

**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 Jan 19, 2016

CONFIDENTIAL: This correspondence is protected by the attorney-client privilege and is not to be shared with other persons

**Inter-Office Correspondence
LOS ANGELES COMMUNITY COLLEGES**

December 8, 2014

TO: Dr. Francisco Rodriguez
Chancellor

FROM: Anne L. Diga 
Associate General Counsel

SUBJECT: Adoption of Procurement, Asset Management and Information Technology Policies and Procedures into Chancellor's Administrative Regulations

The following policies and procedures were created, consulted and are now being requested for formal adoption as policies and procedures under their corresponding Administrative Regulations:

- Attachment 1 Procurement Policies and Procedures appended to Administrative Regulation B-19**
- Attachment 2 Asset Management Policies and Procedures appended to B-10**
- Attachment 3 Information Technology Policies and Procedures appended to B-27**

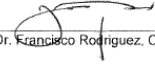
Since Administrative Regulations are adopted and revised under the authority of the Chancellor, we request that you approve the adoption of the above-mentioned policies and procedures to the corresponding Administrative Regulation attached hereto as Attachment 1, 2 and 3.

While the Procurement Policies and Procedures have been in use since August of 2008 and the Asset Management Policies and Procedures have been in use since April of 2009, we have determined that it would be better to document their adoption as administrative regulations.

The Information Technology Policies and Procedures were recently created, consulted and are awaiting formal adoption by the Chancellor. Information Technology Policies and Procedures have been approved by the Chief Information Officer after appropriate consultation, the Asset Management Procedures were approved by the CFO/Treasurer and the Procurement Policies and Procedures were presented to the Cabinet.

If you have any questions related to this matter, please contact me at extension 2188.

I hereby authorize the Office of General Counsel to append the above-mentioned policies and procedures to the corresponding Administrative Regulations.



Dr. Francisco Rodriguez, Chancellor

Attachment(s)
ALD

Cc: Jeanette Gordon, Chief Financial Officer/Treasurer
Jorge Mata, Chief Information Officer
Leila Menzies, Acting Contracts Manager

TABLE OF CONTENTS
INFORMATION TECHNOLOGY POLICIES AND PROCEDURES

B-27	Use of District and College Computing Facilities
07-00	Overview and Policy
07-01	Information Technology Responsibilities and Organization
07-02	Data Ownership and Acquisition
07-03	Data Security Protection
07-04	Data Use and Access
	-User Accounts
07-05	Email Retention
07-06	Electronic Discovery
07-07	Use of Computing Facilities and Equipment and Forms

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*.

ITP 07-00 OVERVIEW AND POLICY

I. OVERVIEW

This chapter addresses the requirements and procedures necessary to accomplish sound data resource management throughout the Los Angeles Community College District (“LACCD”) involving computerized and information technology resources and tools in effectively supporting LACCD’s mission, objectives and operations.

“Data Management” is the development, execution, and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data information.

II. OBJECTIVES

The LACCD’s data management process should adhere to the following objectives:

1. Comply with laws, regulations, rules and policies governing data management among public/government entities, community college districts in California and conform to board rules and administrative regulations within the LACCD.
2. Adopt best information technology business practices to the management of data throughout the LACCD.
3. Employ appropriate safeguards and security in protecting confidential data information during data acquisition, retention, transfer and destruction while ensuring that data is accessible and available to transact the necessary operations of LACCD.
4. Maintain the integrity of data by prudently and effectively managing the resources and tools employed to house the data.
5. Educate information technology staff and users in the legal requirements, procedures and appropriate business practices of data management.
6. Establish policies and procedures that ensure business continuity and successful disaster recovery.

III. POLICY

The LACCD is committed to providing excellent support and services in the data management of its electronic information resources and tools. As a result, the Education Services Center Information Technology Division and the College Information Systems Office shall work together to establish and enforce procedures, guidelines and mechanisms to ensure that the integrity of its data systems are maintained while providing

the ability for the LACCD to function in its daily business operations. All information technology management practices shall be implemented in a manner that upholds the basic principles of security, confidentiality, and appropriate accessibility.

Compliance with data management procedures and guidelines shall be the responsibility of all data information system users and shall be administered through the information technology management at the direction and support of LACCD and College administration.

IV. DEFINITIONS

Whenever the following terms appear in these policies and procedures, the definitions will have the corresponding meanings.

“Business Continuity” – An organizational effort that helps reduce risk associated with lax informational management controls (security and risk management) that interrupts critical business functions.

“Data” shall mean electronically stored information.

“Database Administrator” - A person who is responsible for the environmental aspects of a database system. In general, these include:

- Recoverability - Creating and testing backups
- Integrity - Verifying or helping to verify data integrity
- Security - Defining and/or implementing access controls to the data
- Availability - Ensuring maximum uptime of the system
- Performance - Ensuring maximum performance
- Development and testing support - Helping programmers and engineers to efficiently utilize the database.

“Data Confidentiality” – The process of ensuring that data information is accessible only to those authorized to have access.

“Data Security” – The means of ensuring that data is kept safe from corruption or unauthorized disclosure where access to data is suitably controlled. Data security supports the goal of keeping confidential or personal data from unauthorized and/or unlawful disclosure.

“Data Cleansing” – The act of removing data no longer required for use from any hard drive or database component.

“Disaster Recovery” - The process, policies and procedures of restoring critical business operations of the LACCD including regaining access to data (records, hardware, software, etc.) and communications, workspace, and other business processes after a natural or human made disaster.

“District” – refers to the Los Angeles Community College District (LACCD) and may be collectively and interchangeably used to refer to the Education Services Center and all nine (9) community colleges.

“Records Management” - The practice of identifying, classifying, archiving, preserving, retrieving and destroying records. District records management policies and procedures shall be more specifically addressed in another business policy and procedure section related to records. It is acknowledged that data records although in electronic format are considered records which should also adhere to District records management requirements.

“System User” – Any individual that utilizes technology tools and services offered by the District including, data and telecommunications.

“Technology Systems” For purposes of these procedures, this term refers to data, audiovisual and telecommunications provided and supported by the District through local information technology offices.

V. LEGAL AUTHORITY, CITATIONS AND OTHER REFERENCES

LACCD Administrative Regulations B-27 and B-28

ITP 07-01 INFORMATION TECHNOLOGY RESPONSIBILITIES AND ORGANIZATION

VI. OVERVIEW

Generally, two different functional areas are responsible for handling the information technology management and support for the District: (1) Education Services Center - Office of Information Technology and (2) College Information Systems Office. Information technology and support responsibilities are divided among these areas based on location, breadth and degree of information management issues.

- A. College Information Systems Office - Each of the nine colleges maintains its own local college information systems office. In most cases, the Manager of Information Systems or information technology administrator at each college reports to the Vice President of Administrative Services.
- B. Office of Information Technology – The Office of Information Technology under the direction of the Chief Information Officer (“CIO”) is located at the Education Services Center. The Office is divided into four specialized technology support and services units: Computer and Network_Operations, Systems/Systems Engineering, Applications, and Enterprise Resource Planning (“ERP”) Systems.

