

**LOS ANGELES COMMUNITY COLLEGES
OFFICE OF THE CHANCELLOR
ADMINISTRATIVE REGULATIONS**

INDEX NUMBER B-27

REFERENCE: B-28	TOPIC: Use of District and College Computing Facilities
ISSUE DATE: March 19, 1986	INITIATED BY: Educational Services
CHANGES: All sections; Regulation transferred to Business Services (formerly E-76); Sections I.(E) and III (A);	DATE OF CHANGES: April 1997; August 1, 2005

I. Policy

- A. The Los Angeles Community College District provides computers, networks and computerized records ("computing facilities"), for use by students, faculty, staff and administrators. These resources are intended to facilitate education, research, academic development and service to the public. Each individual user of these facilities ("user") is expected to exercise responsibility, use computing resources ethically and respect the rights and privacy of others.
- B. All employees and students using computing facilities are expected to operate within the bounds of federal and state law and of District policies and standards. All existing District rules, regulations and policies apply to the use of computing facilities, including those that apply generally to personal conduct.
- C. The College President or Division Vice Chancellor shall designate an administrator to be responsible for the implementation of this policy.
- D. Each college is responsible for communicating the provisions of this policy to its campus users of computing facilities. Each college may establish guidelines regarding who may use campus computing facilities, consistent with the provisions of this policy.
- E. This policy is intended to supplement Administrative Regulation B-28, the District's Network Security Policy, as appropriate.

II. Communications and Privacy

- A. Due to the nature of the technology and the public character of the District's business, there is no guarantee that a user's files, account and/or electronic mail are private. Documents created and/or stored on

District computers and networks may be considered public records, subject to disclosure under the Public Records Act or other laws or as a result of litigation. While the District does not routinely monitor computer files, e-mail or Internet use, the District reserves the right to examine material stored on or transmitted through its computing facilities as it deems necessary.

- B. Users are warned that they may encounter material which may be considered offensive or objectionable in nature or content. If a user alleges that a District rule or policy has been violated, he or she may initiate action through the applicable grievance or complaint procedure.

III. **User Responsibilities**

- A. Individual users assume full responsibility and accountability for using computing facilities in accordance with District rules and policies, which includes but is not limited to, compliance with the Policy Violations listed at section IV of this policy. Users must respect the rights of others, respect the integrity of the computing facilities and observe all laws, regulations and contractual obligations.
- B. As a condition of access to computing facilities, every computer user must observe the following guidelines:
 - 1. Maintain an environment conducive to learning and to working by using computing facilities according to the highest standards of professional and personal courtesy;
 - 2. Maintain a secure environment for the systems by immediately reporting any security loopholes or unauthorized use of the facilities;
 - 3. Assume responsibility for the protection of files by backing up data and programs; and
 - 4. Make economical and wise use of shared computer resources.
- C. Passwords provide employees and students access to computing facilities. The security of passwords is essential to the privacy of students and employees in accordance with State and Federal laws. In order to maintain a secure environment, the following rules should be observed:
 - 1. A unique user identification and password shall be issued to each individual who is provided with access to computing facilities.
 - 2. Users should not write their password in any location where another person can find it.

3. Passwords shall be modified periodically as required by the system administrator.
 4. In the event a user's identification and password are used for unauthorized purposes by someone other than the user, the user should immediately report the activity to the administrator in charge of implementing this policy.
 5. Employees and students shall participate in appropriate orientation and training prior to using computing facilities, when deemed necessary by the College President, Vice Chancellor or the administrator in charge of implementing this policy.
 6. Each individual user is completely responsible for all activity on computing facilities performed under his/her identification and password. This is especially critical for those who have access to any of the update systems. Accordingly, computing facilities should not be left unattended.
- D. Employees, which includes student workers, may be provided access to computing facilities as part of their assigned duties. Employee users must limit their use of computing facilities to activity within the scope of their employment and necessary to conduct District business.
1. Employee users are prohibited from using computing facilities for inappropriate purposes, which includes, but is not limited to, the following:
 - a. Employee users are prohibited from personally benefiting or allowing others to benefit from any inappropriate access to confidential information.
 - b. Employee users are prohibited from divulging the contents of any report or record to any person except in the execution of assigned duties and responsibilities.
 - c. Employee users may not knowingly include or cause to be included in any record or report a false, inaccurate or misleading entry. Employee users may not expunge or cause to be expunged a data entry from any record or report, except in the execution of assigned duties. Correctly, employee users are not responsible for the accuracy of the data assigned to them to be entered.

