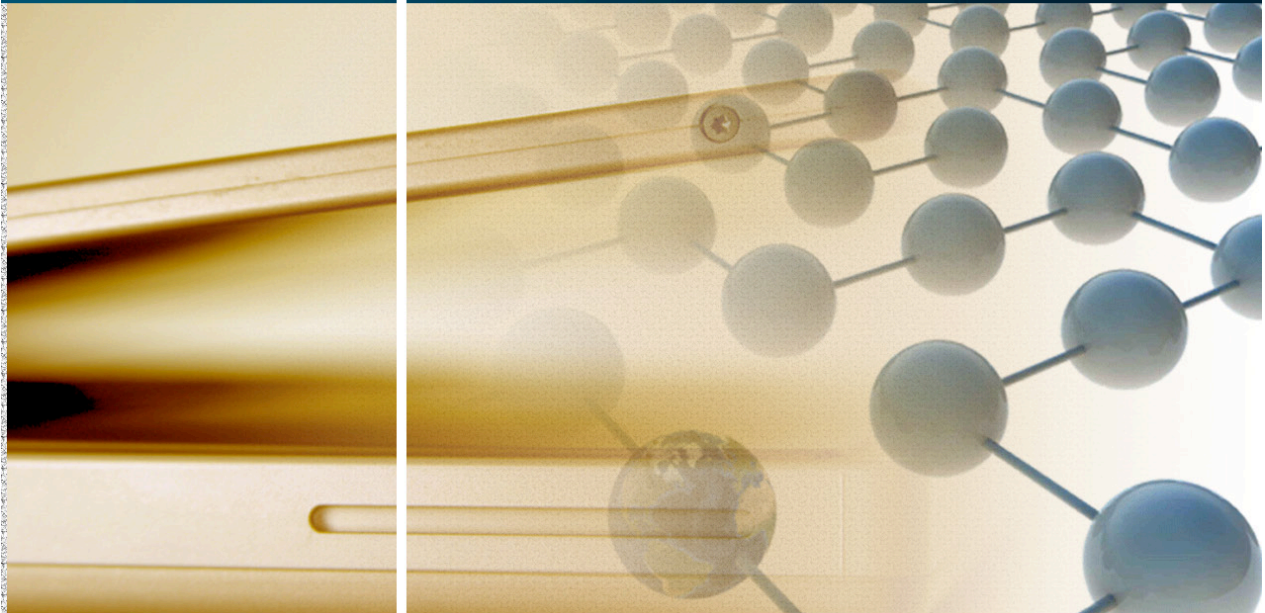




Technology Plan



2009

Porterville College

TABLE OF CONTENTS

Information Technology Mission Statement.....	1
Background.....	1
Information Technology Staff.....	2
Staff Reporting Structure	2
Participatory Governance.....	3
Information Technology Budget.....	3-4
Training Students and Staff on the use of Information Technology.....	4
Process for Providing New/Upgraded Technology Equipment and Software.....	5
Process for Repairing Technology Equipment.....	5
Minimum Computer Standards.....	6
Wireless Network.....	7-9
Wireless Policies and Procedures.....	9-10
Student use of Faculty and Staff Computers.....	10-11
Computer Lab use Procedures.....	11-12
Board Policy Section.....	12-17
Computer and Network Prohibitions.....	17-18
Computer Software use Procedures.....	18-20
Porterville College Web Page Guidelines.....	20-23
Media Services Guidelines.....	23-24

INFORMATION TECHNOLOGY MISSION STATEMENT

The goal of the Porterville College Information Technology Department is to provide a reliable technological environment that meets the needs of students, faculty, classified staff and administration and promotes a student-centered learning environment.

BACKGROUND

The current IT team has a combined experience of 50 years of service in IT. They work as a dedicated team with complete cross-training. They all have a strong desire to improve their expertise and service as much as possible.

The IT team of Porterville College supports and maintains a variety of IT equipment on the campus. They also maintain connectivity with the WAN (Wide-Area Network). They provide a full spectrum of IT services from the end user's workstation to the Internet. In addition to maintaining computers, they furnish support for a variety of printers, scanners, and other hardware and software.

As stated in the College mission statement, students are our focus. In that regard, the PC IT team collaborates district-wide with other IT professionals to provide the best possible learning environment with the most advanced technology available. They contribute to all aspects of instruction and student services by maintaining the technology involved in those areas. Additionally, they ensure that students have access to reliable computers and peripheral equipment in student computer labs.

The IT team provides desktop support for hardware and software via telephone and in person. They handle hardware repairs for computers and, peripheral devices. In addition, the team provides some training for end-users on an individual basis as needed.

The timely maintenance of equipment from the end-user's computer to the Internet and quick response time for repairs ensures that IT disruption to the College is minimized. The goal of IT is to meet technology needs as quickly and effectively as possible.

The IT team maintains approximately 650 machines for administrative, faculty, staff, and student use, including those in computer labs, classrooms, and the library. The IT team supports all staff, faculty, and administrative services including student services and business services. There is not an area on campus that does not depend upon IT to some degree. This team keeps critical campus IT operations running.

