

ACADEMIC COMPUTING CENTER

Telephone: 610-436-3065  
Email: [webmaster@wcupa.edu](mailto:webmaster@wcupa.edu)

ACADEMIC COMPUTING  
DIVISION OF INFORMATION SERVICES

## Information Services Policies

### Information Assurance Policy

*Draft 1.3*

- 1 Purpose.
  - 1.1 Introduction.
    - 1.1.1 General Information.
    - 1.1.2 Objectives.
    - 1.1.3 Sanctions.
  - 1.2 Responsible Organizational Structure.
    - 1.2.1 Vice-President of Information Services.
    - 1.2.2 Overview.
    - 1.2.3 Information Security Manager
    - 1.2.4 Networking, Operations & Telecommunications.
    - 1.2.5 Administrative Computing.
    - 1.2.6 Information Technology & Academic Computing.
  - 1.3 Related Policies.
    - 1.3.1 Information Protection.
    - 1.3.2 Use of Computing Resources.
    - 1.3.3 Privacy.
    - 1.3.4 Use of Computer Software.
- 2 System Administrator Responsibilities.
  - 2.1 General.
    - 2.1.1 Scope and Documentation.
    - 2.1.2 Physical Security.
  - 2.2 Logical Security.
    - 2.2.1 Authentication.
    - 2.2.2 Secured Hosts.
    - 2.2.3 Virus Scanning.
    - 2.2.4 Active Monitoring.
  - 2.3 Backup and Recovery.
    - 2.3.1 Workstation Backup Procedures.

3 Security Services and Procedures.  
3.1 Risk Assessment and Monitoring..  
3.1.1 PeopleSoft Systems.  
3.1.2 Mainframe Systems.  
3.1.3 Model 204.  
3.2 Incident Response.

4 On-going Activities.  
4.1 Implementation.  
4.2 Reports.  
4.3 Reviews.

Appendix A – Definitions.

---

# 1 Purpose

## 1.1 Introduction

### 1.1.1 General Information

Information resources are vital assets that require protection. This policy is intended to protect and defend the integrity of West Chester University of Pennsylvania's information and information systems. This document defines the security and data ownership responsibilities, along with relevant and necessary authorities to undertake these assigned responsibilities, of the information system resources that are maintained and operated by WCU Information Services.

The university has a legal responsibility to secure its computers and networks from misuse. While the value of equipment such as computer hardware is easily appreciated, we must not overlook the larger investment in less tangible information assets - such as data, software, and automated processes. Computers and network resources can provide access to these less tangible resources both on and off campus.

Failure to exercise due diligence may lead to financial liability for damage done by persons accessing the network from or through West Chester University of Pennsylvania. At the extreme, an unprotected WCU network open to abuse might be denied access to parts of the larger network community.

### 1.1.2 Objectives

The university reserves the right to limit, restrict, or extend computing privileges and access to its resources. Access to the university's information system facilities and resources is granted solely to West Chester University of Pennsylvania faculty, staff,

registered students, and authorized individuals outside the university. This user community is expected to cooperate with Information Services in its operation of the information systems and networks as well as in the investigation of misuse or abuse of those assets.

Open access to IS-provided resources is a privilege implicit in WCU's grant of access to users. Such open access requires that individual users act in a responsible and acceptable manner. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. Acceptable use demonstrates respect for intellectual property, truth in communication, ownership of data, system security mechanisms, and individuals' right to privacy and freedom from intimidation, harassment, and unwarranted annoyance. The university considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to test and monitor security, and copy and examine any files or information resident on university systems.

Data, whether stored in central computers accessible through remote terminals, processed locally on microcomputers, delivered via email, or generated by word processing systems, are vulnerable to a variety of threats and must be afforded adequate safeguards. A combination of protection, detection, and reaction capabilities will be employed to protect the information system and data. Maximization of the five information assurance security objectives of:

1. availability
2. integrity
3. authentication
4. confidentiality
5. non-repudiation

will serve as the goal for information systems security for the University.

WCU faculty, staff, and students need to be aware of the value of these resources and the means of protecting them. User awareness through education is the first line of defense in maintaining confidentiality, reliability, availability, and integrity of WCU information resources. The West Chester University of Pennsylvania's Information Assurance Policy's success is dependent on education of faculty, staff, and students in the need for and means of protecting WCU information resources. This education will include exposure to our authentication and password policies, and other physical loss prevention policies, the distribution and regular updating of virus protection software to all users, the use of encryption tools for critical data, and, if necessary, the implementation of back up and recovery procedures for all systems and other policies and procedures deemed necessary.

