2014-
2017

PORTERVILLE COLLEGE
IT PLAN

Porterville College Information Technology Plan - 2014-2017

Revised: November 3, 2014

TABLE OF CONTENTS

INFORMATION TECHNOLOGY MISSION STATEMENT

The Porterville College Information Technology Department will maintain a reliable technological environment by providing comprehensive support that meets the needs of students, faculty, classified staff and administration to promote a student-centered environment for teaching and learning.

BACKGROUND

The current IT (Information Technology) team has a combined experience of 65 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 work closely with KCCD (Kern Community College District) IT staff to maintain connectivity with the WAN (Wide Area Network).

As stated in the College mission statement, students are our focus. In that regard, the PC IT team collaborates with other district-wide 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.

The IT team provides desktop support for hardware and software via telephone and in person, remotely, and over the phone when needed. The IT team ensures that students have access to reliable computers and peripheral equipment in student computer labs.

The IT team handles hardware repairs for computers and peripheral devices. In addition, they provide some training for end-users on an individual basis as needed.

The timely maintenance of equipment from the end-user's computer to the infrastructure 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 responsively and effectively as possible.

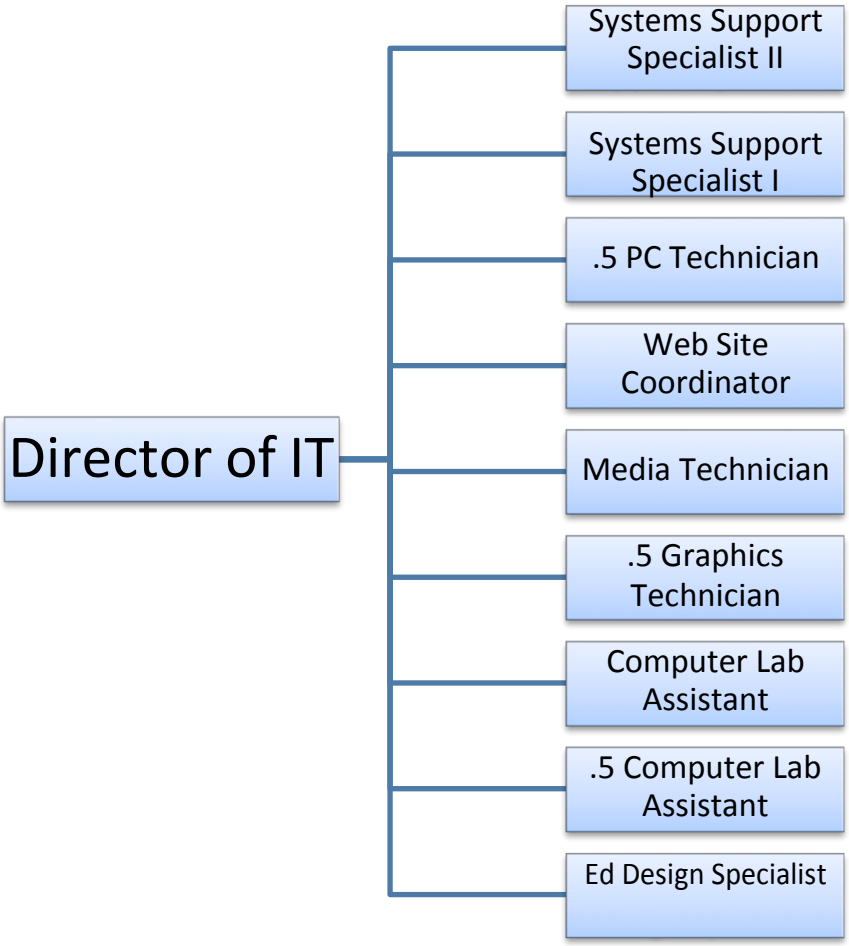
The IT team maintains approximately 700 machines for administrative, faculty, staff, and student use, including those in computer labs, classrooms, and the library.

The IT team supports all staff, faculty, and administrative services including student services and business services. The team keeps critical campus IT operations running.

INFORMATION TECHNOLOGY STAFF

The staffing structure within the Information Technology Department is designed around cooperative teamwork with the highest efficiency possible. This streamlined approach to staffing has forced the team to continually cross train. Cross training allows for a 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:



As the network grows and as the College budget allows for it, the one part-time PC Technician and one part-time Graphics Technician should both be made full- time.

