3E1 Computing and Network Use

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

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

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

e. Appropriate Information Technology Security policies, procedures, and guidelines

f. An Information Technology Security Awareness and Information Dissemination plan

g. 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.