- d. No official record or report, or copy thereof, may be removed from the office where it is maintained except in the performance of assigned duties.
2. Computing facilities shall not be located in such locations that the display can be seen by unauthorized persons. These locations shall be reviewed periodically by the appropriate administrator.
3. Employee users should not give their personal password to any other person.
4. Employees who do not have a password but have a need for limited and specific use of computing facilities must be under direct supervision of a user who has a password.
5. Printouts of student records shall be provided in accordance with Federal, State and District privacy rules and regulations.
 - a. No printout shall be given to a student who does not have proper identification.
 - b. "Unofficial" shall be stamped on all computer screen printouts, including study list and permanent record printouts, issued by offices other than Admissions and Records.
6. Printouts of employee records may only be made by users who have been authorized to use the screens in question, and in accordance with Federal, State and District privacy rules and regulations.
7. In order to maintain the privacy of employees and students, the following rules apply with respect to the release of and/or access to student and/or employee records:
 - a. The release of and/or access to confidential information shall be made in accordance with Federal, State and District privacy rules and regulations.
 - b. Any release of and/or access to computerized records to third parties, in response to an employee's or student's written consent; a lawfully issued subpoena; or a court order, shall be made only by the office directly responsible for such records, under authority of the administrator-in-charge of that office.
8. Upon termination or transfer of an employee, the College President, Division Vice Chancellor or the

administrator assigned to implement this policy shall ensure that access to computing facilities by the employee is terminated or modified, as appropriate.

- E. Students may be provided an account for computer access from the college's designated system administrator and their use shall be limited to college-related activities only.

IV. **Policy Violations**

Conduct which is considered to violate District policy with respect to computing facilities includes, but is not limited to, the following:

1. Sending harassing, intimidating and/or threatening messages through electronic mail or other means;
2. Downloading, storing or displaying obscene or pornographic material;
3. Using computing facilities in a manner that violates copyrights, patent protections or license agreements, including using pirated or unlicensed software;
4. Knowingly performing an act which will interfere with the normal operation of computing facilities, cause damage or place excessive load on the system;
5. Attempting to circumvent data protection schemes, uncover security loopholes or gain unauthorized access to any information or files;
6. Intentionally entering, recording or causing to be recorded any false, inaccurate or misleading information into the systems;
7. Sending mass advertisements or solicitations; or political mass mailings as defined by the Fair Political Practices Commission;
8. Using computing facilities for commercial or personal financial gain;
9. Taking computer hardware or software from District or college facilities for any purpose without prior written approval; and
10. Using computing facilities in a manner that violates existing state and federal laws or District rules and regulations.

V. **Consequences of Misuse**

- A. Misuse of computing facilities may result in the loss of computing privileges. Additionally, misuse may require financial restitution to the District for funds expended and could result in disciplinary, civil or criminal action.
- B. Users may be held accountable for their conduct under any applicable District policy, procedure or collective

bargaining agreement. Violations of these policies will be enforced in the same manner as other District policies. Disciplinary review includes the full range of sanctions, up to and including, but not limited to, employee dismissal, student expulsion and/or legal action. Misuse can also be prosecuted as a criminal offense under applicable statutes, such as Penal Code section 502 which identifies certain crimes associated with the use of computer systems.

VI. **Guidelines for Electronic Civility**

- A. While the District encourages the free exchange and debate of ideas, it is expected that this exchange will reflect the high ethical standards of the academic community. When sending or responding to a sensitive or controversial topic, the user should keep in mind that e-mail is permanent and public. Once a message is sent, it may be saved, printed or forwarded without the knowledge or consent of the author. The user should take the time to consider the impact of all e-mail messages which he or she sends.
- B. Electronic mail does not convey "body language," facial expressions or tone so attempts at humor, irony or sarcasm may be easily misinterpreted. Therefore, careful writing is advised. Electronic messages should be brief, clear and professional.