### **1.1.3 Sanctions**

Those WCU authorized users who do not abide by the policies and guidelines outlined in this policy should expect disciplinary action in accordance with university rules for misconduct and existing judicial, disciplinary, or personnel processes. Offenders will also be subject to criminal prosecution under federal or state laws, and should expect the university to pursue such action. Information Services should be notified about violations of computer laws and policies, as well as about potential loopholes in the security of its information systems and network.

## **1.2 Responsible Organizational Structure**

### **1.2.1 Vice-President of Information Services**

The Vice-President of Information Services is responsible for the administration of this policy, including the definition of documentation standards are noted section 2.1.1 Scope and Documentation. The WCU Vice-President of Information Services is the Chief Information Technology Officer. The VP of IS will delegate operational responsibility and accountability to the senior managers within each WCU technology Operational Group as detailed in 1.2.2 Overview (Exec. Director Information Technology & Academic Computing, Director Networking, Telecommunications & Operations, Director of Administrative Computing, Director of Institutional Research.).

### **1.2.2 Overview**

WCU advisory and operational technology units are defined as follows:

#### **Advisory Groups:**

*Instructional Technology Task Force (ITTF)* – Consists of faculty representatives from each college as well as representatives from university administrative and support units. Serves the role of reviewing policy and providing advice regarding technology support related to the academic mission.

*Point Project Steering Committee (IS3)* – The Steering Committee will provide project vision, advocacy, and leadership. It will make policy and budgetary decisions. It will be composed of West Chester University Vice Presidents, Associate Vice President for Information Services, Director of Institutional Research, and Software Project Manager.

*Web Advisory Committee (WAC)*

*Campus Community Task Force (CCTF)*

*Web Technical Committee (WTC)*

*Information Services Technical Group (ISTech)* – Membership consists of representatives of all the operational groups. This group is lead by the VP of Information Services. Used as a sounding board for technical issues occurring throughout the Information Services Division.

*Network Security Incident Response Team (NSIRT)* – Will provide a centralized service charged with investigating violations and reporting violations to law enforcement authorities as needed. The members of NSIRT consists of Information Services staff from various areas within the IS division, including Systems, Network Operations, Client Services, and Academic Computing. Other areas on campus that could become involved on an incident basis may include Student Judicial Affairs, Campus Police, Social Equity, Academic Affairs and/or Human Resources. Finally, off-campus resources such as the FBI, State Police, and CERT/CC may be contacted for additional assistance. The Coordinator reports to the Director of NetTel and Vice-President of Information Services.

### **Operational Groups:**

*Administrative Computing (ADC)* – responsible for support of administrative business systems (PeopleSoft, M204) including applications development. The ADC Director reports to the Vice President of Information Services.

*Academic Computing Services (ACS)* – The mission of Information Technologies & Academic Computing Services’ is to serve the computing and information technology needs of the campus community, and in doing so is responsible for the support of computers on campus. These resources exist to support, promote, and contribute to the effective use of computing and information technology in education and its supporting enterprise. The ACS Exec. Director reports to the Vice President of Information Services.

*Networking, Operations & Telecommunications (NetTel)* – Responsible for data and voice communications infrastructure and network/server operations. The Director of NetTel reports to the Vice President of Information Services.

### **1.2.3 Information Security Manager**

The Information Security Manager coordinates any of the activities involving the five information assurance security objectives stated in 1.1.2 Objectives. The ISM will also work with any of the Advisory and Operational groups to ensure this policy is followed.

The ISM is the Chief Information Security Officer and also the NSIRT Coordinator. The ISM reports to the Director of Networking, Operations & Telecommunications and Vice President of Information Services.

### **1.2.4 Networking, Operations & Telecommunications**

Services: E-mail, network services & infrastructure (IP addresses, Internet connectivity), software administration, central user name space management.

- Advisory body: ISTech

Housing/student services (RESNET): providing access to campus network services for student residents, residence hall computer labs.

## **1.2.5 Administrative Computing**

Services: Implementation and support for administrative business systems (PeopleSoft, M204, System25)

- Advisory unit: IS3, ISTech

## **1.2.6 Information Technology & Academic Computing**

Services: end-user support, local network administration & network services, application specific services (e.g. disciplinary-specific software/hardware), computer labs, technology classrooms, university web presence, and digital media services.