VII. RESPONSIBILITIES

- A. Office of Information Technology - the Office of Information Technology operates under the direction of the CIO. The CIO plans, organizes, coordinates, evaluates and directs all operations of the Office of Information Technology at the Education Services Center consisting of four (4) main technology support areas. Each area is supervised by a specialized manager in that specific area as identified below. In addition, the CIO develops district long and short range plans for systems development, systems maintenance, production activities and support services. Such plans for development of district-wide information technology resources and tools shall be a highly coordinated effort with the College Managers of Information Systems.
 - 1. Computer and Network Operations –Plans, organizes and provides local area network (LAN), telephone, and videoconferencing operations to the

District Office. Plans and coordinates the telecommunications support at the Education Services Center. Works cooperatively with the college information systems offices to develop technical standards and procedures for district-wide use, as well as the standardization and the development of specifications for the acquisition of computers, servers and network equipment. A manager in this area may act as Chief Information Officer in his/her absence.

2. Systems Engineering – Plans, designs, operates, and secures the network systems.
3. Data Services and Applications (except web based ERP) – Maintains master and daily schedules for computer, terminal, and ancillary data processing equipment and resolves job processing problems. Participates in the formation procedures for the control and processing of productions applications, especially the student information system.
4. Enterprise Resource Planning Systems (“ERP”) – Oversees the planning, design, coordination, configuration, testing, training, implementation, system security, user and maintenance support of all ERP system modules which includes the human resources and payroll, financials and procurement systems, including but not limited system applications, self-service portals and on-line features such as data reports, conflict of interest filing, electronic work request, and budget transfer.

B. College Information Systems Office – The College Information Systems Office operates under the direction of the Manager of College Information Systems (“MCIS”) or local technology administrator, and may be at some colleges a director or dean position at the college. The information technology leadership position oversees all technology related matters related to capital construction and renovations; participates in strategic, operational and technology plan development; manages information technology resources, staff and projects at the College. MCIS or local technology administrator is also responsible for budgeting for all campus, staffing and resources; administers technology licensing; provides technical support for all information systems on campus; and represents the College on all technology matters. Moreover, MCIS also ensures that the campus

technology plan is in alignment with the District strategic plan, college objectives, education programming and available facilities.

1. The College Information Systems Office staff performs the following functions:

a. Network Administration

Administers telecommunications infrastructure supporting the Fire/Life Safety Systems on campus, responsible for local network design and maintenance including all network infrastructure, applications, systems and services, traffic routing and network systems security and infrastructure cabling;

b. Server/Client and Application Software and Administration

Responsible for server/client design, set up, testing, pilot, deployment training of users and maintenance, maintains computer hardware, provides email administration, manages software licensing, supports Education Services Center technology projects, supports academic and administrative web presence including helping academic, student services and administrative departments in achieving their goals and objectives.

c. Desktop Support.

Supports users in all information technology desktop hardware and software maintenance and in some cases supports projects initiated and led at the Education Services Center (ESC).

d. Media Services

Retains all audio/visual equipment and classroom instructional media, responds to all academic, student service and administrative department requests for audio visual support.

C. Information System Users – Keeps the privacy of their information systems passwords confidential. Maintains the confidentiality of data records involved in transacting business and adheres to the strict rules, policies and procedures for

use of the network and computing facilities. These requirements are further discussed in ITP 07-04 – Data Use and Access.

VIII. LEGAL AUTHORITY, CITATIONS AND OTHER REFERENCES

LACCD Administrative Regulations B-27 and B-28

ITP 07-04

ITP 07-02 DATA OWNERSHIP

I. OVERVIEW

The purpose of this procedure is to establish data ownership guidelines which secure and protect information transacted throughout the District's information systems. "District-owned data" is data that is contained on the district information systems and data that resides on a district owned or issued computing device.

Generally, district data should not be stored on personally owned computing devices or third party storage systems not maintained or supported by the District.

If it is necessary for a personally owned computing device to be used for District business purposes, the user of the personally owned computing device must first receive approval for use by the Vice President of Administrative Services at the College or the Deputy Chancellor if the need for use arises at the Education Services Center. Personal computing devices approved for district purposes must be inspected prior to use and the data managed and protected by the local information technology department. Further data security protections are articulated in "ITP 07-03 - Data Security" and specific requirements for issuance of district computing devices can be found on "ITP 07-07 – Use of Computing Facilities and Equipment."

In order to ensure that data is protected successfully in the District information systems, the roles and responsibilities of those who develop, secure and use the data must be well-defined in the Information Technology Procedures. District data cannot be sold, used or conveyed to other third parties without the required written consent of the Board of Trustees or its designee(s), unless legally required by law. Guidelines for release of data are governed by federal and state laws, board rules and administrative regulations governing the types of records released.

II. DEFINITIONS

a) "Data Owners" are those senior managers with the authority for acquiring, creating and maintaining data in an information system within their area of responsibility. Data owners are responsible for:

1. Authorizing release of information data records when appropriate and determining permissible uses of the data;
2. Verifying that data record contents remain correct and acceptable for input and use;
3. Insuring that their staff, identified as end users in the system, are adequately trained and informed in entering or modifying the data in the information system;
4. Assisting the information technology areas in planning efforts to protect data information confidentiality and sensitivity in their areas of responsibility; and
5. Serving as custodians of records for the data record content inputted in the information systems within their area of responsibility. An example of this would be that the Payroll Manager is deemed to be the “custodian of records” for Human Resource payroll records in the electronic payroll system.

“Custodian of Records” is an individual who is responsible for certifying to the validity, content and preparation of records in a legal proceeding or a legal affidavit. In most cases, the Data Owner and Custodian of Record will be the same individual if the record is in data format.

b) “Information System Custodians” are defined as those individuals in the Information Technology Division and College Information Systems Office that are responsible for:

1. Protecting the information in the data system from unauthorized access, alteration, destruction or usage;
2. Providing and administering internal data system controls such as routine back-up and recovery systems consistent with LACCD rules, administrative regulations, policies and procedures.
3. Establishing monitoring and operating information systems in a manner consistent with LACCD rules, administrative regulations, policies procedures; and
4. Verifying that the technological aspects of the information system are operating appropriately or as planned.

c) “System Users” are those individuals who have been granted appropriate access to the information systems to input, display and transact data records as part of their daily and routine job responsibilities. System users that input

data records in the information systems do not have any “reasonable expectation of privacy” in the data records they create in the LACCD information systems, except in data related to their own employee or student records in accordance with the law. Moreover, system users do not have any reasonable expectation of privacy in work related data records they create on their personal computing devices utilized for work purposes. More detail on this matter can be found in Information Technology Procedure 07-07 entitled “Use of Computing Devices and Facilities”.

- d) “Data” is electronically stored information.
- e) “Confidential data” is data which includes sensitive personal information of individual(s) or institutional information which are given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access to personal confidential information may result in significant invasion of privacy issues and financial exposure for the District. Examples of “Confidential Data” may be the data records protected by privacy laws such as Family Educational Rights and Privacy Act (FERPA) and Healthcare Information Portability Protection Act (HIPAA), medical and health insurance covered under the California Health and Safety Code; personally identifiable information resulting in exposure to identity theft; information to financial and banking records of the District, and legally protected attorney-client privileged information.

III. PROCEDURE

The LACCD shall establish access control solutions and capabilities which shall protect the data records in its information systems. As such, information technology administrators should meet regularly with district and college administration to plan efforts and implement district-wide controls and solutions. This planning shall include regular review of identification and authentication processes configured in the information systems, evaluation of the authorization policy granting access to data records for system users, ensuring that sensitive data information contains proper safeguards and audit functions. Such planning should emphasize short term operational needs as well as long term security objectives in maintaining the integrity of the District information systems.