VII. **Applicable Laws and Regulations**

- A. The following list identifies some, but not all, of the additional District rules and regulations that apply to the use of computing facilities:
 - 1. Board Rule 9803.26 - Theft or Abuse of Computer Resources
 - 2. Board Rules 1202, 1203 - Nondiscrimination Policy and Complaint Procedures
 - 3. Board Rules, Chapter XV - Sexual Harassment Policy
 - 4. Board Rules, Chapter IX - Article VIII - Conduct on Campus
 - 5. Board Rules, Chapter IX, Article XI - Student Discipline
 - 6. Administrative Regulation E-55 - Student Grievance Procedure
- B. This policy supersedes and replaces Chancellor's Directive No. 67, *Guidelines on Use of the LACCD Computer Network*.

**LOS ANGELES COMMUNITY COLLEGES
OFFICE OF THE CHANCELLOR
ADMINISTRATIVE REGULATIONS**

INDEX NUMBER B-28

REFERENCE: B-27	TOPIC: Network Security Policy
ISSUE DATE: July 17, 2005	INITIATED BY:
CHANGES:	DATE OF CHANGES:

Scope

The scope of this document is to define Los Angeles Community College District (LACCD) policies regarding network security. This policy covers the employees, students, the vendors, and the consultants of the Los Angeles Community College District. It exists in order to protect the district network, both WAN's and LAN's and to thereby improve productivity and to increase workflow, communication, efficiency. This policy is intended to supplement the District's Computer Use Policy, Administrative Regulation B-27 (formerly E-76) and is not meant to replace that document. The components of the network are considered to be:

- All cabling used for carrying voice and electronic information (data).
- All devices used for controlling the flow of voice and electronic information including (but not limited to) firewalls, routers, CSU/DSU's, switches, hubs, concentrators, PBX's, KSU's, punch down blocks, and patch panels.
- All computer components including (but not limited to) monitors, cases, storage devices, modems, network cards, memory chips, keyboards, mice, scanners, cameras, and cables.
- All computer software.
- All input/output devices including printers and fax machines.

Personnel

The LACCD personnel that are responsible for the daily operations of the LACCD LAN and WAN and network operations include, but are not limited to, the following local campus and District Office Information Technology technicians and managers: Chief Information Officer, Software Systems Manager, Dean of Information Technology, College Information Systems Manager, Senior Computer and Network Support Specialist, Computer and Network Support Specialist, Assistant Computer and Network Support Specialist, Software Systems Engineer, and Data Communications Specialist.

The personnel generally responsible for WAN operations including monitoring, maintenance, installation & configuration, and access to WAN hardware and software, are the Data Communications Specialists. Cabling or wiring "to the plug" will, whenever possible, being accomplished by the appropriate crafts or Unit responsible for that activity according to District agreements.

The LACCD personnel as described above are collectively referred to as the Authorized Technical Staff (ATS) within this document.

Purpose

The purpose of the Network Security Policy (NSP) is to promote management practices that will ensure the security and reliability, confidentiality, integrity, and availability of organizational information resources. To achieve this goal, the District must reflect the highest standards of ethical conduct and technical competence. Therefore the NSP will establish policies which will move the District forward to secure the continuation of use of the LACCD WAN/LAN system. Unless computer Users implement proper security procedures, computer viruses such as Code Red and the "I Love You" virus and others, as well as denial-of-service attacks, Trojan horse programs, and other malicious activities can take advantage of computer vulnerabilities and result in substantial damage to the District networks. This policy will help to develop procedures and guidelines to protect our systems from becoming victims of attacks from outside and allowing poor internal security to create weaknesses from within to corrupt the system.

Generally, this document was compiled to promote good information security concepts and practices by the following:

- Creating controls and defining good technical practices to support a dependable Information Technology Network within the District.
- Working in conjunction with and reinforcing the District's B-27 (formerly E-76) Computer Usage Policy.
- Maintaining the confidentiality of all proprietary or otherwise sensitive information encountered in the course of professional activities.
- Discharging professional responsibilities with diligence and honesty.
- Refraining from any activities that might constitute a conflict of interest or otherwise damage the reputation of the LACCD.