- Advisory units: ACS, ITTF, ISTech

Housing/student services (RESNET): providing support to for residence hall computer labs and student computing needs.

# **1.3 Related Policies**

## **1.3.1 Information Protection**

All WCU Users and Systems Administrators are subject to the Access, Use, and Maintenance responsibilities defined with the WCU Acceptable Use Policy.

<http://www.wcupa.edu/infoservices/Policies/NetworkPolicies.html>

## **1.3.2 Use of Computing Resources**

All WCU Users are subject to the responsible use of computing resources and all System Administrators are obligated to suspend activities which pose a clear and present threat to efficient operation of and equitable access to university computing resources as defined in the WCU Acceptable Use Policy.

## **1.3.3 Privacy**

University computer systems, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized

university use. The University supports each individual's right to reasonable privacy when using WCU computing resources for authorized university business, and will take reasonable steps to ensure security of these resources. WCU computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Use of this WCU computer system, authorized or unauthorized, constitutes consent to monitoring of system activities for information assurance.

Data contained on University computer systems is accessible to System Administrators. Access to private information is granted only on a “need to know”, “need to create”, or “need to fix” basis. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on, or sent over this system may be monitored. Unauthorized use may be subject to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. System Administrators are also responsible for responding to authorized requests for system information from compulsory legal entities.

### **1.3.4 Use of Computer Software**

All WCU Users and System Administrators are responsible for the legal and ethical use of computer hardware and software, including the use, copying, or distribution of contractually protected or copyrighted educational, commercial, or administrative software as defined in the WCU Computer Software Policy.

## **2 System Administrator Responsibilities**

### **2.1 General**

#### **2.1.1 Scope and Documentation**

Every system connected to the WCU network must have a designated System Administrator. A System Administrator is responsible for the implementation and maintenance of all University security policies and any local College/Unit policies for every system for which the System Administrator is directly responsible. The System Administrator will develop and maintain documentation of security compliance and make the documentation available to the Information Security Manager. Said documentation, which will follow a format defined by the Information Security Manager, will address all items detailed in sections 2.2 Logical Security and 2.3 Backup and Recovery.

#### **2.1.2 Physical Security**

Servers, networking equipment, and related hardware is to be housed in a physically secure area with access restricted to designated System Administrators.

## **2.2 Logical Security**

### **2.2.1 Authentication**

System Administrators are responsible for limiting access to computing resources to authorized users from the University or its affiliates. Access will be granted based on the minimum access required. Public access will be restricted to pre-defined cases documented by the System Administrator. System Administrators must document and follow account management procedures that detail the creation, maintenance, and removal of accounts on each system and associated account password standards.

In addition, System Administrators will limit access to root, administrator, or privileged accounts/rights to employees that absolutely require such access.

### **2.2.2 Secured Hosts**

All systems connected to the university network will be administered with a “secured host” model where all unnecessary services are removed and all vendor security patches are applied to each system before it is placed into production. Moreover, once the system is in production the System Administrator is responsible for monitoring and installing security patches released by vendors whose products are utilized on each system and maintaining documentation of same.

### **2.2.3 Virus Scanning**

System Administrators will install and actively maintain virus scanning software on their systems and the systems of their Users.

### **2.2.4 Active Monitoring**

System Administrators will actively monitor all logs for the systems that they administer, including the deployment of any appropriate Intrusion Detection Systems. System Administrators may conduct security scans for any systems that they directly administer. Security scans of other systems on the University network are strictly prohibited unless prior written permission is obtained from the Information Security Manager except for the central Risk Assessment & Monitoring functions performed by Information Services as detailed in item (3).

## **2.3 Backup and Recovery**

Each system must have an appropriate backup and recovery model defined by the System Administrator, including a Disaster Recovery plan. Records will be maintained of all backups created. Critical backups will be maintained off site in a secure facility.

### **2.3.1 Workstation Backup Procedures**

West Chester University offers a data backup service for mission critical workstations as part of the University's plan for business continuity. Each selected client is given a quota of approximately 2.5 GB. Data is backed up remotely using automated scheduling on each client workstation. The data is then archived to AIT Tape media and stored off-site.

Backups of general software applications for recovery are stored off-site at a different building on campus.

