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 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 custodian 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 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 computing data equipment or devices when necessary to prevent possible data security breaches and prior to retirement or disposal of district owned 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 notice the College President, Vice President of Administrative Services, Deputy Chancellor (in case where breach occurs at Education Services Center), Chief Information Officer and General Counsel of the breach. After initial assessment of the data security breach is made, 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 their 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 (if breach occurs at the Education Services Center) the Vice President of Administrative Services or Deputy Chancellor shall be briefed 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 District is subject to notification of 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 data breach occurs of medical information, 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 things 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 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 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 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 ability to download data content from the internet.

Disabling of User Access: Guest 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.
c) Surrendering User Access Account and Password and Escrowing of Accounts.

IV. LEGAL AUTHORITY, CITATIONS OR OTHER REFERENCES

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