INFORMATION TECHNOLOGY STAFF

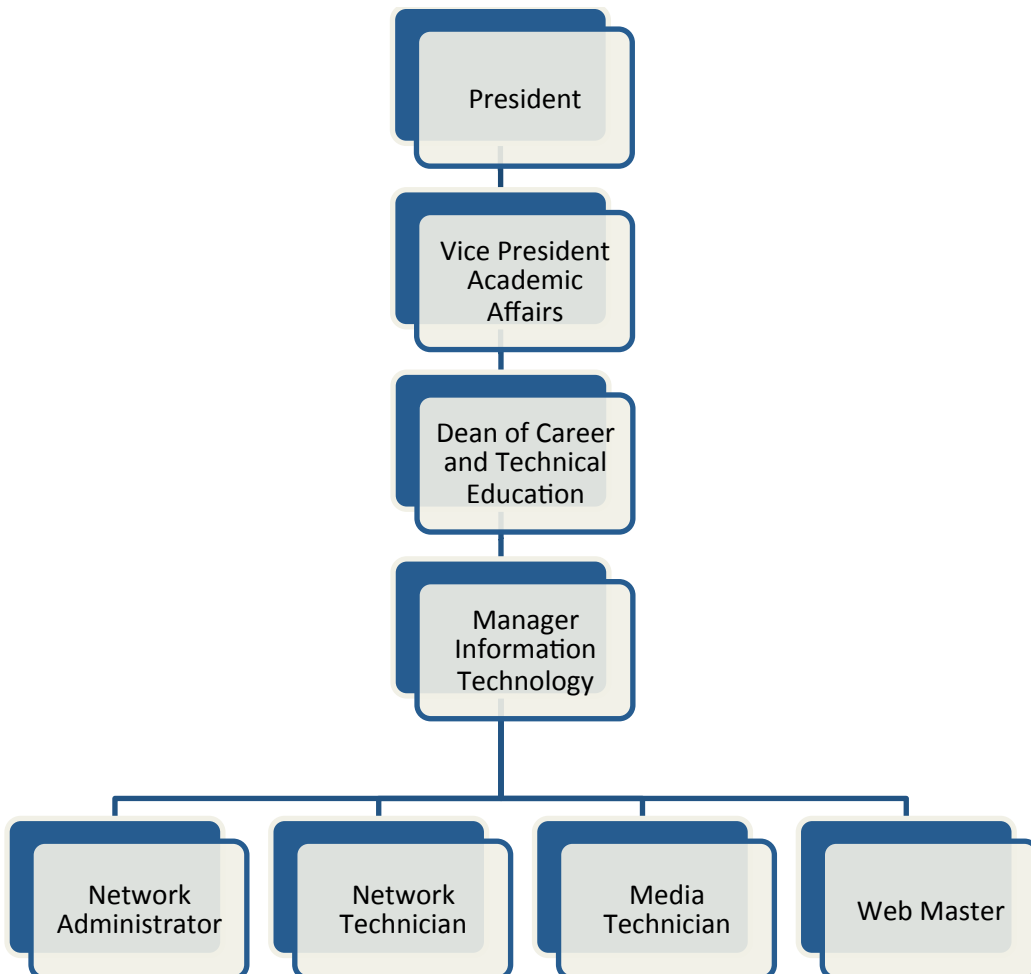
The staffing structure within the Information Technology department is designed around cooperative teamwork and 100% efficiency. This streamlined approach to staffing has forced the team to continually cross train. This cross training allows for any one member of the team to be absent yet still have their responsibilities taken care of with little or no downtime to the campus.

The current IT staff consists of the following:

One Manager of Information Technology, one Network Administrator, one Network Technician, one Media Technician, and one Web Site Coordinator.

As the network grows and as the College budget allows for it, one or two additional Network Technicians should be added to staffing structure. Adding one or more Network Technicians will allow for greater coverage, i.e. evening and early morning coverage, as well as less stress on the current IT staff.

STAFF REPORTING STRUCTURE



PARTICIPATORY GOVERNANCE

Porterville College Information Technology staff is a valuable fixture in all aspects of the college's operations therefore, they actively participate in a variety of the college's most important participatory governance committees including:

- Technology Leadership Committee
- District Wide Network Managers Committee
- District Wide Technicians Meeting
- Information Technology Committee
- College Learning Council
- Facilities Planning and Advisory Committee
- Presidents Cabinet
- Budget Committee
- Strategic Planning Committee

INFORMATION TECHNOLOGY BUDGET

The Porterville College Information Technology Department budget is based primarily on supporting the department's identified student learning outcomes - Improving student access to information technology resources and providing cutting edge technology to support student learning. Further information on the IT department's student learning outcomes can be found in the IT Program Review.

\$20,000	Supplies & Materials - Technology Services needs many supplies and materials to operate efficiently such as, hubs, switches, patch cables, software, and tools.
\$2,500	Web Coordinator – Software, supplies, materials, camera, and web design machine backup system.
\$10,000	Software Upgrade and Replacement - Many specialized software packages are being used on the campus with little or no funds to support future upgrades. This money would allow us to upgrade these packages on a regular basis.
\$10,500	Training - The technicians on the campus are very capable of doing their jobs, but with the proper training some jobs could be completed quicker and more efficiently.
\$27,615	Service Contract - Extreme service contract for the backbone of the network. This fee must be paid or the campus will run into major problems.
\$27,000	Back-up System Upgrade - As the campus network grows so should the backup system to support its needs. This will allow us to upgrade the

backup system on an annual basis and keep up with the current growth rate.

\$60,000 **Virtualization** – This will allow us to begin to the virtualization of the campus servers. Virtualization is a standard that is being adopted district wide that will ultimately reduce operation cost by reducing the amount of machines that must be maintained.

\$151,500 **Campus wide equipment replacement** - Porterville College currently has 650 systems in operation. Each new machine purchased falls under a four-year service contract.