Network Management

Network Management is the responsibility of the local Information Technology staff or Authorized Technical Staff (ATS) assigned the responsibility for a specific network. All network maintenance, including configuration changes to desktop systems, is to be made solely by the ATS. Contractors are not allowed to make system modifications, even to the workstations issued to them by the District. Any of the following activities are considered a modification to the system (but not limited to):

- Patching a system's network drop to a new location.
- Using a system's devices to boot-up using an alternate operating system.
- Removing a system's case or cover.
- Installing any software package, including downloaded from the Internet.

Hardware management is restricted in order to insure that warranties are not inadvertently voided and that security precautions are not circumvented. Software installation is restricted in order to insure that the District remain in compliance with software licensing laws. This requirement also insures that proper support for software can be provided by the ATS and that software incompatibilities are avoided. Major changes in network infrastructure must be communicated to the District Office Data Communications Specialist to insure that connectivity, compatibility and security are maintained within the District network LAN/WAN.

Network Information

Certain network information is available to the ATS only. Access to this information is restricted, and is protected by User ID and password. All requests for specific network information are to be made in writing to an ATS member who will then forward the request with a recommendation to the college administrator or Network Security Officer for evaluation. This information may include (but not limited to)

- Router and Firewall configurations.
- IP addresses.
- Network performance information.
- TP screen information.
- User ID and password for specific network devices.

In all cases the Chief Information Officer (CIO) and/or the college president, or designee, will be notified of requests for network information that may compromise the security of the network. All information about the LACCD network is to be treated with the utmost confidentiality.

Network Separation

The Administration LAN and the Academic LAN are kept separate by using separate switch or router ports, VLANs, separate IP address range, or a combination of these. As technology changes and security can be maintained without this separation the District Technology Committee will make recommendations to the CIO as to the applicability of these new applications.

Virus Prevention Policy

All computer resources are to be protected by anti-virus software. No one using the LACCD network shall disable, circumvent or defeat any District installed virus protection software. If the employee receives any type of warning from the anti-virus software running on the system, he or she is to immediately cease using the system and contact an ATS.

It is the responsibility of the LACCD network staff to keep all anti-virus software up to date. Employees who suspect that their anti-virus software has not been updated in the last 60 days should contact a member of the ATS department.

Remote Network Access

The LACCD allows for Internet-based VPN access to network resources. This is the only sanctioned method of remote network access. Connecting an unauthorized modem and a telephone line to any part of the network (including desktop workstations) is strictly prohibited and is considered a serious breach of network security.

Remote network access is provided on an as-needed basis. Any employee or vendor who requires remote access to network resources must have his or her direct supervisor submit a request form to the college administrator for approval. The employee/vendor will then be issued the following:

- A security token for access network resources.
- Required software for creating an encrypted VPN session over the Internet.
- Directions for installing the VPN software.
- Directions for accessing the network remotely.

The District does not accept responsibility for supporting the system which the employee or vendor plans to use for remote access. The employee or vendor agrees that by accepting the software, he or she is responsible for any and all upgrades required to support remote access. This includes (but is not limited to)

- A telephone line.
- A modem or network interface card.
- A faster processor.
- Additional disk drive space.
- An Internet account with an Internet Service Provider.
- A firewall or firewall software on the employee's or vendors remote system.

In addition, support for remote access will be provided by the ATS only for the internal network up to and including the network perimeter. The employee or vendor is responsible for providing his or her own support for connectivity problems outside of this scope. The employee or vendor agrees to keep all information regarding remote network access confidential. The employee or vendor will not disclose password information or make copies of the VPN software; even for other employees or members of the vendor staff. Propagating remote access details is considered a security breach that cause substantial damage to the District WAN/LAN system.

General Internet Access Policy

LACCD network resources, including those used to gain access to Internet-based sites, are only to be used for the express purpose of performing administrative or academic work-related duties. This policy is to insure the effective use of networking resources and shall apply equally to all employees. Direct supervisors may approve the use of network resources beyond the scope of this limited access policy when said use meets the following conditions:

The intended use of network resource(s):

- is incidental.
- does not interfere with the employee's regular duties.
- serves a legitimate company interest.
- is for educational purposes and within the scope of the employee's job function.
- does not break any local, state, or federal laws.
- will not compromise network integrity.

When accessing Internet-based Web sites on or off campus, while at work, employees are to use a Web browser that meets the LACCD standard. This standard requires the use of the following configuration:

- No unauthorized plug-ins or applets.