Regular review of storage or destruction of data should be performed by the department head or designee in order to ensure proper data review and cleansing. Methods of effective retrieval of data documents stored should be a part of both short term and long term planning. Such planning and procedures should be in accordance with the records policies related to the type of record.

IV. LEGAL AUTHORITY, CITATIONS AND OTHER

REFERENCES

LACCD Administrative Regulation B-27, B-28, C-10, E-106 and E-111
LACCD Board Rules 7700-7709.11, 8400-8403

ITP 07-03 DATA SECURITY AND PROTECTION

I. OVERVIEW

The purpose of this policy and procedure is to establish roles and responsibilities within the District which support and maintain the necessary safeguards to protect data within district information systems and district owned and issued computing devices; provide guidance in implementing safeguards that will ensure that district data integrity is not compromised and breaches of the data information systems do not occur. In addition, such efforts to secure data within the district information systems must at all times meet the requirements of the law in handling confidential information and handling potential security breaches. All users within the district information systems shall adhere strictly to necessary data security and protection policies and procedures.

II. DEFINITIONS

- a) District: Refers to the Los Angeles Community College District (LACCD) and may be collectively and interchangeably used to refer to the Education Services Center and all nine (9) community colleges.
- b) Users: Person(s) that use the district information systems.
- c) Data: Any electronically stored information.
- d) Data Classification: The process of classifying data into categories to determine the level of security that should be afforded that data record. These categories

of classification can be identified as the following: (1) confidential, (2) internal use only, and (3) public.

- e) Confidential Data: Data which includes sensitive personal information of individuals(s) or institutional information which are given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access to personal confidential information may result in significant invasion of privacy issues and financial exposure for the District. Some examples of “Confidential Data” may be the following electronically stored records: information protected by privacy laws such as Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA), medical and health insurance information covered by the California Health and Safety Code; personally identifiable information resulting in exposure to identity theft; information related to financial and banking records of individuals and the District, and legally privileged information.
- f) Personal Information: According to California law, an individual’s first name or first initial and last name plus one or more of the following data elements: (1) Social Security Number (SSN); (2) driver’s license number or state issued identification card number; (3) account number, credit or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information contained with medical and health insurance records. Personal information does not include publicly available information that is lawfully required to be made available to the general public based on the California Public Records Act and any other federal, state or local laws.
- g) Data Security Breach: The unlawful and/or unauthorized acquisition of data including personal information that compromises the security, integrity and confidentiality of the data.

III. RESPONSIBILITIES

- a) Chief Information Officer: Plans, coordinates and manages data security for all district-wide information systems.
- b) Data or Network Security Administrator: While it is typical of organizations to have an individual dedicated to this position or role, it is a responsibility currently

shared by the Chief Information Officer and his/her System Program Manager, ERP Manager, and Network Operations Manager, as well as the Manager of College Information Systems or the local information technology administrator at each college.

- c) Information Systems Manager or Administrator: Plans, coordinates and manages the data security for each of their own local area network information systems. This role includes updating and maintaining all necessary security infrastructure requirements and advising on the acquisition of data security tools and products.

When a data security breach occurs, the Manager of College Information Systems or local technology administrator reports the breach and supports district leadership in identifying the cause and the necessary measures to secure the system from repeat occurrences of such an event.

- d) Data Custodians of Records: Data Custodians are defined as administrators or supervisors having functional responsibility over the electronic data record in the District information systems. Data Custodians shall at all times ensure that the necessary safeguards and practices needed protect data within their responsible departments are transacted in a manner which complies with the requirements of data protection laws and when feasible best practices for the handling of the category of data. Data custodians shall be knowledgeable of the relevant security requirements pertaining to the type of data within their custody and control.
- e) Users: All users have the responsibility for protecting the confidentiality and security of data. Users shall institute necessary safeguards to protect data in accordance with the law, including but not limited to notifying the local information technology administrator of any potential data security breach, including but not limited to breach as a result of loss of computing equipment or devices.
- f) Data providers or transmitters of data (not users): Data providers or transmitters of data in conducting district business shall be subject to stringent confidentiality provisions in services agreements or individual non-disclosure/confidentiality agreements and all relevant data privacy laws when handling district data for

legitimate business purposes. District employed project managers or supervisors overseeing such data providers or transmitters shall ensure strict adherence to the District policy and guidelines related to data security.

IV. PROCEDURES

- a) System Security – The Chief Information Officer and staff in conjunction with the Manager of College Information Systems or local technology administrator and staff shall implement security software updates, patches and any other system maintenance measures to district information systems in a manner which ensures on-going security of the system. When prudent and feasible to do so, encryption of confidential data records or information will occur in a manner that ensures the security of such confidential data or information transmitted within and outside of the district information systems.

Authentication and stringent control of user identification and passwords shall be maintained. This includes limited provisioning of administrative user rights outside of the local information technology department and careful review, prior to installation on any district system or computing device, of all third party software and applications not obtained through the normal course of district authorized procurement.

- b) Portable Computing Device Security – When necessary, the district information technology departments may employ kill switches, computer drive cleansing, wiping and other means of data destruction on district-owned or district-issued computing data equipment or devices when necessary to prevent possible data security breaches and prior to retirement or disposal of district owned or district-issued computing equipment in order to ensure district data does not fall in the hands of unauthorized third parties. All destruction of data records must follow the requisite disposal of records process if the data records are deemed to be the original record.

For users utilizing personally-owned computing devices and equipment to download district data or access the district intranet, global encryption should be implemented to protect data from being obtained by unauthorized users or prevent from inadvertent disclosure.

- c) Physical Security – In conjunction with local technology administrator, the Facilities Director or Director of Business Services (if at Education Services Center) ensure that data systems are housed in locked rooms and/or areas where limited access is provided to appropriate individuals. Whenever necessary and appropriate, employ monitoring or surveillance on and around data information systems to provide visibility of individuals accessing such systems.
- d) Privacy and confidentiality practices – District shall ensure that ongoing education and training of staff occurs with respect to records confidentiality, system security and all legal compliance requirements related to data security breaches.

V. SECURITY BREACH REPORTING REQUIREMENTS AND NOTIFICATIONS

- a) Breach Notification – Once a data security breach has occurred, the local information technology department shall immediately notify the College President, Vice President of Administrative Services, Deputy Chancellor (in the case where the breach occurs at Education Services Center), Chief Information Officer and General Counsel. After an initial assessment of the data security breach, further notice may extend to the Chief Business Officer, Chief Financial Officer, Vice Chancellor of Human Resources or Director of Business Services. Immediately within this time frame of notification of district administration, the necessary parties shall meet and discuss the measures necessary to secure the data information system, inform employees, students or other necessary parties of the security breach which may have compromised confidential data information as required by law and determine any necessary follow up measures taken in resolving this matter. When necessary, appropriate law enforcement may also be notified of the data security breach.

In initially assessing the breach, the Manager of College Information Systems or local technology administrator should gather information necessary to consider the following questions:

- When was the breach detected?
- How did the breach occur (if possible to ascertain)?