\$309,115 **TOTAL ANNUAL BUDGET**

TRAINING STUDENTS AND STAFF ON THE USE OF INFORMATION TECHNOLOGY

Porterville College operates two general study computer labs that are staffed with Teaching Assistants and Adjunct Faculty to assist, train, and otherwise support students in all their technology training needs. Students may enroll in the zero credit Information Systems P090 class at no charge to receive these services. Students seeking help that lab staff cannot answer may find additional support through the Technology Learning Center's Educational Media Design Specialist located in the Library.

Staff seeking training and support services on the latest technology for office and classroom use can find assistance in the Porterville College Technology Learning Center. The Technology Learning Center is staffed by an Educational Media Design Specialist that is prepared to assist staff in their instructional technology needs. Holding a vast array of state of the art technological equipment the Technology Learning Center is sure to meet any instructional training requirement. Some of the most popular forms of training requested include but are not limited to:

- Online & Hybrid classes
- Making web pages
- Integrating technology into classes
- Technology use in your job

For additional information regarding the services provided by the Porterville College Technology Learning Center can be found at <http://www.portervillecollege.edu/tlc/>

PROCESS FOR PROVIDING NEW / UPGRADED TECHNOLOGY EQUIPMENT AND SOFTWARE

Request for new / upgraded technology equipment and software must go through the IT department before it is ordered to ensure the product meets all district and campus compatibility and minimum standard requirements. The following procedure must be followed for the purchase of any new technology equipment and software to be used on the Porterville College campus. Products purchased outside the following guidelines will not be installed or supported by the Porterville College IT department.

1. End-user request specific product quote from IT staff.
2. Staff reviews product request if it meets minimum standards. IT staff will provide end-user a quote from a district and campus approved vendor.
3. End-user purchases product using provided quote through the standard purchase order process. End-user must supply all funds for purchase.
4. Once the product arrives IT staff will inventory product and generate a work order to install new product in area designated by the end-user.
5. End-user signs inventory book acknowledging they received the new product.
6. IT staff closes work order.

PROCESS FOR REPAIRING TECHNOLOGY EQUIPMENT

Porterville College technology repair request will be handled through the District office help desk. All work to be performed on Porterville College technology equipment must first be entered into the District approved work order system known as Issue Track. Work orders can be submitted via email at helpdesk@kccd.edu or over the phone at 5197. IT is not permitted to work on any equipment that has not been officially entered into the Issue Track system. The process is as follows:

1. End-user having issue contacts help desk either via email or over the phone.
2. Helpdesk staff will make an attempt to repair the issue remotely if unsuccessful helpdesk staff will log the issue in the Issue Track database.
3. Local IT staff will prioritize issue and assign a Tech to the issue within the Issue Track system.
4. Staff member completes repair to end-user's satisfaction.
5. Staff member closes issue and email is sent to end-user with the resolution of the job.

MINIMUM COMPUTER STANDARDS

Porterville College continually strives to remain at the forefront of technology by maintaining high minimum standards when purchasing new computers. It has been decided that DELL Computers will be the standard brand for computers and servers for the Porterville College campus. The minimum standard machine and laptop will include the following specifications:

Dell Optiplex 760 Desktop:

- OptiPlex 760 Desktop Standard Power Supply
- Intel Core 2 Duo E8400 (3.0GHz, 6M, 1333MHz FSB)
- Windows Vista Business Downgrade, XP Professional SP3
- 4GB DDR2 Non-ECC SDRAM, 800MHz
- 256MB ATI RADEON HD 3450 (2 DVI and 2 VGA/1 TV-out Video Card
- Dell USB Keyboard
- Dell USB Optical Mouse with Scroll
- Dell 19 inch UltraSharp 1908FP Flat Panel, height adjustable stand, VGA/DVI
- 160GB SATA 3.0Gb/s and 8MB DataBurst Cache
- No Floppy
- 16x DVD+/-RW SATA
- Dell AX210 Speakers
- 4 Year ProSupport for IT and 4 Year NBD Onsite Service

Dell Precision M4400 Laptop:

- Intel Core 2 DUO T9400 (2.53GHz, 6M L2 Cache, 1066MHz FSB)
- Genuine Windows Vista Business Downgrade, XP Professional SP3
- 15.4 UltraSharp WXGA+ (1440x900) LED Display
- NVIDIA Quadro FX 770M, 512MB Video Card
- 2.0GB, DDR2-800 SDRAM, 2 DIMMS
- Internal English Keyboard
- Integrated webcam with microphone
- 80GB Hard Drive, 5400 RPM
- 8x DVD+/-RW w/Roxio and Cyberlink Power DVD Software
- 9 Cell Battery
- 130W 3P, A/C Adapter
- Dell Wireless 1397 802.11b/g Mini Card
- 4 Year Basic Limited Warranty and 4 Year NBD Onsite Service

MINIMUM STANDARD SOFTWARE

All computers installed on the Porterville College network will have the District approved minimum standard software packages installed. These packages include:

1. Microsoft Windows XP SP3 or Vista
2. Microsoft Office 2007 Professional
3. Microsoft Internet Explorer 7
4. Adobe Photoshop 6.0 or greater

Additional software for specific offices may include:

1. Internet Native Banner (INB)
2. SARS Grid and SARS TRAK
3. Schedule Plus
4. Classroom Performance System (CPS)

Student labs will have a variety of software packages installed that may not be considered “standard” for installation; this is to meet the needs of individual class requirements. All other software installation must be approved by the IT department and the campus IT committee before it is made a standard for installation on any machine.