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:

- District Wide Network Managers Committee
- Information Technology Committee
- College Learning Council
- Facilities Planning and Advisory Committee
- President's Cabinet
- Budget Committee
- Strategic Planning Committee
- Distance Education 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.

4313 Non-Instructional Supplies and Materials	$16,000
5119 Other Non-Instructional Consulting Services	$2,500
5220 Employee Travel	$2,000
5650 Software Licensing/ Maintenance	$22,500
5685 Computer Hardware Maintenance Agreements	$40,000
5690 Other Maintenance/Repairs	$4,500
5880 Taxes – Licenses & Permits	$117

5890 Other Services & Expenses	$550
6214 Buildings – Testing & Inspection	$500
6412 Computer/Technology Equipment	$58,000
6412FA Computer/Technology Equipment Fixed Assets	$22,256
TOTAL ANNUAL DISCRETIONARY BUDGET	$168,923

TRAINING STUDENTS AND STAFF ON THE USE OF INFORMATION TECHNOLOGY

Porterville College has made it a priority to effectively implement technology in support of its institutional mission, and training is a key component. There are a number of ways in which training for effective use of technology is accomplished at the College. The college offers a number of training opportunities for students.

- Free workshops on popular Microsoft Office (MS Office) programs.
- Learning Center orientations provided by the Learning Center Technician (LCT).
- One-on-one help from the LCT as needed.
- Microsoft Office online tutorials provided on the College's website.

College employees have a number of support resources when it comes to effective use of technology. These include:

1) A staff technology lab (Technology Learning Center or TLC). This contains state-of-the-art computer hardware and software. The Educational Media Design Specialist (EMDS) assists with employee use of the lab equipment by appointment and as needed. There is also a binder in the TLC with step-by-step instructions for the most commonly performed functions, in the event that the EMDS is unavailable.

2) The TLC Website. Employees can find job-aids, technology tips, and links to a wide variety of technology training resources.

3) FLEX day's technology training events. Presenters include the College's Web Coordinator, the College's IT Technicians, the EMDS,

a KCCD technology representative, or occasionally hardware or software representatives.

4) Technology workshops. The EMDS offers a variety of technology workshops each semester to help faculty and staff effectively incorporate technology into their college functions.

5) Technology training camps. Immediately after the spring semester, the EMDS frequently offers a technology training camp, involving multiple days of training and culminating in a completed project.

6) One-on-one assistance from TLC. Faculty members who utilize the College's Learning Center receive training from the LCT on the special software used in that lab.

In addition to the training opportunities previously mentioned, all employees and students of the College can get immediate assistance with technical questions by contacting the help desk, which is available by phone or the Web, 24 hours a day, 7 days a week. Students working on computers in the Computer Commons can get immediate help from the on duty Computer Lab Assistant.

EXISTING AND FUTURE TECHNOLOGY

Currently, Porterville College is connected to the Kern Community College District via two 30MB data line connections. These connections allow access to district based applications and also provide internet access for the College connecting through the District Office.

This current data line is scheduled to be upgraded with a 1GB fiber data connection back to the District Office. 300MB of the 1GB will initially be allocated for the network connection. The data line upgrade is scheduled to be implemented by Spring 2015.

The College is scheduled to connect directly to the internet and will no longer connect out through the District Office. The installation should be complete by Spring 2016. This new connection to the internet will be via an additional 1GB fiber data connection. It will allow for a greater bandwidth connection, which will increase internet response times.

The College currently offers Wi-Fi access to users via two Wi-Fi SSID groups, KCCDOpen and KCCDSecure. The Wi-Fi access points for these groups connect via the 802.11 b/g standard. Future projects will include upgrading all Wi-Fi access points to the newer standards of 802.11ac, to allow for faster connection speeds to the network.

STANDARD ANNUAL IT REPLACEMENT PLAN

The goal for technology equipment replacement is to replace equipment which is three years old or older.

1. Emphasis for equipment replacement will be placed on student use areas such as classrooms, commons areas, computer labs and student work rooms.

2. Equipment will be evaluated for replacement. Any equipment which is still functioning and useful may have hardware upgrades or rebuilds applied to them. This equipment may then be sent to other areas for use.