- Did the breach involve a device or system and what was there a security measure in place to protect the device or system?
- Did the breach involve confidential data or another type of data?
- How much data or what volume of records were inadvertently disclosed or taken?
- Was the breach localized to the college, involve multiple colleges or district-wide?
- What subsequent measures have been or will be put in place to re-secure the data?
- What other follow-up actions need to be taken?
 - Notices issued
 - Corrective actions

After the initial assessment is made at the local college technology department or information technology office shall brief the Vice President of Administrative Services or Deputy Chancellor (if a breach occurs at the Education Services Center) on the incident. If it is determined that a data security breach has occurred, an incident report will be provided by the Manager of College Information Systems or local technology administrator to the Office of General Counsel through their Vice President of Administrative Services or Deputy Chancellor.

- b) Additional Reporting requirements – As required by law, if the breach requires the District to notify more than 500 California residents as a result of a single breach, the District must submit a single sample copy of the notification letter to the Attorney General’s Office. If a breach occurs of medical information data as identified by law, the Department of Health Services must be notified no later than 5 business days after the unauthorized access, use or disclosure has been detected by the District.

VI. LEGAL AUTHORITY, CITATIONS AND OTHER REFERENCES

California Civil Code sections 1798-1798.78

California Health and Safety Code Sections 1204, 1250, 1725, and 1745

LACCD Board Rules 7708 and 7709

LACCD Administrative Regulations B-27 and B-28

Red Flags Rule

ITP 07-07 Use of Computing Facilities and Equipment

ITP 07-04 NETWORK AND DATA ACCESS

I. OVERVIEW

The purpose of this procedure is to establish acceptable guidelines for issuance of network access to employees and district contractors to perform district and college operations, conduct district business, and offer on-line information technology resources to students or guests while on campus or at a district facility. Such guidelines shall support appropriate user access to these functions but also afford protection of the District's information systems and data. In order to ensure that access to network systems and data is successfully protected, the issuance of network and/or data access in the district network systems must be well-defined, consistent and reasonably controlled. Use of the district information systems is a privilege. Access to sensitive data in the district information systems shall be provided to those users in direct need for such access.

II. DEFINITIONS

- a) Network access and data control (NAC): A traditional network access server (NAS) is a server that performs authentication and authorization functions for potential users by verifying logon information. In addition to these functions, NAC restricts the data that each particular user can access, as well as implementing anti-threat applications such as firewalls, anti-virus software and spy-ware detection programs. District has implemented NAC protocol which regulates and restricts the functions individual subscribers can do once they are connected.
- b) Users: Person(s) that use the district information systems.
- c) Role-based authorization(s): Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members or staff (or other system users) are assigned particular roles, and through those role assignments acquire the computer permissions to perform particular computer-system functions. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply

assigning appropriate roles to the user's account; this simplifies common operations, such as adding a user, or changing a user's department. Such role-based authorizations are utilized in the issuance of access to the District Enterprise Resource Planning (ERP) systems.

- d) Authentication: The process of identifying an individual usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication is designed to ensure the individual provides a form of identification representing who he or she claims to be, but says nothing about the access rights of the individual.
- e) District – Refers to the Los Angeles Community College District and may be collectively and interchangeably used to refer to the Education Services Center and all nine (9) community colleges.
- f) District Project Manager – For purposes of this procedure, an employee of the District who is assigned to oversee employees and/or outside contractors assigned to a specific project or program.
- g) District Sponsor - A district employee responsible for coordinating or hosting the event or individuals at the district facilities.
- h) Learning Management Systems– A classroom based software application used to facilitate learning and instruction such as “Moodle” or “E-tudes”.

III. PROCEDURE

a) **Users and Issuance/Disabling of User Access**

1. **Employees** – For purposes of this procedure, employees are defined as those persons hired by the District for the purposes of conducting its operations and business in exchange for receiving a salary or compensation and employee benefits. Employees include full-time, part-time, adjunct and temporary workers.

- a. Student Workers - While student workers are considered employees of the District, access to information systems and data within the district is very limited and is non-interactive with the district information systems, except when the student worker is updating his/her personal employment or student data in the information system.

Issuance of User Access: Once an individual is fully entered as an employee in the SAP ERP HR system, the system generates a new network user account for the employee. The user account and type of access granted to an employee is based upon an employee's assigned position or assignment with the District. Depending on the employee's position, there is a preset role based authorization attached which permits an employee access to the appropriate District information system(s), module or on-line function.

Password protected user accounts are issued to users employed by the District. Passwords and user accounts are unique and individual to employee users. Passwords and other sensitive user account information must never be shared with others.

Disabling User Access: Upon termination or separation of district employees, user accounts are disabled within 90 days, unless circumstances necessitate immediate disabling. Employee data on the district server is provided to the employee's immediate manager to determine storage and/or retention of data.

In the event that an employee is placed on administrative leave or terminated from the District, accounts may be disabled immediately at the request of the appropriate District administrator to prevent destruction of data records and protect the District information systems from misuse.

- a. Student Workers – user access shall be fixed to expire six (6) months from the date assignment is entered in SAP system or at the end of the term of the assignment whichever is the soonest.

- 2. **Students** – Students are defined as persons enrolled in classes in at least one of the nine (9) community colleges within the District.

Issuance of User Access: Upon enrollment of the student at a college, the student receives an automatically generated identification number and student email address. Student shall utilize their district-issued email as the official means of communication with the district. Once a student is issued an identification number and enrolled in a class for the active term through the student information system, the student is able to access learning management, instructional and library systems, as well as the wireless internet network.

Disabling User Access: A student user account is subject to being disabled upon request by the College President or Vice President of Student Services as a result of disciplinary measures.

On a routine basis, student user accounts on the college network systems are disabled at the end of each semester until the student enrolls and is admitted to a subsequent semester.

3. **District contractors** – District contractors are those persons who are employed by a third party vendor or service provider that has a written agreement with the District to provide services or perform work requested by the District.

Issuance of User Access: In order for a district contract to be issued temporary access to the district network the following process must be followed:

- a) District project manager will determine what user access is to be provided to a contractor and shall request such access from the local information technology department with the approval of the appropriate District administrator. Remote access provided to a contractor shall be separately determined and reviewed by the same parties.
- b) Prior to receiving user access, the contracted user shall sign a data confidentiality agreement which the original document shall be kept by the District project manager with a copy to the contract file.
- c) Prior to use within the district information systems, all district contractors shall surrender their computing devices for inspection to the local information technology department to prevent the introduction of viruses, spyware, and other unauthorized, malicious and destructive elements to district information systems.

- d) On a periodic routine basis, district project manager will review district contractor user accounts and determine the need for continued access and appropriateness of user assigned role.

Disabling of User Access: When a district contractor's assignment has ended, such contractor user account shall be disabled. Any data generated through a district contractor while assigned to a project or program shall be copied to a district server prior to disabling the account, the data shall be provided to the district project manager to determine storage retention or destruction. Contractor user accounts should be timed to disable six (6) months from issuance or at the end of the term of their contract whichever is soonest.

- 4. **Guests** – Guests are defined as visitors to a district facility that are not employee, student, or district contractor. Guests that have access to the district or college network typically obtain access on temporary single day use basis or extended daily use as a result of an event occurring on campus or at a district facility.

Issuance of User Access: A district sponsor may request guest access for an individual or group of individuals on campus. When feasible, guests may be asked to register prior to receiving access.