WIRELESS NETWORK

Porterville College IT staff is instituting a phased wireless network service deployment using Aruba equipment following the accepted district-wide standard. The Porterville College IT staff would like to primarily focus on guaranteed connectivity speed rather than coverage. This speed will have to be determined by a team/taskforce on wireless (For an example only; a standard might be 20 connections with a minimum of 50Mbps connection speed).

Current Status:

Porterville College has begun its wireless conversion to the District standard of Aruba wireless products. The college IT staff has purchased and received an Aruba 3600 controller and 24 Aruba 65 wireless Access Points more commonly known as AP Duals as well as the required licensing. A wireless site survey has been completed by an outside vendor to help the IT staff determine the placement of APs for each building on campus.

Porterville College IT staff has developed a four-phase wireless implementation plan. The four-phase plan is based on funding capabilities and the order in which buildings are constructed and remodeled. Our technical staff has had the training necessary for this deployment.

PHASE 1 – Summer/Fall 2009:

The equipment for phase one has been purchased through the Library construction project and will include:

- Library – Number of Access Points will depend on wireless site survey however, this is an open building and should not require many Access Points.
- Science Math – This is a two story building consisting of 2x6 wall construction and cinder block walls will most likely require many access points to achieve the required connectivity.

Reasoning: Porterville College has taken possession of the new Library as of 5-19-2008 and the Science Math building is scheduled to come online sometime during the summer. The Library Resource Center is still a year from completion therefore we decided to put it in phase two of the project.

PHASE 2 – 2009:

Phase 2 will include:

- The Library Resource Center - The LRC being the largest portion of this phase.
- Gym and Fitness Center - There will not be a big requirement for wireless in the Gym and Fitness Center. The IT staff is anticipating on relying on coverage rather than connectivity speed in the Gym and Fitness Center.

Reasoning: Library Resource Center will be the primary hub for the campus once it is brought online therefore, it should be put on wireless as soon as possible. The gym and Fitness center will not require as much wireless equipment therefore, it is reasonable to add it to the LRC implementation phase.

PHASE 3 – Timeline depends on budget:

Phase 3 will include:

- Academic Center - The Academic Center holds the largest wireless requirement in this phase. Many Information System classes are conducted in this building therefore; the IT staff would like to focus on connectivity rather than coverage in this area.
- Student Center - The Student Center already has DSL fed wireless access, when phase 3 is implemented Porterville College IT staff intends to shutdown that connection in order to move the building to the new Aruba standard of wireless. The Student Center is an open area that can be easily covered with few access points.
- Fine Arts buildings - Fine Arts should have the same connectivity as the Academic Center and other student populated areas.

Reasoning: The Student Center can wait until this phase because they already have wireless connectivity via the DSL connection. The Academic Center was put on this phase because the IT staff is trying to keep up with the new and remodeled buildings. If they tried to bring the AC building online with or before the other two phases there would be no funds to keep up with the other buildings on the campus.

Phase 4 – Timeline depends on budget

Phase 4 will include any remaining outlying buildings:

- M&O
- Power Tech
- Trade Industry
- Health Careers
- Child Care

Reasoning: These buildings are not heavily populated by students and will only require wireless coverage not a guaranteed connection speed. It is anticipated that very few Access Points will be needed for each of these areas. Outdoor coverage can be addressed in this phase as well depending on district standards for outdoor wireless coverage.

WIRELESS POLICIES AND PROCEDURES

Wireless internet and network access is provided to all employees, students, and guest/visitors. Both personal and district owned equipment may be attached to the wireless network. It is for this reason we have two different wifi connections, KCCDopen and KCCDsecure. KCCDopen can be used by anyone on any machine as long as they have a valid network log-on account.

KCCDopen can be used on any wireless machine. To protect the network from out-of-date virus protection and potentially harmful software; KCCDopen will only allow internet access via a wifi connection. It is still strongly recommended that virus protection is installed on the machine and fully up-to-date before connecting to the network. There is no special account required for wifi access for employees and students, simply use the same account that is used on the standard computers on the network preceded by the pc\ in the username field.

KCCDsecure is for employees who make use of a **district owned** laptop or wireless devices who wish to get their network drives as well as internet access via the campus wifi. The process is a little different than KCCDopen. First the wireless device must be owned by the district i.e. purchased via some form of funding within the district. This does not include someone purchasing the equipment and then “donating” it to the campus.

The wireless device must be brought to the Technology Services office where the machine can be inventoried, have up-to-date virus protection installed, and be put in a special group on the network that will give it the rights to map the desired drives. There will be no exceptions to this policy the equipment must be district owned and be brought to the Technology Services office before it can access the KCCDsecure SSID and get mapped network drives.

Guest/visitors who wish to access the internet via wifi must go to the computer commons in the LRC to obtain a four hour log-in account to use the wireless. Guest/visitor accounts are required to access the wifi and will automatically expire four hours from the time of creation. If extended time is needed we can make exceptions on an as needed basis.

Access to the wireless network does not open the door for personal equipment on the network. Personal equipment is still not allowed on the network and will be removed if it is found connected. No one should ever plug-in personal equipment into the network via a network cable or any other method. The use of personal equipment on the district network puts everyone at risk of, viruses, hacking, and poor network performance.

When using the wifi or any other form of network or internet access via a district connection staff are bound to the procedures and prohibitions found in the Board Policy section 3E, as well as the procedures, prohibitions, and acceptable use policies found in the Porterville College IT Plan and on the wifi log-in page.