These settings are to insure that the employee does not inadvertently load a malicious application while browsing Internet Web sites. Failure to comply with these security settings can result in the loss of Internet privileges. Web browser software should only be installed by an ATS. In order to maintain proper software licensing employees are prohibited from retrieving browser software or upgrades from any other source. Anyone who needs clarification on the approved browsers should contact the ATS at their location.

Privacy and Login

All District network resources and information, stored or printed whether fixed or portable, are owned solely by the LACCD. This includes (but not limited to) e-mail messages, encrypted files, stored files, and network transmissions. The LACCD reserves the right to monitor and/or log all network-based activity. The employee is responsible for surrendering all passwords, files, and/or other required resources, if requested to do so, in the presence to direct supervisor or member of the senior staff at their location.

Encryption

In all cases, employees or any LACCD LAN User may not use any unauthorized encryption mechanism to encrypt any files including, but not limited to, E-mail messages. Only LACCD approved encryption methods may be used. Any and all key information used to encrypt and decrypt files is to be kept by the ATS.

Additional Information

All queries regarding information within this document, as well as issues that have not been specifically covered should be directed to the employee's immediate supervisor. The immediate supervisor is responsible for relaying all queries to the administrator who has responsibility for the local systems.

GLOSSORY of TERMS

ATS- Authorized Technical Staff, usually a local LACCD college technician but can be any LACCD technical staff person who is a member of Information Technology at a college or at the District Office.

Campus - any one of the 10 locations of the Los Angeles Community College District including, City College, the District Office, East L.A. College, Harbor College, Mission College, Pierce College, Southwest College, Trade Tech College, Valley College, West L.A. College, and various satellite locations.

Communications - **1.** Information transfer, among Users or processes, according to agreed conventions. **2.** The branch of technology concerned with the representation, transfer, interpretation, and processing of data among persons, places, and machines. *Note:* The meaning assigned to the data must be preserved during these operations.

Communications network: An organization of stations capable of intercommunications, but not necessarily on the same channel

Computer network: **1.** A network of data processing nodes that are interconnected for the purpose of data communication. **2.** A communications network in which the end instruments are computers

Computer security (COMPUSEC) - **1.** Measures and controls that ensure confidentiality, integrity, and availability of information-system (IS) assets including hardware, software, firmware, and information being processed, stored, and communicated. *Synonym* **automated information systems security.** **2.** The application of hardware, firmware and software security features to a computer system in order to protect against, or prevent, the unauthorized disclosure, manipulation, deletion of information or denial of service. **3.** The protection resulting from all measures to deny unauthorized access and exploitation of friendly, or related, computer systems.

Computer system - A functional unit, consisting of one or more computers and associated software, that (a) uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program, (b) executes User-written or User-designated programs, and (c) performs User-designated data manipulation, including arithmetic and logic operations. *Note:* A computer system may be a stand-alone system or may consist of several interconnected systems.

Concentrator - An electrical hardware device that is the network interface point for many workstations. Rarely used terminology for a modern hub type device.

CSU/DSU - Hardware for connecting a LAN interface device to a WAN telephone line for digital service.

Data - Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as digital information, characters or analog quantities to which meaning is or might be assigned.

Data communication: The transfer of information between functional units by means of data transmission according to a protocol. *Note:* Data are transferred from one or more sources to one or more sinks over one or more data links.

Data processing -The systematic performance of operations upon data such as handling, merging, sorting, and computing. *Note:* The semantic content of the original data should not be changed. The semantic content of the processed data may be changed. *Synonym information processing.*

District - All legal entities in the Los Angeles Community College District.

District Office - The headquarters for the **LACCD** located at 770 Wilshire Blvd, Los Angeles.

Firewall - a device that keeps separate networks from each other. This device can inspect and filter unwanted packets from gaining entrance to a secure LAN by using specific addresses and ports.

Hub - this is a simple device for connecting multiple computers located in the same physical area to a network.

Information: **1.** Facts, data, or instructions in any medium or form. [JP 1-02] **2.** The meaning that a human assigns to data by means of the known conventions used in their representation.

Interconnection - **1.** The linking together of interoperable systems. [JP 1-02] **2.** The linkage used to join two or more communications units, such as systems, networks, links, nodes, equipment, circuits, and devices.