- a. Guest access permits access to the wireless internet only. Wireless internet access varies based upon whether the individual or group of individuals are granted guest use as (1) attendees to a district sponsored event, (2) invitees to a third party hosted event for which the party is appropriately renting college or Education Services Center facilities or (3) a random individual who is at a district facility unsponsored and not attending a hosted event on campus.
- b. Guest use under district sponsored and third party hosted events will be given general internet access. Guest use for random unsponsored or non-hosted individuals shall be given limited access to internet sites and reduced ability to download data content from the internet.

Disabling of User Access: Guest user access is temporary. Hosted guest user accounts and passwords are typically set to expire at the conclusion of

the hosted event. Unhosted guest user accounts and passwords will expire on a daily basis. Guest users may be denied access if the user has violated the District acceptable use policy set forth in Administrative Regulations B-27 and B-28 or engaged in any other unlawful use of the district internet.

b) Reporting Unauthorized Network or Data Access

1. **Employees.** Employees shall not share passwords with others. Misuse of password and user account information is a violation of Administrative Regulation B-27 and compromises the security of the district information systems.

Any misuse of such passwords or logon user account information should be reported to the Vice President of Administrative Services in writing. If such misuse represents a significant security breach to the network system or its data, the Vice President of Administrative Services shall alert the College President. If such misuse occurs at the Education Services Center, such activity shall be reported to the Deputy Chancellor.

Employees engaged in such unauthorized activity may be subject to discipline up to termination.

2. **Students**

Students shall not share passwords with others. Any student gaining unauthorized network or data access to district information systems should be reported to the Dean of Student Services. Any discipline issued to a student as a result of a student's unauthorized network or data access shall follow the procedures set forth in Student Discipline - Board Rule 91101 et.seq.

IV. LEGAL AUTHORITY, CITATIONS OR OTHER REFERENCES

LACCD Board Rule 91101 et.seq. – Student Discipline Procedures
LACCD Administrative Regulations B-27 and B-28

ITP 07-05 EMAIL RETENTION POLICY

IX. OVERVIEW

This section addresses the use of the email server system(s), including cloud computing systems, utilized by the Board of Trustees, administration, faculty and staff of the Los Angeles Community College District. The District recognizes that email communication has become a primary tool for correspondence and transacting of business throughout the organization. As a result, the District shall establish prudent policies and procedures which shall reflect compliance with state and federal regulations, as well as support proper usage and accountability by all email users of the system(s).

Email users do not have an inherent reasonable expectation of privacy in any email sent or received from their District email inboxes. Any email, including its electronic attachments, created, received, maintained or sent from a District email server constitutes an “electronic record” which may be subject to public inspection if requested and not otherwise exempted from disclosure under the California Public Records Act or other such legal authority.

Since emails are public records, users shall be responsible for adhering to the requirements of Board Rules 7700-7709.11 in the production and destruction of these records and any other relevant state or federal law. District email systems are not intended for personal use unrelated to district business and shall not serve as a location for long term data storage.

X. OBJECTIVES

A. The objectives of this policy are to ensure the following:

1. Comply with all laws, regulations, and rules governing public/government entities retention of electronic records.
2. Encourage the application of best practices in the efficient management of email system(s) throughout the LACCD.
3. Employ appropriate procedures, tools, safeguards and security in protecting confidential records transacted via email, retrieving email for appropriate business purposes and ensuring that proper destruction of records occur if an email is deemed to be in those classes of records identified by the board rules and Education Code requiring board approval prior to destruction.

4. Educate District email users in the legal requirements, responsibilities, procedures and appropriate business practices that should be exercised in daily email use, as well as preservation of such email records if required in an administrative/litigation proceeding or public records request.

III. DEFINITIONS

- A. Electronic mail record – For purposes of this policy and procedures, shall mean any record that is created, received, maintained or stored in the District/College email servers. Some examples of these records may include, but not be limited to, the following: electronic mail messages, word processing documents, spreadsheets, reports and any file attachments.
- B. Transitory email messages – shall mean email messages which contain transient information which have no long term or permanent business information value. Some examples of these email messages may include, but not be limited to the following: emails related to scheduling meetings or email announcements of events once passed are no longer useful, spam, advertisements or personal emails. These emails should be purged immediately by the email user after the meeting/event or receipt. If not purged by the email user, the email server shall routinely purge the message after the default retention period has passed. However, users are encouraged to regularly cleanse and delete from their email boxes these types of messages in order to encourage efficiency and maintain storage capacity in the email system.
- C. Lasting or long term value email messages - shall mean email messages which are designated in the areas set forth by Board Rule 7708, email constituting a project or program record which provides permanent informational value to the on-going project, matter or transaction, any other email messages deemed by the District/College administration to have permanent value. These messages should be retained by the email system server for at least through the default retention period and thereafter relocated by the email user to a retention folder on their desktop or an appropriate data storage location if required to be kept longer in accordance with Board Rule 7708.

- D. Default retention period – The default retention period shall mean the three (3) year period of time, beginning with the time an email is created, sent or received into the District email server(s) system, of which thereafter, the email server will automatically purge emails if the user has not moved the email to a data retention folder not on the email system.
- E. Ordinary retention period –The ordinary retention period shall mean the six (6) month period from the time the email record is created, sent or received in the District email server system. Email users are required to regularly review their email boxes to either delete or move email messages six (6) months or older into the retention file folder not on the email system.
- F. Authorized email users – shall mean those District board members administrators, faculty and staff and authorized consultants performing services for the District who have been issued an authorized email address and password by their local information technology department.

For those temporary employees or authorized consultants of the District, email accounts will be de-activated upon termination of assignment or services.
- G. District Records Policy – Board Rules 7700 through 7709.11.
- H. Custodian of email record - shall mean the creator of the email message if sent by a District email user; the District email user recipient of the email if message is sent by a non-District third party; or the District email user that forwards the email message to another email user for information purposes. The custodian retains the legal responsibility for the archiving and retention of the email records.
- I. Back up Retention Period: shall mean the minimum three (3) months up to three (3) **year** retention period the local information technology departments at the colleges or District Office shall keep any back up tape or file for the email system(s) in order to perform email system restoration activities.

IV. POLICY STATEMENT

- A. Responsible Use
 - 1. The use of the District email server system(s) shall be utilized for the transacting and communicating of legitimate District business in accordance

with Administrative Regulations B-27 and B-28, as well as any applicable state or federal law.

Absent any documented evidence to the contrary, email users shall generally be held responsible for all email messages sent from and maintained in their District-issued email in-boxes. Email users shall not share their email passwords with others.

Emails constitute electronic records. Depending on the information contained in the emails, users shall be responsible for maintaining these emails in compliance with the District Records Policy.

2. Emails that are transitory in value should be purged every six (6) months by the email user.

Emails with a permanent or long lasting value shall be held over for long term records retention up to the default retention period and thereafter must either be manually transferred by the email user to a retention folder or other district data storage location. Otherwise, the email shall be automatically purged from the District email server system. After the default retention period, the email system shall automatically purge any email not stored for long term retention.

3. This policy is intended to apply to the following:
 - a. All District email server system(s);
 - b. All users of the District's email server system(s);
 - c. All email messages sent or received on the District's email server systems;
 - d. All emails sent via district-owned and/or district-issued desktop workstations, laptops, cellular phones or other such mobile communication devices transmitted through the District email server; and
 - e. When District email accounts are accessed for use from outside of the workplace.