3. Dependent upon budgetary constraints, equipment replaced under the annual replacement plan may be replaced with brand new equipment or certified refurbished equipment.

4. Software will be evaluated to ensure it is still required. If newer versions are available and are compatible with current operating systems, recommendations will be made for software upgrades.

PROCESS FOR PROVIDING NEW / UPGRADED TECHNOLOGY EQUIPMENT AND SOFTWARE NOT ON STANDARD ANNUAL IT REPLACEMENT PLAN

Requests for new or replacement technology equipment and software, not on the standard annual IT replacement plan, must go through the IT department before it is ordered. This will ensure that the product meets all

district and campus compatibility and minimum standard requirements. The following procedure must be followed for the purchase of any new or replacement 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 requests specific product quote from IT staff.

2) Staff reviews product request to determine if it meets minimum standards.

3) IT Director will review requesting departments Program Review for justification of the request.

4) IT staff will provide end-user a quote from a district and campus approved vendor.

5) End-user purchases product using provided quote through the standard purchase order process. End-user must supply all funds for purchase.

6) Once the product arrives, IT staff will inventory the product and generate a work order to install the new product in the area designated by the end-user.

7) End-user signs inventory book acknowledging they have received the new product.

8) IT staff closes work order.

PROCESS FOR REPAIRING TECHNOLOGY EQUIPMENT

Porterville College technology repair request will be handled through the outsourced help desk service. All work to be performed on Porterville College technology equipment must first be entered into the work order system.

Work orders can be submitted electronically at support.kccd.edu or over the phone at 877-382-3508 or at 5197 for calls from within the district. IT is not

permitted for any work to be done on equipment that has not been officially reported to the help desk service.

The process is as follows:

1) End-user contacts help desk either via web ticket at http://support.kccd.edu or over the phone.

2) Helpdesk staff makes an attempt to repair the issue remotely. If unsuccessful the helpdesk staff will log the issue in the work order systems.

3) During normal business hours 8:00am – 5:30pm, instructional down situations are expedited and local technical staff are called immediately. After 5:30pm, instructional down situations are handled by the help desk service.

4) Local IT staff will prioritize the issue and assign a technician to deal with the issue within the work order system.

5) IT staff member completes repair to end-user's satisfaction.

6) IT staff member closes issue an 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 determined that DELL will be the standard brand for desktop computers and servers for the Porterville College campus. The minimum standard desktop and laptop will include the following specifications:

Dell Desktop:

- Desktop Small Form Factor
- Intel i5 Processor 3.0GHz
- Windows 7 Enterprise
- 8GB RAM
- 1GB NVIDIA VGA Dual Monitor Support Video Card

- USB Keyboard
- USB Optical Mouse with Scroll
- 22 inch Professional P2214H Widescreen Monitor, Height Adjustable Stand, VGA/DVI
- 250GB SATA Hard Drive
- No Floppy
- 16x DVD+/-RW SATA
- Speakers

Dell or Lenovo Laptop:

- Intel i5 Processor 2.5GHz
- Windows 7 Enterprise
- 14 inch HD WXGA+ LED Display
- GeForce 1GB Video Card
- 8GB RAM
- Integrated English Keyboard
- 320GB Hard Drive, 5400 RPM
- 8x DVD+/-RW w/Roxio and Cyberlink Power DVD Software
- 9-Cell Battery
- 65W, A/C Adapter
- Wireless 1707 802.11n Mini Card

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 Wi-Fi SSID's, KCCDopen and KCCDsecure.

KCCDopen can be used by anyone on any wireless machine as long as they have a valid network log-on account. To protect the network from out of date virus protection and potentially harmful software; KCCDopen will only allow internet access.

It is still strongly recommended that virus protection is installed on the machine and fully up-to-date before connecting to any Wi-Fi network. There is no special account required for Wi-Fi access. Employees and students simply use the same account that is used on the standard computers on the network.

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 Wi-Fi. 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 Wi-Fi network and get mapped network drives.

Guest/visitors who wish to access the Wi-Fi must attach to the KCCDopen network and follow the Visitors link below the captive portal login page in the web browser.