KSU - Key Service Unit, this is an electrical device that multiple telephone lines connect to be programmed to appear on multiple telephone sets.

Linkage - In computer security, the purposeful combining of data or information from one data processing system with data or information from another system to derive protected information.

Medium - **1.** In telecommunications, the transmission path along which a signal propagates, such as a wire pair, coaxial cable, waveguide, optical fiber, or radio path. **2.** The material on which data are or may be recorded, such as plain paper, paper tapes, punched cards, magnetic tapes, magnetic disks, or optical disks.

Network - **1.** An interconnection of three or more communicating entities. **2.** An interconnection of usually passive electronic components that performs a specific function (which is usually limited in scope), e.g., to simulate a transmission line or to perform a mathematical function such as integration or differentiation. *Note:* A network may be part of a larger circuit.
computer network: **1.** A network of data processing nodes that are interconnected for the purpose of data communication. **2.** A communications network in which the end instruments are computers.

Patch panel- an intermediate connecting device between in-house cabling from a workstation to a hub or concentrator.

PBX- Private Branch eXchange refers to voice communications where a specialized computer, the PBX, is the connecting point for all telephone circuits at a given location. The PBX is a smart device that is able to provide signaling and routing for many voice circuits. Also provides the signaling for special features on multi-line telephone sets.

Punch-down block- this refers to the actual termination point for voice circuits in a telephone closet. The way to make a connection is to use a punch tool that will take a telephone wire and punch it down to the block on one side for connecting telephones or circuits to a PBX or KSU device on the other side of the block.

Protocol - **1.** A formal set of conventions governing the format and control of interaction among communicating functional units. *Note:* Protocols may govern portions of a network, types of service, or administrative procedures. For example, a data link protocol is the specification of methods whereby data communications over a data link are performed in terms of the particular transmission mode, control procedures, and recovery procedures. **2.** In layered communications system architecture, a formal set of procedures that are adopted to facilitate functional interoperation within the layered hierarchy.

LACCD - Los Angeles Community College District

LAN - Local Area Network. Electronic network composed of computers and peripheral equipment at the local level. Each LACCD location has a LAN.

Router- a smart multi-port network device that routes LAN packet traffic through a network or multiple networks.

Security token- A battery operated computerized device that displays a random sequence of numbers every 30 seconds that works in conjunction with previously installed software on a system or server that generate the same random number as the token. When a User uses their password and the number displayed on the token at the precise time of login, the system being logged onto will recognize the User ID and password as valid and with the random token number, allow the User to gain access to a remote system, server or LAN.

Switch- a highly complex network device that transports packets between switch ports and various switch networks at high speed.

System - **1.** Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. [JP 1-02] **2.** A combination of two or more interrelated equipment (sets) arranged in a functional package to perform an operational function or to satisfy a requirement. [JP 1-02] **3.** A collection of personnel, equipment, and methods organized to accomplish a set of specific functions.

Transmission - **1.** The dispatching, for reception elsewhere, of a signal, message, or other form of information. **2.** The propagation of a signal, message, or other form of information by any means, such as by telegraph, telephone, radio, television, or facsimile via any medium, such as wire, coaxial cable, microwave, optical fiber, or radio frequency. **3.** In communications systems, a series of data units, such as blocks, messages, or frames. **4.** The transfer of electrical power from one location to another via conductors.

User(s) - Any person, organization, process, device, program, protocol, or system which uses a service provided by others. In this instance the service, comprised of computer services, computer network or any computer system or network owned by LACCD, is that provided by the Los Angeles Community College district or any of its colleges, organizations or entities.

VLAN - Virtual Local Area Network, similar to a local area network with the exception that a switch and router or a single layer 3 switch separates multiple LAN networks logically within the hardware.

VPN- Virtual Private Network. A private network built on a public network. Terminal on the private network use encryption to send data to other private terminals.

WAN - Wide Area Network, Electronic network composed of remote LANs within a large geographic area. The LACCD WAN is composed of all the remote LANs at each campus and satellite locations.

Further definitions are contained in the American National Standard (<http://www.atis.org/tg2k/t1g2k.html>), created by the Standards Committee T1 Telecommunications