B. Back- Up Files

Regular back ups of the email servers are performed on a routinely scheduled basis by the local information technology departments for purposes of disaster recovery or system restoration only. Local back up files will be maintained for a minimum of three (3) months but no longer than the default retention period. Back ups shall be performed in accordance with the district-wide back up procedures. The local

information technology departments are not the legal custodian of any email records.

C. Retrieval of Email

Except for retrieval under provision (C) 4 herein, when email is retrieved for the purposes identified below, email users will be informed by the Office of General Counsel regarding the request for retrieval and advised of their duty to maintain email records. Email users should be aware that any such deletion after the notice is issued may subject the District to potential court sanctions, as well as discipline of the employee, up to and including termination, if intentional deletion of email records occurs after notice is given the email user.

The retrieval and review of such records will be performed by the Office of General Counsel in the manner identified below. Any emails that the Office of General Counsel determines as being exempt from public disclosure due to an employee or student right of privacy, attorney-client privilege, or other matters supporting legal exemption of the email will be withheld.

1. **Public Records Request** – When a records request is issued by a member of the public, the Office of General Counsel shall utilize the email archive to retrieve any relevant and legally disclosable email records responsive to the request.
2. **Litigation Hold** – When the Office of General Counsel is informed of any pending or threatened litigation, a litigation hold may be directed to the legal custodian of the email records. Litigation holds shall follow the process outlined in ITP 07-06.
3. **Matters involving audit or investigation** – If the Office of General Counsel in collaboration with Human Resources, Personnel Commission, Internal Audit Department or Bond Monitor determine that email records are required in a financial or performance audit, personnel investigation or other matters requiring review by these offices, the Office of General Counsel shall facilitate the retrieval and review of such email records for these purposes.
4. **Recovery needed for legitimate business purposes not involving audit or investigation** – Upon written approval from the College President, Chancellor, Deputy Chancellor or designee, temporary access may be granted by the local

information technology department to the email archival management system to an email user seeking to retrieve email for legitimate business purposes.

- D. Access to Email Archive – Although the email archive may contain data records that are considered public records, in order to safeguard the integrity of the records and to prevent from misuse, access to the email archive shall be granted to facilitate and support the matters listed above only.

“Ongoing and active” email archive access may be granted to the attorney(s) and paralegal(s) of the Office of General Counsel.

“Temporary Access” to the email archive may be approved by the Chancellor or his/her designee to the internal auditors or investigators handling the limited matters above. A College President or his/her designee may grant temporary access to the email archive if the request to review such email records is related to a legitimate business purpose need. User access profiles to the email archive shall be determined by the respective approver above when request is granted.

Termination of temporary access to the archive shall occur immediately after the matter is concluded or the need to review such email for business purposes is satisfied. Termination of ongoing and active access to the archive shall occur when the district employee no longer serves in their position as attorney, or paralegal for the District.

An audit of users accessing the email archive system shall occur upon request by the Chancellor or designee or on a yearly basis to ensure appropriate use of the email archive.

- E. Enforcement - Failure to comply with this policy and the rules and regulations cited in this section may result in disciplinary action, up to and including termination of employment, and any other penalties applicable by law.

V. LEGAL AUTHORITY, CITATIONS AND OTHER REFERENCES

Federal Rule of Civil Procedure

California Code of Civil Procedure

Title 5 C.C.R. Sections 59020 et seq.

LACCD Board Rules 7700-7709.11

LACCD Administrative Regulation B-27, B-28

Information Technology Procedure 07-06

ITP 07-06 ELECTRONIC DISCOVERY

I. OVERVIEW

In compliance with the Federal Rules of Civil Procedures regarding the retrieval and presentation of electronically stored information in order to prevent spoliation of evidence provided in litigation, this procedure establishes the guidelines necessary to ensure that any electronically stored information (“ESI”) anticipated to be a part of a discovery request during litigation or as a part of a personnel/administrative investigation shall be preserved in its entirety using the planning and methodology discussed below. The planning and readiness of the relevant local and/or Education Services Center information technology departments in conjunction with the Office of General Counsel and College/District administration are critical to successful compliance with discovery requests and information needed to support findings in an investigation. In order to facilitate ease in obtaining electronically stored information under a discovery request, all electronically stored information should be saved to the appropriate district data servers and not exclusively onto a local desktop or mobile data storage unit.

II. DEFINITIONS

- A. Electronically Stored Information – all electronically formatted documents or other documentary materials made, or received by the Board, its officers, administrators, employees or students of the Los Angeles Community College District in connection with any transaction of public business and education including but not limited to desktops, laptops, and other forms of mobile computing devices such as palmtops, personal handheld assistants (“PDAs”).

- B. Metadata – refers to the embedded, largely invisible electronic information about or behind the on-screen document, such as revision history, authors or cell formulas.

- C. Back-up – creation of an electronic replica of information from on-line systems intended to facilitate when necessary recovery of lost or damaged electronic information.
- D. Custodian of Electronic Record – For information technology (“IT”) retrieval purposes, the IT staff responsible for back up of the system for which the ESI is held.
- E. Electronic Discovery Response Team (“EDRT”) – the group composed of relevant District and College administration, including but not limited to, the Vice President of Administrative Services, the local manager of information systems, relevant IT staff, Office of General Counsel and when applicable, the business user of the data specifically assembled for the purpose of identifying, preserving and retrieving ESI for investigation or litigation purposes.
- F. Responsible information technology department – The IT department who is held responsible for back up and

Storage of ESI.
- G. Transaction logging – the means of identifying in the system where back door changes were made in an electronic transaction.
- H. Discovery – the pre-trial phase of a lawsuit in which the parties may obtain evidence by various means from the opposing party through request for production of documents, depositions (interviews) or interrogatories (questionnaire).

III. PROCEDURES

- A. Discovery requests as a result of anticipated or actual litigation

1. The Office of General Counsel shall immediately notify the Vice President of Administrative Services, local technology administrator and/or the Chief Information Officer at the Education Services Center of any request for electronically stored information. Notification to the appropriate information technology department shall be made based on any possible database location where the electronic information resides. If the electronic information is kept in multiple locations throughout the District, the Office of General Counsel, with the assistance and coordination of the Chief Information Officer, shall inform the local technology department and college administration in the relevant locations. The Office of General Counsel with the responsible manager of information technology and Vice President of Administrative Services will immediately work together to assemble the appropriate “EDRT”.
2. Once the request is issued by the Office of General Counsel, the local information technology administrator and/or Chief Information Officer at the District shall meet immediately with the identified EDRT. At the meeting, the following shall be established in order to effectuate the “litigation” hold:
 - a. Identify the electronic information to be retrieved and placed on hold;
 - b. Establish proposed timelines for production or use of the records;
 - c. Identify all storage devices or databases that the information may reside;
 - d. Determine whether the information is in a searchable format;
 - e. Determine any processes required for data download or transfer in order to store and/or produce the electronic records;
 - f. Determine the form of production of the electronic information;
 - g. Discuss a mechanism for recovering back up data when necessary; and
 - h. Identify an appropriate method of securing and safeguarding the information retrieved for litigation hold purposes.