On the visitor login page if you don't already have a login click on the "Don't have a Wi-Fi visitor username and password?" link below the user name and password login boxes. Fill out the required information on the next page and a visitor account will be created for you to access the Wi-Fi network.

Personal equipment is allowed to connect ONLY to the KCCDopen Wi-Fi network for internet access. Personal equipment will not be allowed to connect to the KCCDSecure Wi-Fi network for work purposes and access to home directories, shared network drives / folders or other network resources will not be available.

It is also not authorized to connect personal equipment to the network via wired Ethernet connections. Any unauthorized equipment connections found will be promptly terminated and removed from the network. The use of personal equipment on the district network puts everyone at risk of viruses, hacking, and poor network performance.

When using the Wi-Fi 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 Wi-Fi log-in page.

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 aides, 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 POLICIES

Introduction:

In pursuit of its mission of instruction, research, and community service, 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) 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.

4) If a user of the network is believed to be in violation of Federal or0 State law, or specific district prohibitions, a user revokes his right to privacy.

5) 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 Director of Information Technology.

6) The second violation of these policies will result in the initiation of disciplinary action. This action will be determined by the Vice President of Student Services, in accordance with the College/District policies and procedures regarding student discipline.

7) Excessive noise and/or a disturbance may result in the restriction of use and/or disciplinary action.

8) Information obtained from the 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.

9) 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.

10) No food or drink allowed in the computer commons.

11) Children are not allowed in the computer commons.

12) Turn cell phone off. After one warning, users will be removed for the day.

13) Computer use is intended for the support of course work conducted for particular class assignments.

14) Students using computers for non-class related activities will be asked to relinquish their workstations when students with class-related assignments are waiting.

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

3E3 Electronic Mail Policy *(Added August 3, 2000)*

See **Procedure 3E3** of the Board Policy Manual for the Electronic Mail Procedure and **Appendix 3E3** for References and Definitions Pertaining to Mail.

3E3A The Kern Community College District (KCCD) recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. There is, however, no absolute right to such privacy provided by law; information retained on, or transmitted via, an employer's computer systems is considered the property of the employer.

3E3B KCCD encourages the use of electronic mail and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic mail without the holder's consent. Subject to the requirements for authorization, notification, and other conditions specified in the accompanying Procedure, KCCD may deny access to its electronic mail services and may inspect, monitor, or disclose electronic mail (a) when required by and consistent with law; (b) when there is substantiated reason to believe that violations of law or of KCCD policies have taken place; (c) when there are compelling circumstances; or (d) under time-dependent, critical operational circumstances.

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)

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. *S*uch 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 coy 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 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

PROCEDURE 3E1F

COLLEGE COMPUTING AND NETWORK USE PROCEDURES

The Colleges of the Kern Community College District may develop, adopt, and implement written computing and network use procedures that are consistent with the District's Computing and Network Use Policy, including, but not limited to references to:

A. The District Computing and Network Use Policy including its ten (10) prohibitions.

B. The legal aspects of computing and network use procedures such as:

(1) The rights of users to freely examine issues.
(2) Sexual harassment and creating a hostile environment
(3) Freedom from intimidation, embarrassment, or fear
(4) Rules related to behavior

C. The development of priorities that emphasize computing and network use that is related to the mission of the College/District.

