COV ITRM Standard SEC2001-01.1 a security tool kit which could entail firewall technology, vulnerability scanners or Intrusion Detection Systems (IDS), and network sniffers must be maintained as an integral part of each Agency's security preparedness documentation. Each agency must utilize firewall technology. Each agency must test its firewall technology on a periodic basis to ensure compliance with security policies. Each agency must deploy multi-layered protection at the Internet gateway, at network servers, as well as at the individual workstations.

3. Procedures

Firewall, DMZ, NAT, TACACS+

Piedmont Virginia Community College is externally connected to Network Virginia (NET.WORK.VA) using a DS3 ATM connection. This single point of entry into the PVCC Network is protected by a Cisco PIX 515 firewall, authentication, authorization, filtering and routing of remote users to the internal systems of the PVCC network. The PVCC web server is hosted off-campus, thus outside the college's network.

Additional firewall security is provided by an integration of a Network Addressing Translation (NAT) feature within the firewall where public IP addresses are translated to private IP addresses which are deployed to every

network device within the internal PVCC network which are not accessible to the outside world.

Remote access to the PVCC network for support purposes only is accomplished by the Windows XP or Windows 2000 Remote Desktop application and is authenticated by the Access Control Server.

Network map and Monitoring– Cisco Works

PVCC will acquire a network administration server that contains a network map and monitoring application called Cisco Works. This application will provide a real-time accurate representation of every device on the PVCC network. It will look at the router tables and automatically discovers and maps all network devices according to the PVCC network hierarchy with separate maps for each subnet. This application will provide the PVCC network administrators with a high level of flexibility and control as well as accurate network monitoring of the status of network devices, services and resources. It provides real-time monitoring of network availability with notification of any specific failure.

Workstation Protection and Management – Faronics DeepFreeze Enterprise

PVCC purchased the Faronics DeepFreeze Enterprise application that has been deployed on all student accessible desktop computers. DeepFreeze Enterprise provides PVCC Information Technology staff with centralized deployment and flexible management control of student accessible classroom and lab desktop computers campus-wide. The computers can be thawed out so that application and configuration updates can be applied. Then the PCs can be frozen to prevent unauthorized changes. The same computers are thawed at specified times so that the Microsoft Updates and new Symantec virus definitions are applied.

Network Performance and Security – CiscoWorks VPN/Security Management (VMS)

PVCC will acquire a Cisco VMS module to enhance security. CiscoWorks VPN/Security Management Solution (VMS) is an integral element of the SAFE Blueprint for Enterprise Network Security from Cisco, and contributes to organizational productivity by combining Web-based tools for configuring, monitoring, and troubleshooting VPNs, firewalls, network intrusion detection systems (IDS), and host intrusion prevention systems. Integrated with other CiscoWorks products, CiscoWorks VMS also includes network device inventory, change audit, and software distribution features.

PVCC has deployed a Fluke Protocol Inspector – a tool that monitors the throughput rates, IP maps for the college network.

XIII. TECHNICAL COMMUNICATION

1. Purpose

Technical communications refer to those practices, technologies and/or services used to communicate technical information and notifications regarding the status of security related events and safeguards.

2. Standard

In accordance with the document, COV ITRM Standard SEC2001-01.1 technical communications must be an integral part of each agency's security preparedness program. In addition to the communications inherent in Security Awareness and Technical Training, the security architecture requires a means to support the timely and meaningful exchange of information regarding: 1) new security technology products and/or features, best practices, emerging industry standards, and security safeguards success stories; 2) proposed changes to the security infrastructure and associated implementation plans; and 3) alerts, status, and recommended actions in response to security attacks. Examples of technical communication medium include internal enterprise list servers, government sponsored security conferences, subscriptions to security research consortiums, etc.

Technical communications are instrumental in the security architecture as they foster both a proactive stance and a systemic view in addressing security issues within a dynamic business and technology environment.

3. Procedures

- The college maintains Network Diagrams with IP addresses, Network Switch configurations, IP address listings and License Key Codes for college programs. All of these items are stored on a private network share to which only the Technical Support Department has access.
- All administrator and other accounts and passwords are stored in a safe location.

XIV. TECHNICAL TRAINING

1. Purpose

Technical Training refers to those practices, technologies and/or services used in training security officers, system administrators and/or other personnel involved in the administration or development of information systems.

2. Standard

In accordance with the document, COV ITRM Standard SEC2001-01.1 technical training must be an integral part of each agency's security preparedness documentation. Technical training is an essential attribute for any security officer, system administrator and/or other personnel involved in the administration or development of information systems.

3. Procedures

The Technical Services Department employs staff members responsible for information technology security safeguards. These individuals have received minimal training in the past but will now receive in-depth training to design and implement techniques to provide security safeguards to ensure protection of College information and technology resources. PVCC will plan for training in the Technology Plan each year.

Starting Fiscal Year 2006, all Technical Services Staff Members will attend technical training courses as time allows. Training records are maintained in the Human Resources Department once training is complete. Most of the proposed department technical training is outlined as part of the employee's Performance Evaluation and discussed with his/her supervisor when applicable and/or on a semi-annual basis. These training classes usually focus on a variety of topics such as managing, administering, designing, developing, implementing, and/or maintaining information resources.

- IT will receive at least one Security Awareness training geared to their level of expertise required for the system components and information resources for which they are responsible.
- The training will include content that enables the individual to identify and evaluate threats, vulnerabilities, and risks specific to those components and resources. The training will include content regarding technical alternatives, methods, and standards which represent best practices appropriate to those components and resources, and which can be utilized to effectively implement safeguards as appropriate.
- Each IT staff member will receive adequate training for their technical responsibilities, such as the Security Officer, LAN administrators, system administrators, or security administrators.
- Training will be given by outside contractors that have the professional level of training that Technical Service staff need. Once training is completed, a form is filled out and sent to Human Resources, to be entered into their training database.
- Technical Services will continue to obtain and maintain appropriate technical reference manuals and documentation to support hardware and software products used in the agency.

- IT will continue to subscribe to technical publications, Dlists and other sources to help technical personnel maintain their knowledge of current technology practices and emerging technologies.
- IT staff will attend, at least every other year; an external security related sponsored workshop and seminar such as SANS Conference, CSI Conference or Microsoft Security. The level of involvement in these classes will be documented on the training records.
- Security procedures that are not already in place will be written during Fiscal Year 2006. These procedures will be based on the College Risk Assessment.