3. When applicable and necessary, the information technology staff on the EDRT shall physically secure all other storage media devices where the information may reside such as hard drives of personal computers ("PCs"), laptops, and personal data assistants ("PDAs".)
4. When a "litigation hold" is placed on electronic information, the information technology staff, with the assistance of the Office of General Counsel and department supervisor having familiarity with such data records, must identify the information and ensure that a back up copy is immediately made of the information. Back up copies must be kept by the relevant information technology department in a safe and secure place where it can be accessed immediately when needed or transferred to the Office of General Counsel in order to preserve the records for litigation. Release of such back up copies shall not occur until clearance has been given by the Office of General Counsel. All automatic purging processes in the data system must cease until after an appropriate and adequate back up copy is made of the data.

Back up media for electronic information on a "litigation hold" shall be segregated from any normal, routine back up tapes. An inventory log shall be made of the information held in storage which should include a brief report on the preservation methods utilized on such records and the name and signature of the responsible information technology staff performing the back up on the held records.

5. The Chief Information Officer and local technology administrators at each campus shall designate and oversee the technology staff responsible for this task in advance. These individuals may be deemed as "person(s) most knowledgeable" in this matter for preserving the electronic data and may be requested to explain in court the system back up procedures taken to preserve the information. In the event of loss of information, these individuals, along with the Chief Information Officer or local technology administrator may

be asked to testify to the manner of preservation, loss or destruction of such data.

6. In most cases, the data systems which contain electronic records at the college or Education Services Center are routinely retained and backed up either nightly, weekly or stored in an off-site location.
7. If the time period between the request for information and the physical date for turning over the information is more than three (3) months, the Office of General Counsel shall periodically issue a reminder notice to the relevant information technology department to ensure such stored information is being safely kept and preserved.

B. Requests for information as a result of an audit or investigation

1. Requests for information during a personnel or administrative investigation or audit shall follow the basic process established for a litigation hold. However, an assessment should be made by the auditor or investigator with consultation from the Office of General Counsel whether a comprehensive EDRT is necessary or a smaller scale response group.
2. Records shall be held until such investigation is complete or until the auditor or investigator in consultation with the Office of General Counsel determines that the records are no longer needed for investigative or audit purposes.
3. If IT staff is involved in the litigation or investigation for which the records request is made, for the purposes of securing the records and preserving their integrity, the IT staff member's access to such electronic systems of record and/or back up mediums shall be disabled. Such a decision to disable or limit access shall be made by the Office of General Counsel in conjunction with the relevant District/College Administrator overseeing the local IT department.

All IT staff shall be routinely informed of the evolving legal requirements in handling electronic records requests.

A review of the litigation or investigation hold process should be made periodically to ensure that the necessary procedures are established and followed.

IV. LEGAL AUTHORITY, CITATIONS AND OTHER REFERENCES

Federal Rules of Civil Procedure 26(a) (1) (b)

Federal Rules of Civil Procedure 26(f)

Federal Rule of Civil Procedure 34(b)

Federal Rule of Civil Procedure 37

ITP-07-07 USE OF COMPUTING DEVICES AND FACILITIES

I. OVERVIEW

The purpose of this procedure is to establish guidelines for appropriate use of district-owned computing facilities and district-owned /issued computing devices on loan, as well as personally owned computing devices that are consensually offered for use, authorized to perform LACCD related business and functions and connected to the LACCD intranet systems.

All district employees and students shall conduct themselves within the bounds of federal and state law and LACCD board rules and administrative regulations in utilizing district-owned computing facilities and district owned/issued computing devices on loan. District employees and students using district owned/issued computing devices and district or college established computing facilities do not have a reasonable expectation of privacy in these devices and facilities and are not guaranteed that their user files, accounts and electronic mail will be kept private.

When personally owned computing devices are authorized and utilized for work related purposes as set forth in this procedure and connected to the district intranet systems, work files located within the personal computing device similarly are not private and may be accessed by the District or College upon request. These procedures are intended to provide greater detail to those policies adopted in Administrative Regulations B-27 and B-28.

Local information technology departments issuing personal computing devices shall have general oversight in tracking the issuance, condition, use and loss of these equipment items. These departments may also perform routine periodic inventory and audits of these equipment items. For purposes of this procedure, a computing device is defined as a lap top, desk top, mobile data storage device i.e., cellular phone or personal data assistant (PDA), including printers, which are taken for use off site from the college or work location.

II. PROCEDURE

a) User Access to Computing Devices and Facilities

1. District or college issued computing devices. When an employee or student is issued a computing device the following procedures must be followed:
 - a. Employee must complete and submit Equipment On Loan form (attached) to their department head/supervisor or program advisor.
 - b. The form must be approved and signed by the employee's supervisor, information technology manager or administrator and Vice President of Administrative Services. (For on-loan computing devices issued at the Education Services Center, the Director of Business Services shall approve and sign the form in place of the Vice President of Administrative Services at a college location.)
 - c. The local information technology department should employ protective technology in order to secure the data on the computing device and/or to remotely locate the device on loan. In the case of computing devices on loan to a student, the form must be completed by the student's course instructor or program advisor to whom the computing device(s) will be issued as the custodian of the equipment. The local Manager of College Information Systems or local technology administrator and Vice President of Administrative Services must approve this completed form. An employee who subsequently issues computing devices to students must maintain a log of students who these devices have been issued to.
 - d. The employee or student instructor/program advisor must sign the form acknowledging notice and understanding of the use policy for district issued computing devices and acknowledgment of responsibility of risk of loss for the item. A student must also sign off on the same acknowledgment of the use policy when issued his/her on-loan computing device by their instructor/program advisor. To the extent it is feasible, employees issuing devices as program instructor or advisor to students shall identify names of students on their on-loan computing device forms.

- e. When a computing device is loaned, the information technology department shall keep an inventory log of these items upon check out. The inventory log shall include:
- the name of the employee;
 - a description of the item(s) on loan;
 - inventory number and description of the computing device (if an inventory tag does not exist on the device, the Receiving Department must be alerted and shall tag the device appropriately);
 - description of the physical condition of the device and its components;
 - expected return date of the computing device; and
 - if possible, name of the student(s) the instructor or program advisor will issue computing device to.
- f. The Vice President of Administrative Services/Director of Business Services shall keep the original request form and provide a copy of the completed and approved form to the local information technology administrator and appropriate department head/supervisor or program advisor.
- Note:** When students are issued computing devices on the basis for their position as a student worker with the District Office or college, the student shall follow the same procedures as an employee but shall require their direct supervisor to approve the form requesting issuance of a computing device.
- g. Computing devices prior to issuance shall be inspected by the local information technology staff before check-in and check out of the device.
- h. For long term computing devices on loan for more than a year, the Vice President of Administrative Services or Director of Business Services may require that at the end of the year, the equipment be returned by the employee or student for inspection, inventory and maintenance by the local information technology staff.

- h. When a computing device is returned, the local information technology staff shall log the return into their inventory. If during the time of use, damage has occurred to the computing device such damaged shall be reported to the Vice President of Administrative Services to determine further action taken.
- i. If in the course of updating the inventory log of computing devices on loan, a local information technology manager or administrator recognizes a repeat pattern of loss or theft of computing devices to a specific employee, the local information technology administrator may flag the losses as an issue for the Vice President of Administrative Services to review and determine whether further action on the matter should be pursued.