COMPUTER USE POLICIES AND PROCEDURES

The computer use policies and procedures for Porterville College are outlined in the District Information Technology Plan on Computer Use Procedures that have been amended to include a Board adopted Policy Section and a Chancellor's Cabinet approved Procedure section.

STUDENT USE OF FACULTY AND STAFF COMPUTERS

Porterville College's network is based on what is commonly known as a Microsoft Domain. Within a domain users are assigned rights or permissions for access on various parts of the network. As such, student users are given far less permissions to critical support service areas of the network such as Banner, than staff and faculty are given. In many areas some staff and faculty have exclusive access to Banner and financial systems that students should never be given access to. It is vital that faculty and staff protect their user names and passwords at all times as not to compromise their access to these critical systems.

Students including student aids should never be allowed to use a faculty or staff member's username or password for any reason. Faculty and staff should never leave

their usernames and or passwords in visible locations for any reason. Writing down a username and or password and leaving it in the work area is strictly prohibited. Students should always be directed to use computers configured and designated for student use.

If for any reason a student must use a faculty or staff computer they must use their own username and password. Students should never be on a faculty or staff computer when the faculty or staff member is logged into the system. Allowing students to access computer systems with faculty or staff login accounts puts the entire campus and district at risk of identity theft, virus attack, hacking, grade changes, and financial disaster.

COMPUTER LAB USE PROCEDURES

Introduction:

In pursuit of its mission, Porterville College provides access to computing and information resources for students, faculty, staff, and other authorized users. This use is restricted by the compliance to the district Computer Use Policy, Porterville College computer Use Policy, and the Porterville College Student Code of conduct, as listed in the Porterville College Student handbook.

Policy:

1. Violation of computer use policies and student codes of conduct may lead to loss of access to computing resources, as well as to disciplinary and/or legal action.
2. Computer use must be within the bounds of Federal and State Law.
3. Computer use is intended for the support of course work conducted for particular class assignments. Students using computers for non-class related activities (including chat rooms) will be asked to relinquish their workstations when students with class-related assignments are waiting.
4. Resources on the Internet could be potentially offensive. Users will respect the rights of others to be free from sexual harassment and a hostile environment by not downloading pornography.

NOTE: There is a zero tolerance policy in the computer commons.

5. Excessive noise and/or creating a disturbance may result in the restriction of use and/or disciplinary action.
6. Information obtained from the World Wide Web and other Internet sources may be inaccurate or misleading. The college cannot be held accountable for the authenticity of information gathered from these sources.
7. Technical difficulties do occur. The college is not responsible for any information that may be lost, damaged or unavailable due to technical or other difficulties.

8. If a user of the network is believed to be in violation of Federal or State law, or specific district prohibitions, a user revokes his right to privacy.
9. The first violation of these policies will result in a warning and an explanation of the violation to the user. The violator's name will be referred to the Vice President, Student Services.
10. The second violation of these policies will result in the initiation of disciplinary action as deemed appropriate by the Dean of Students, in accordance with the College/District policies and procedures regarding student discipline.

BOARD POLICY SECTION

- 3E1** Computing and Network Use (*Revised July 9, 2009*)
- 3E1A** The Kern Community College District shall provide computing and network resources that benefit faculty, staff, and students and support the instructional and administrative activities of the Colleges and the District. The District is committed to policies which promote the mission of the Colleges and encourage respect for the rights of individuals. These policies shall apply to all individuals using College and District computing and network resources, regardless of access method.
- 3E1B** Computing and network resources and all user accounts provided by the Kern Community College District are the property of the Kern Community College District. Access to College/District computing and network resources is a privilege that may be wholly or partially restricted by the Kern Community College District without prior notice and without the consent of the user if required by and consistent with policy or law, when there is substantiated reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs.
- 3E1C** Employees have no privacy whatsoever in their personal or work-related use of District computers, electronic devices, network and other electronic information resources or to any communications or other information in Kern Community College District computing and network systems or that may be transmitted through Kern Community College District computing and network systems.
- 3E1D** Kern Community College District retains the right, with or without cause, and with or without notice to the employee, to remotely monitor, physically inspect or examine Kern Community College District computers, electronic devices, network or other computing and network resources and any communication or information stored or transmitted through Kern Community College District computing and network resources including

but not limited to software, data, image files, Internet use, emails, text messages and voicemail.

Kern Community College District shall exercise this right only when required by and consistent with policy or law, when there is substantiated reason to believe that violations of policy or law have taken place, or in exceptional cases, when required to meet time-dependent, critical operational needs.

- 3E1E** Use of computing and network resources must be for activities related to the mission of the Colleges and the District. Computing and network resources are to be used in an effective, efficient, ethical, and lawful manner.
- 3E1F** Use of computing and network resources imposes responsibilities and obligations on the part of users. Users are expected to demonstrate respect for intellectual property, data ownership, system security, individuals' rights to access information, and freedom from intimidation or harassment. (See **Procedure 3E1C(a)** of this Manual for Computing and Network Use Prohibitions; **Policy 3E4** of this Manual for Information Technology Security Policy; **Policy 3E3** of this Manual for Email Policy; Procedure **3E1C(b)** of this Manual for Computer Software Use Procedures; and **Appendix 3E1C** of this Manual for the Software Registration form.)
- 3E1G** Computing and network use shall be consistent with the educational, academic, and administrative purposes of the Colleges/District and shall respect the rights of individuals.
- 3E1H** The Colleges may develop and implement procedures related to college computing and network use. (See **Procedure 3E1F** of this Manual for College Computing and Network Use Procedures.)
- 3E1I** Sanctions for violation of the District/College Computing and Network Use Policies or Procedures may be imposed. Sanctions may range from a warning, to restriction of use, to disciplinary action, and/or legal action.
- 3E1J** Definition of Kern Community College District Computing and Network Resources includes, but is not limited to:
Any computer, including a laptop computer, that is:
- Owned, leased, or rented by the Kern Community College District
 - Purchased with funds from a grant awarded to the Kern Community College District