## **3 Security Services and Procedures**

### **3.1 Risk Assessment and Monitoring**

The Department of Networking, Operations, & Telecommunications will operate and maintain a risk assessment system on the WCU production network to monitor network traffic and scan WCU hosts for security problems. Risks will be escalated to the System Administrator of a given system. Based on the threat level of a given incident, network access may be suspended under the WCU Acceptable Use Policy.

#### **3.1.1 PeopleSoft Systems**

The University has a support contract with Compaq for all PS production servers. There are also support contracts with Oracle, PeopleSoft, and Veritas.

Compaq Insight Manager and Survey utilities are fully implemented and provide inventories of both hardware and software for all PS servers. A hardcopy report of the server configuration is printed every ninety days. The Insight Manager software installed is at different release levels causing some servers not to be monitored.

Key documentation is kept online, is backed to tape, and is kept off-site. There is no hardcopy of the key documentation. There should be a hardcopy document of general guidelines to recovery in case of a disaster.

The backup and restore process for PeopleSoft/Oracle databases has been fully tested and documented. Databases are routinely migrated through the development cycle from Development to Test and Training, and Production copies.

#### **3.1.2 Mainframe Systems**

Procedures are in place for restoring the mainframe. The VM operating system is primarily backed up using VMBACKUP. The following lists all the backups for VM and other mainframe software products:

- One full and four incremental backups completed every week
- Standalone backup of Sysres volume completed weekly
- VMBACKUP (backup software) is backed up daily
- The tape catalog is backed up weekly
- Spool space is backed up daily T-S
- CP Module, CMS nucleus, and save segments are backed up (standalone) every sixty days or when a change occurs. Two sets are created for on and off site.
- Standalone utility tapes - ICKDSF, DDR, VMBRITS and VMBSAR are stored on and off site
- The source directory is backed up M-F
- A hardcopy layout of the disk system is printed weekly
- A list of backup tapes and critical tapes is printed daily
- A hardcopy of the restore procedures are store in the computer room safe

### **3.1.3 Model 204**

- Journal is backed up every time the database comes down, usually twice a day
- A hot backup of the data files is done daily

## **3.2 Incident Response**

The Directors of Information Services (will) maintain a Technical Emergency Response Plan. Security incidents will be classified with the categories defined with the plan and the associated procedures will be followed to address the incident with appropriate communications, documentation, and actions. System Administrators must follow the provisions of the emergency response plan. Incident Response will work with the Information Security Manager and NSIRT.

## **4 On-going Activities**

### **4.1 Implementation**

To be effective, the WCU Information Assurance Policy must be enforced for all systems connected to the university network. This enforcement must be an on-going effort applied to both new and existing systems. Information Assurance is a dynamic and demanding field. Information Services Management at WCU (as outlined in Section 1 of this policy) will limit System Administrator responsibilities to approved personnel.

### **4.2 Reports**

Each System Administrator will submit a report to the Information Security Manager in May and December of each year documenting compliance with all items defined in Section 2 of this policy. On-going documentation is a requirement of the documentation defined in Section 2. As such, the Information Security Manager will have “on demand” access to all required documentation maintained by System Administrators in the event of an incident or audit.

### 4.3 Reviews

Under the direction of the Vice-President of Information Services, the WCU Information Assurance Policy will be reviewed annually between October and December.

## Appendix A – Definitions

Authentication	Verification of the identity of an individual or the source of the information
Availability	Prevention of unauthorized withholding of information resources
Confidentiality	Ensuring that data is not disclosed to those not authorized to see it
Information Assurance (IA)	Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
Information Security Manager	WCU employee responsible for the administration of the WCU Information Assurance Policy and Information Security Policies.
Integrity	Assurance that data cannot be deleted, modified, duplicated, or forged without detection
IS3	The Steering Committee will provide project vision, advocacy, and leadership. It will make policy and budgetary decisions. It will be composed of West Chester University Vice Presidents, Director of Institutional Research, and Software Project Manager
ITTF	Instructional Technology Task Force - consists of faculty representatives from each college as well as representatives from university administrative and support units. Serves the role of reviewing policy and providing advice regarding technology support related to the academic mission.
Non-repudiation	Verification of the origin and receipt of messages and data
System Administrator	A WCU employee who is responsible for the technical administration of a University Information Services resource with direct control of the hardware and software of the resource.
User	Anyone who accesses a University Information Technology resource