2. Personally owned computing devices utilized for work related purposes connected to the intranet.

Generally, allowing use of personally owned computing devices to perform work related business by employees shall not be the standard means of equipping a college/district operation or program. In determining whether a personally owned computing device is necessitated for use and connection to the intranet, the following considerations must be made prior to permitting use of personal equipment in place of district or college issued equipment:

- a. Evidence of limited resources within a department or program. This justification must be explained on the request for use form;
- b. Determine whether the work to be performed on the personal computing device is appropriate to be entered or maintained on a personal computing device due to the confidentiality of its data; and
- c. Evaluate whether there is a business need to connect such device to the intranet.

Note: Connection to intranet network services is an extremely rare occurrence and requests for such connectivity requires careful review by college/district and information technology administration and may require

additional approvals. Furthermore, additional security protocols may be requested, such as encryption, in order to secure confidential data if placed on such device.

If it is determined by an employee's supervisor that an employee owned personal computing device is required for work related purposes the following process must be followed:

- a. Employee must complete and submit a Personal Computing Device Work Use Authorization form (attached).
- b. The employee must sign the form and obtain approval signatures from their immediate supervisor and the Vice President of Administrative Services/Director of Business Services.
- c. The employee must sign off on all acknowledgments on the form including providing access to work-related computer files upon request by the district or college, acceptance of user policy and acknowledgment of risk of use and loss.
- d. Requests made to the local information technology department to install software licensed by the district or college onto the personal computing device shall not be allowed due to legal limitations on licensed software.
- e. Personal computing devices shall meet standards defined by the local information technology department to ensure that the item is virus free, security protected, and non-disruptive to the existing information technology systems operations.
- f. Owners of personal computing devices offered for use in district and college related business under this procedure shall grant the local information technology department at their location administrative level access to their computing device.

3. Computing facilities

- a. **Employees.** Access to computing facilities are provided to employees in order to transact district or college business functions. Any use of these computing facilities must be in accordance with Administrative

Regulations B-27 and B-28. Similar to use of computing devices, employees shall not use any computing facilities for any inappropriate purposes or to conduct their own personal business. Inappropriate use of district or college computing facilities may subject an employee to discipline up to and including dismissal. Employees using computing facilities to conduct district or college business shall not disclose confidential data records or provide unauthorized access to such records.

All personal passwords issued to employees shall not be disclosed and utilized by others. A periodic audit of employee passwords shall be performed to ensure appropriate and updated use of passwords.

- b. Students.** Students are issued accounts for computer facilities use upon enrollment in classes. Students shall use the college's computing facilities for college related activities and educational studies only. Use of college facilities for computing shall be in accordance with all applicable rules, regulations, state and federal laws. Failure to adhere to these legal requirements or inappropriate use of computing devices and facilities may subject a student to disciplinary action including and up to expulsion from the college.

III. LEGAL AUTHORITY, CITATIONS OR OTHER REFERENCES

LACCD Board Rule 9803.26
LACCD Administrative Regulations B-27 and B-28
Asset Procedures 05-10
Title 18, Section 1030, Computer Fraud and Abuse Act
Request for Computing Device on Loan Form
Request for Use of Personally Owned Computing Device Work Use Form
Student Conduct Code

APPROVAL REQUEST FORM FOR COMPUTING DEVICE ON LOAN

1. Requestor Name: _____ Employee# _____

2. Department/Program: _____ Date of request: _____

3. Request use of the following device(s) for Check Out:

Description of device	Serial No.	Inventory No.	Expected Return date	Condition

(*See attached form for additional listing of devices.)

4. The Requestor shall utilize such device(s) for the purpose of:

If computing device(s) are being checked out by an instructor or program advisor for purposes of loaning device(s) to students, please identify the names of the students here: (Attach additional form if needed.)

(Please provide Use Policy Acknowledgement Form to all students to sign and provide copies to local information technology manager or administrator.)

5. As Requestor of the above device(s) on loan I understand and agree to the following:

(Please initial that you have read each item below.)

_____] I have read the guidelines provided to me along with this form and agree to abide by the use of the device(s) on loan in accordance with all guidelines related to my usage including but not limited to, Administrative Regulations B-27 and B-28.

_____] I shall keep the device(s) secure from loss or damage. If damage or loss occurs to the device which is a result of my failure to follow the appropriate guidelines or employ reasonable safeguards, I understand that I shall be responsible for such loss or damage and shall be asked to reimburse the College/District.

_____] I shall maintain the confidentiality of any District or College data that is placed on such device(s).

_____] I shall not place any inappropriate data or software programs on the device(s) that has not been approved for download by the local information technology department.

_____] I shall report any loss or theft of the device(s) immediately to the Sheriff's Department and to the local information technology department.

_____] I shall not alter, revise or modify the existing hardware or software configuration or settings, including but not limited to disabling security features of the computing device.

Requestor Signature: _____ Date: _____

Print Name: _____

Supervisor Signature: _____ Date: _____

Print Name: _____

Manager of College Information Systems/IT Administrator Signature: _____ Date: _____

Print Name: _____

VP of Administrative Services/Director of Business Services Signature: _____ Date: _____

Print Name: _____

The following devices were Checked In: (To be completed by Manager of College Information Systems or local technology administrator.)

Description of device	Serial No.	Inventory No.	Return date	Condition

(Attach additional form for additional devices checked-in)

*All Items Above Inspected and Received by:

_____ Date

_____ Signature

PLEASE OBTAIN STUDENT SIGNATURES IF DEVICE IS ISSUED BY PROGRAM INSTRUCTOR OR PROGRAM ADVISOR TO STUDENT(S)

*Use of Computing Devices are subject to the regulations, policies and procedures found in Administrative Regulations B-27, B-28 and ITP 07-07. I acknowledge that I am informed of such regulations, policies and procedures and agreed to abide by the terms set forth in these documents and in this approval request form.

Student Signature: _____ Date: _____

Attach additional form with student signatures if necessary.

**USE OF PERSONAL COMPUTING DEVICE
FOR WORK-RELATED BUSINESS AND ACCESS TO INTRANET**

1. Requestor Name: _____ Employee ID# _____

_____ (includes consultants/professional experts)

2. Department/Program: _____ Date of request: _____

3. Request use of the following device(s):

Description of device	Serial No.	Expected length of use	Condition

4. The Requestor shall utilize their personal computing device(s) for the purpose of:

5. As Requestor, I understand and agree to the following: **(Please initial each box.)**

a.	I shall safeguard and maintain the confidentiality of any District or College data that is placed on my personal computing device.
b.	When deemed necessary, I shall provide access to work related data files on my personal computing device to the College/District.
c.	I acknowledge the risk of offering my personal computing device for work related use and understand that any loss or damage that occurs to my personal computing device in this capacity may not be compensated by the College/District.
d.	I shall ensure that my personal computing device is free from any virus or other defective conditions which may render my personal computing inhospitable for work-related use. I agree to work with the local IT Department at my location to verify that my personal computing device is suitable for use.
e.	I understand that any district procured licenses for software applications cannot be loaded to my personally-owned device.
f.	I understand that the District/College is not responsible for the condition of my device prior to use and access onto the intranet for LACCD related business purposes.

Requestor Signature: _____ Date: _____

Supervisor Signature: _____ Date: _____

Print Name: _____

Manager of Information Systems/IT Administrator Signature: _____ Date: _____

Print Name: _____

VP of Administrative Services Signature: _____ Date:

Print Name: _____

Please attach ITP 07-07 to this Form.