- Borrowed by the Kern Community College District from another agency, company, or entity
- Any electronic device other than a computer that is capable of transmitting, receiving, or storing digital media and is:
 - Owned, leased, or rented by the Kern Community College District
 - Purchased with funds from a grant awarded to the Kern Community College District
- Borrowed by the Kern Community College District from another agency, company, or entity

Electronic devices include, but are not limited to:

- Telephones
- Cellular Telephones
- Push-to-Talk Radios
- Pagers
- Radios
- Digital Cameras
- Personal Digital Assistants such as Palm Pilots and Smart Phones
- Portable storage devices such as USB thumb drives
- Portable media devices such as iPods and MP3 players
- Printers and copiers
- Fax machines

Any component that is used to build or support the Kern Community College District network including, but not limited to:

- Routers
- Switches
- Servers
- Enterprise Storage Systems
- Microwave Components
- Firewalls
- Cabling Infrastructure
- Wireless Access Points and Controllers
- Telephone Switches
- Voicemail Systems
- Network Management and Monitoring Systems

3E4 Security Policy (*Added July 9, 2009*)

3E4A Introduction

Kern Community College District has an obligation to ensure that all Information Technology data, equipment, and processes in its domain of

ownership and control are properly secured. This obligation is shared, to varying degrees, by the Colleges and their Centers and every employee of the Kern Community College District. Meeting this obligation is critical to achieving Kern Community College District's mission of providing outstanding educational programs and services that are responsive to our diverse students and communities.

In order to carry out its mission, Kern Community College District shall provide secure yet open and accessible Information Technology resources to all employees and students. Toward this end, Kern Community College District will strive to balance its Information Technology Security Program efforts with identified risks that threaten the availability and performance of mission critical computing and network resources.

Kern Community College District shall ensure that the use of Information Technology resources complies with the appropriate Kern Community College District policies and procedures and applicable Federal and State regulations.

3E4A1 Definitions

a. Information Technology Resources: people, processes, and technology needed to deliver Information Technology services (Banner, e-mail, online classes, etc.) to Kern Community College District employees and students.

b. Computing and Network Resources: any and all technology (servers, personal computers, applications, laptops, routers, etc.) that make up Kern Community College District's vast Information Technology operation.

3E4B Scope of Information Technology Security

3E4B1 Information Technology Security Defined

Information Technology Security is defined as the state of being relatively free of risk. This risk concerns the following categories of losses:

a. Confidentiality of Information Technology data or privacy of personal data and college data

b. Integrity or accuracy of personal data and college data stored in Information Technology systems

c. Information Technology assets which include Information Technology systems, networks, facilities, programs, documentation, and data

d. Personal and college data stored in Information Technology systems

Information Technology Security is also viewed as balancing the implementation of security measures against the risks that have been identified and weighted against the effective operation of the Kern Community College District.

3E4B2 Domains of Information Technology Security

Kern Community College District's Information Technology Security shall deal with the following domains of security:

- a. Computer Systems' Security: servers, workstations, applications, laptops, mobile devices, operating systems, and related peripherals used by Kern Community College District employees and students
- b. Network and Communications Security: all equipment, people, and processes in place to operate Kern Community College District's network and communications infrastructure
- c. Physical Security: premises occupied by Information Technology personnel and core (not end-user) Information Technology equipment such as servers, routers, and switches
- d. Operational Security: environmental systems such as HVAC, power, and other related operational systems

3E4B3 Information Technology Security Program

Kern Community College District shall have an Information Technology Security Program comprised of the following components:

- a. A framework for classifying, reviewing, and updating Kern Community College District's Security risk posture (Risk Assessment)
- b. A framework for identifying location, type, sensitivity, and access requirements for all data residing anywhere within the Kern Community College District

Documentation of Information Technology Security Program roles, responsibilities, processes, and architecture

A plan for identifying, prioritizing, and addressing applicable Federal, State, and other legal compliance requirements

Appropriate Information Technology Security policies, procedures, and guidelines An Information Technology Security Awareness and Information Dissemination plan

A plan for identifying, validating, prioritizing, implementing, and auditing Information Technology security technology initiatives needed to effectively secure Kern Community College District's Information Technology operations

3E4C Roles and Responsibilities

3E4C1 Within the context of Information Technology Security, all Kern Community College District employees and students are responsible to some degree for safeguarding the Information Technology resources they use. Equally, all Kern Community College District employees and students are expected to comply with all Kern Community College District Information Technology Security policies and related procedures.

3E4C2 The Information Technology Managers from the three Colleges and the District Office are responsible for Information Technology Security throughout Kern Community College District.

3E4C3 Kern Community College District's Director, Information Technology is responsible for carrying out Kern Community College District's Information Technology Security Program as outlined in 3E4B3

3E4C4 Appropriate College and District-wide committees shall have the opportunity to provide input on the development of Information Technology Security policies and procedures.

3E4D Sanctions

3E4D1 Violations of this policy are subject to the established Kern Community College District disciplinary processes as outlined in Kern Community College District Board Policy and Kern Community College District employee contracts.