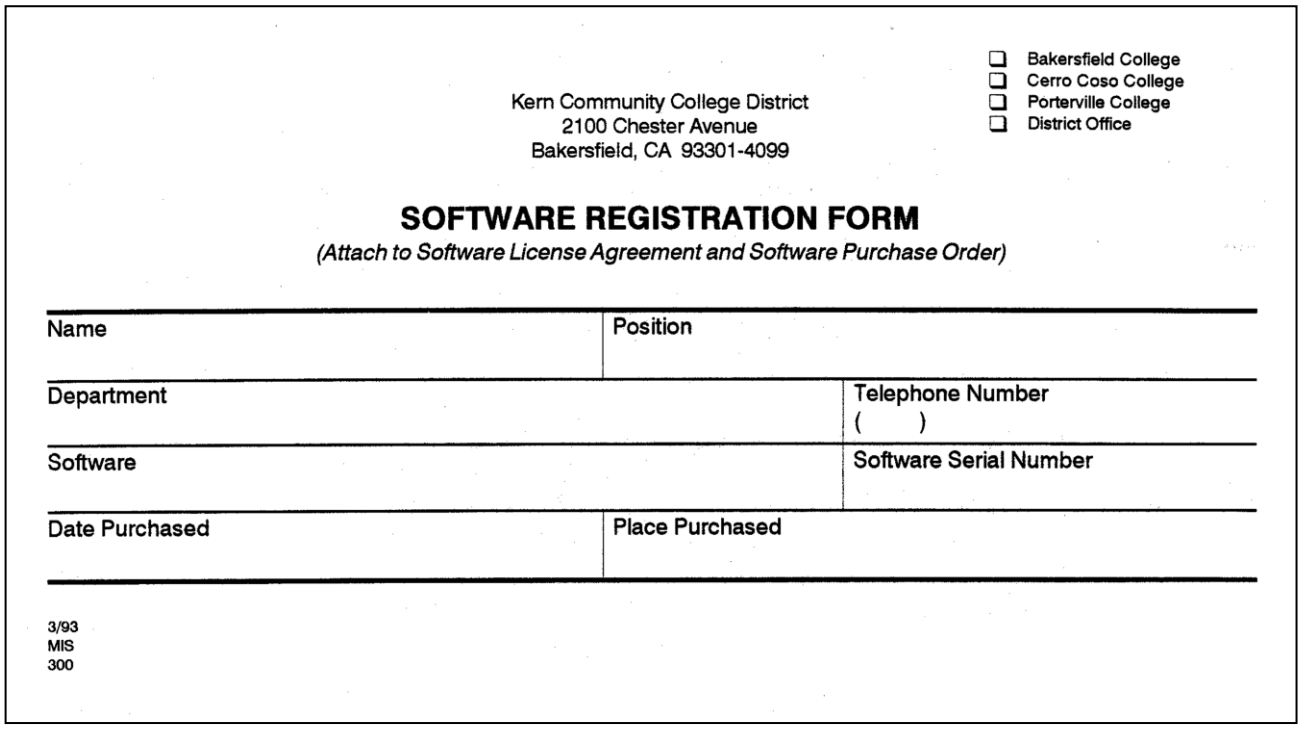
D. Sanctions that range from a warning, to restriction of use, to disciplinary action, to legal action.

E. College Computing and Network Use Procedures will have the approval of the President, will be given wide dissemination to users, and will be forwarded to the District Director, Information Technology.

Reviewed and Recommended by
Chancellor's Cabinet
September 16, 2008

Reviewed and Recommended by
District Consultation Council
May 18, 2009

APPENDIX 3E1C



❑ Bakersfield College
❑ Cerro Coso College
❑ Porterville College
❑ District Office

Kern Community College District
2100 Chester Avenue
Bakersfield, CA 93301-4099

SOFTWARE REGISTRATION FORM

(Attach to Software License Agreement and Software Purchase Order)

Name	Position
Department	Telephone Number ( )
Software	Software Serial Number
Date Purchased	Place Purchased

3/93
MIS
300

WEB PAGE GUIDELINES

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 log-in and password to the PC web site.

PC Web Site Coordinator:

The Porterville College Web Site Coordinator reviews all PC website content submissions and website links. The Coordinator monitors materials attached to the PC home page for compliance to Porterville College and Accessibility standards. Before content is submitted to the Web Site Coordinator, Division Chairs or the appropriate department head may review them and sign-off.

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

General Website Content Standards:

- Web pages must conform to Section 508 Accessibility Standards. (Please see Accessibility Guide Sheet)
- 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.
- 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 have not been 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 KCCD 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 KCCD 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:

Faculty and Staff may request websites housed on the home.portervillecollege.edu domain. 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.
- 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 have been developed to help identify the services available.

Duplication:

CD's and DVD's 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:

- Laptops, iPads and LCD projectors are available for checkout and can be ready for pickup at the LRC. Staff is encouraged to reserve early, as inventories are limited.
- All equipment requests must be made 48 hours in advance. After 3:00pm, neither staff nor equipment is available.
- 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 prior to your class.

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 since 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:

Audio cassettes can be transferred to CD and ½" VHS can be transferred to DVD. Video editing is available by appointment only. Appointments can be made with Media Services during regular business hours.