Acknowledgements: Kern Community College District acknowledges Murdoch University of Perth, Western Australia (www.murdoch.edu.au), and the University of Minnesota (www.umn.edu) for allowing Kern Community College District to use their Information Technology Security policy material.

PROCEDURE 3E1C(a)

Computing and Network Use Prohibitions

Improper uses of Colleges/District computing and network resources are prohibited as follows:

(1) The use of computing and network resources for cheating, plagiarism, furnishing false information, other acts of academic dishonesty, or malicious behavior that interferes with meeting the College/District educational mission is prohibited.

(2) The use of computing and network resources shall not interfere with the work of employees or students nor disrupt the normal operation of the Colleges/District.

(3) Computing and network use that monopolizes resources; network use that creates unnecessary network traffic; broadcast of inappropriate electronic mail and messages; transmission of electronic chain letters or other requests for money; and distribution or circulation of media known or suspected to contain computer viruses are prohibited.

(4) Copying, distributing (either free or for monetary gain), or receiving copyrighted software or electronic information without paying the specified royalty (U.S. copyright laws) are prohibited.

(5) Unauthorized computing and network account sharing is prohibited.

(6) Attempts to gain unauthorized access to any computing or network resource are prohibited.

(7) Unauthorized commercial or business use of Colleges/District computing and network resources for individual or private gain is prohibited.

(8) Use of Colleges/District computing and network resources to intentionally transmit, receive, display or copy obscene, pornographic, discriminatory or harassing materials not related to coursework or research is prohibited.

(9) Use of Colleges/District computing and network resources to access or attempt to access student or employee information for any purpose not specifically job-related violates state and federal laws and District policy and is prohibited.

(10) The Electronic Communications Privacy Act (federal law) includes electronic mail and messages in the same category as U.S. mail and telephone calls, and defines unauthorized attempts to access another user's information as unlawful behavior. Such behavior is prohibited.

Reviewed and Recommended by
Chancellor's Cabinet, September 16, 2008
District Consultation Council, May 18, 2009

PROCEDURE 3E1C(b)

COMPUTER SOFTWARE USE PROCEDURES

- 1) Only software which falls into one of the following categories may be used on equipment which is under the jurisdiction of the Kern Community College District:
 - a) The software has been purchased by the District in sufficient quantities to account for one purchase for each machine on which the software is used, and a written record of the purchase is available in District files.

- b) The software is covered by a licensing agreement with the software author, vendor, or developer, as applicable; no tenets of the agreement have been violated by the user; and a written copy of the agreement is available in District files.
 - c) The software has been donated to the District in accordance with the software license, and a written record of the donation or its acceptance is available in District files.
 - d) The software has been developed or written by a District employee for use on District equipment, and full credit has been given to the developer by other users.
 - e) The software is in the public domain, and documentation exists to substantiate its public domain status.
 - f) The software is being reviewed or demonstrated as part of a purchasing or licensing decision, and arrangements for such review or demonstration have been satisfactorily reached between the District and the appropriate vendor or representative.
 - g) The software is the personal property of the user, and these procedures and software license requirements are followed.
- 2) According to law, all copies are illegal unless they fall into one of the following categories:
- a) The copy is created as an essential step in the utilization of the computer program in conjunction with a machine, and it is used in no other manner.
 - b) The copy is for archival purposes only, and all archival copies are destroyed when continued possession of the computer program ceases to be rightful.
 - c) The copy is in compliance with the license agreement.
- 3) In order to certify the District's right-to-use software installed on District-owned computers, copies of all software licenses shall be on file at a designated location. When installing software on a District-owned computer, the person completing the installation is responsible for the following:
- a) Installation of the software according to instructions provided by the software author/distributor.
 - b) Completion of a Software Registration Form.

- c) Forwarding the Software Registration Form, the Software License Agreement received with the software, and a copy of the software purchase order to the designated location. These documents constitute an archival record.
- 4) If a software audit is performed either by District staff, law enforcement officers, or regulatory agencies, the archival records will be used to prove ownership of specific software products. If an archival record does not exist for a specific copy of software and the user is unable to provide proof of legal use as stated in these Procedures, the software will be deleted from the computer's storage media, and all backup copies will be destroyed.

This section was approved by the Chancellor's Cabinet
May 23, 1993
Renumbered 4/21/94, 2/11/97, and 10/11/00

PORTERVILLE COLLEGE WEB PAGE GUIDELINES

Faculty and staff at Porterville College design a variety of web pages. These pages play an important role in the institutional image and advancement of the college. These pages require coordination and guidelines if they are to demonstrate a professional appearance and common "look and feel" for consistency.

Information presented on the PC website should be accurate, timely and germane, while still allowing for an appropriate measure of freedom of expression. For these reasons, a periodic review and evaluation of sites is needed. This web page guideline procedure is the first step in establishing reasonable standards. The procedures include a listing of page elements, recommended style guidelines and suggestions.

Web Access:

Any PC staff member wishing to develop a website should contact the Web Site Coordinator for a web directory, log-in and password to the PC web server.

PC Web Site Coordinator:

The Porterville College Web Site Coordinator reviews all PC website submissions and website links. The Coordinator monitors materials attached to the PC home page for compliance to Porterville College and Accessibility standards. Before submission to the Web Site Coordinator, Division Chairs or the appropriate department head may review them and sign-off. The Coordinator may suggest modifications for "look and feel" conformity or assess the merits of the site against the campus standards.

Web Pages:

Web pages represent both the college and the faculty or staff member's best effort. The pages should:

- Reflect a high level of excellence related to the educational program, student service areas or college activities;
- Support the mission and goals of the college;
- Have a common “look and feel.”

General Website Content Standards:

- Porterville College’s name must appear in the page title **and** near the top of the page.
- Links returning to the PC home page: www.portervillecollege.edu must be on each page.
- The title of the department or division or subject identifier should be located near the top of the web page.
- Web pages must conform to Section 508 Accessibility Standards. (Please see Accessibility Guide Sheet)
- The initiator is responsible for the currency and revision of his/her web site.
- Materials approved by division or department heads are published to the web server and, after review by the Web Site Coordinator, linked to the PC Web Page.
- External links are related to the website theme.

It is important to the college that our web sites:

- Have correct and timely information.
- Have content appropriate for our audience.
- Are branded appropriately.
- Are easy to use.
- Comply with Section 508 and other applicable laws.
- Are interactive where appropriate. (Use technology for a purpose)
- Use correct grammar and spelling.

As such, we recommend the following policies:

- With few exceptions, sites that aren’t updated at least once in the last 6 months will be removed.
- Monthly reviews are recommended. Exceptions will include archived information like past class schedules, catalogs, publications, history, etc.
- Agreeing to create a website obligates the requestor to update the site regularly as if it were part of their job description. If at any point a site doesn’t have someone assigned to update it regularly, the site will be removed.
- Content will be managed and updated by staff and faculty around the campus but the Web Coordinator will manage the placement content within our site. Content that is particularly useful and is regularly updated will be featured more prominently.

Unacceptable Materials:

These materials or practices are unacceptable because they may violate copyright laws, accepted practice or protocol:

- Copyrighted materials in any form, unless granted written permission and identified as such
- Confidential information as defined by laws or KCCCD policy.
- Photographs or videos of persons without the authors/publishers expressed written permission
- Personal, private or commercial activities or advertisements.
- Other content/material prohibited by law or KCCCD policy.

Division/Department Home Page Standards:

In addition to the items listed above, the following standards are suggested:

- Description of the division/department
- Description of the division/department programs
- List of faculty members: email addresses
- Name and email address to Division Chair or Division contact person

Faculty/Staff Home Page Requirements:

The following guidelines are suggested:

- Courses taught and/or services provided
- Course syllabi
- Office hours
- Personal information
- Photo (optional, service available from Web Site Coordinator)
- Background: education and/or experience

Graphics and Background Guidelines:

Graphics and background can add attractive enhancements to a website. Developers should use them to enhance their site. These guidelines are provided to support these enhancements:

- Keep file sizes small. Large and complex graphics may have a very long load time. [Section 508 Standards, Section 1194.22 (a) - A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).
- GIF and JPEG are the preferred formats for graphics or digital photos.

- Attractive backgrounds benefit from light colored, pastel or faded graphics. An attractive background is easier to read.
- Avoid bright, distracting colors.
- Keep animations to a minimum. (only one per page)
- Blinking images or text violates Section 508 guidelines, as does the “marquee” function.
- Related pages should use commonly colored backgrounds for consistency.
- Section 1194.22, (c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.

Testing Guides:

Websites are built to work. Computerized devices don't always work as they should, so developers are required to test their website. The following are some possible steps:

- View pages through an Internet browser to check for errors.
- Cross check errors: run through two or more browsers to ensure maximum compatibility; for example, Netscape 4.0 or higher and Microsoft Explorer 4.0 or higher.
- Test links to assure that they go to the intended website.
- Return linked sites to source home page.

Other Thoughts:

The PC site showcases current and upcoming events or activities. If there is something that faculty or staff would like placed on the site, contact the Web Site Coordinator. The PC website, like the Internet, is in a constant state of flux. The basic nature of both systems is change.

MEDIA SERVICES GUIDELINES

One of the most vital support services the Information Technology department provides is Media Services. Media Services can provide many support functions to faculty and staff. Services include but are not limited to, equipment checkout and service, media duplications, multimedia support, video tapping, and editing. The following list of Media Services guidelines has been developed to help identify the services available.

Duplication:

Audiocassettes, CD, and DVD can be copied by high-speed duplicators (if NOT in violation of copyright). Media will be duplicated within 48 hours (unless in large quantity).

Equipment:

Media equipment can be delivered to your classroom or be ready for pickup at the LRC. All equipment requests must be made 48 hours in advance. After 3:00pm, neither staff nor equipment is available. Staff are encouraged to reserve early. We have only 1/2" VHS and DVD.

Equipment failure in a classroom can only be repaired during the day. No evening service for media equipment is available.

Multimedia equipment requests must be made 2 weeks in advance. With the exception of videotaping classroom activities, equipment must be operated by the instructor. If you need instruction on any piece of equipment, please call the Media Department for a special hands-on session in advance of your class.

Satellite:

CCCSAT (California Community College Satellite) programming is available on campus and tapes can be made (within copyright guidelines). Contact Media Services as far in advance as possible.

Video:

Video Camera request must be made through the helpdesk. If a student needs to use video camera for class, the instructor will need to request and pickup/return the camera. The instructor will be responsible for the camera.

Video Taping of Your Class or Activities:

Media Services will videotape speakers or other special activities. Please request 2 weeks in advance for staff work schedules may have to be rearranged to videotape at the time you need it. For all campus and/or guest speakers, the staff member in charge of the activity will need to get a written permission from the speaker to be videotape.

Video Editing/Format Transfer:

Video editing is available by appointment only. Appointments can be made with Media Services during regular business hours.