

## 1.0 Definitions

### 1.1 “Conflict of Interest”

1.1.1 A “conflict of interest” exists when a Los Rios Community College District employee, in their role as a District/College employee, participates in a decision or transaction or provides services where the employee personally benefits from the decision, transaction, or services.

1.1.2 A “conflict of interest” also exists when a Los Rios Community College District employee, in their role as a District/College employee, participates in a decision or transaction or provides services where a member of the employee’s immediate family personally benefits from the decision, transaction, or services.

1.1.3 A benefit may either be financial or non-financial.

1.1.3.1 A financial benefit exists when an employee or a member of his or her immediate family receives a monetary benefit or his or her existing financial interests are materially affected by the decision, transaction, or services.

1.1.3.2 A non-financial benefit exists when an employee or a member of his or her immediate family receives a non-monetary benefit (for example, the employee or family member receives a grade, a service, an enrollment, priority enrollment, or special treatment) by the decision, transaction, or services.

1.1.4 Where the benefit received in the transaction is indirect and immaterial, a conflict of interest does not exist.

1.2 The immediate family of an employee is defined as: mother, father, grandparent, or grandchild of the employee or of the employee’s spouse or domestic partner; step-mother, step-father, spouse, domestic partner, son, mother-in-law, father-in law, son-in-law, step-son, daughter, daughter-in-law, step-daughter; brother, brother-in-law, sister, sister-in-law, aunt, or uncle of the employee; child of a domestic partner, sibling of a domestic partner; wife or husband of a domestic partner’s child; or any person living in the immediate household of the employee.

1.3 A District/College employee “participates in a decision” when the employee, in his or her role as a District/College employee, makes or participates in the making of a decision. A District/College employee “participates in a transaction” or “provides services” when the employee, in his or her role as a District/College employee, participates in, executes, processes, reviews, or approves a transaction or services.

1.4 “Financial interest” means a District/College employee’s investment in or position with business entities, interests in real property, sources of income, sources of gifts,

the personal finances of the employee, or the personal finances of a member of the immediate family of the employee.

## 2.0 Conflict of Interest Prohibited

2.1 A District/College employee shall not participate in a decision or transaction or provide services when they have a conflict of interest.

2.1.1 If it is unclear whether a conflict of interest exists, the determination shall be made by the General Counsel.

## 3.0 Purchasing Transactions

3.1 A District/College employee shall not participate in the preparation of specifications for the purchase of equipment or material, the selection of a vendor, or the selection of a contractor if such participation constitutes a conflict of interest.

3.2 A District/College employee who participates in the selection of a vendor shall sign the following conflict of interest disclaimer statement:

“This is to certify that the undersigned employee has no economic interests which may foreseeably be materially affected by having participated in the development of the specifications for equipment and/or material represented by this requisition.”

3.3 No purchase or lease of goods or contract for services shall be made from any District/College employee or a member of the immediate family of an employee unless there has been a specific determination in writing by the Director of General Services that the goods or services are not available from any other source.

## 4.0 Specific Employee and Immediate Family Transactions

4.1 A District/College employee shall not participate in a decision or transaction or provide services that will benefit the employee or a member of the immediate family of the employee in the following areas:

4.1.1 Student record transactions: Examples include, but are not limited to, grade changes, course enrollments, and providing permission numbers.

4.1.2 Financial transactions: Examples include, but are not limited to, payroll, fee payments, retail purchases (bookstore, cafeteria, etc.), and box office transactions.

4.1.3 Human resource transactions: Examples include, but are not limited to, hiring, discipline, termination, employee record changes, and absence report or timesheet processing.

- 4.1.4 Financial aid transactions: Examples include, but are not limited to, application, approval and disbursement for grants, loans, fee waivers, and scholarships.
- 4.1.5 Student services: Examples include, but are not limited to, counseling, CalWORKs, DSPS, EOP&S, and Child Development Centers.

## 5.0 Incompatible Activities

- 5.1 A District/College employee shall not engage in any employment, activity, or enterprise which is clearly inconsistent, incompatible, in conflict with, contrary to, or inimical to his or her duties as a District/College employee. Prohibited activities include, but are not limited to, the following:
  - 5.1.1 Using the prestige or influence of the District/College(s) for the employee's private gain or advantage or the private gain or advantage of another.
  - 5.1.2 Using District/College(s) time, facilities, equipment, or supplies for the employee's private gain or advantage or the private gain or advantage of another.
  - 5.1.3 Using, or having access to, confidential information available by virtue of District/College(s) employment for private gain or advantage or providing confidential information to persons to whom issuance of this information has not been authorized.
  - 5.1.4 Receiving or accepting money or any other consideration for the performance of his or her duties as a District/College employee from anyone other than the District.
  - 5.1.5 Performance of an act in other than his or her capacity as a District/College employee knowing that the act may later be subject, directly or indirectly, to the control, inspection, review, audit, or enforcement by the same employee.
  - 5.1.6 Receiving or accepting, directly or indirectly, any gift, including money, or any service, gratuity, favor, entertainment, hospitality, loan, or any other thing of value from anyone who is doing or is seeking to do business of any kind with the District/College(s) or whose activities are regulated or controlled by the District/College(s) under circumstances from which it reasonably could be substantiated that the gift was intended to influence the employee in his or her official duties or was intended as a reward for any official actions performed by the District/College employee.
  - 5.1.7 Subject to any other laws, rules, or regulations as pertain thereto, not devoting his or her full time, attention, and efforts to the

District/College(s) during his or her hours of duty as a District/College employee.

## 6.0 Student Loans [Higher Ed. Opportunity Act, Pub. Law No 110-315, § 493]

6.1 As it relates to student loans, the following prohibitions also apply to the District/College and its employees:

- 6.1.1 A District/College employee is prohibited from steering students to use one particular student loan lender over another or delaying the processing of a loan with one student loan lender over another lender. Students must select the student loan lender of their choice.
- 6.1.2 A District/College employee shall not make the offer of private student loans to a student contingent upon a specific number of Title IV loans being offered to a student loan lender.
- 6.1.3 A District/College employee shall not request or accept from any lender any assistance in calling students or working in the financial aid offices of the Colleges. Notwithstanding this prohibition, student loan lenders may provide professional development training and educational counseling materials as long as the materials identify the lender that assisted in preparing the materials and student loan lenders may provide staffing services on a short-term, non-recurring basis during emergencies or disasters.

## 7.0 Exceptions

- 7.1 Employees shall make every effort to avoid conflicts of interest or perceived or potential conflicts of interest. In the event an employee believes they may have a conflict of interest, they shall discuss that matter with their immediate supervisor. As appropriate, the immediate supervisor shall inform the Vice Presidents of Administration for College employees or a Director of Accounting Services for District Office employees.
- 7.2 There are certain decisions, transactions or services that may benefit an employee or a member of the immediate family of the employee where employees are required to participate due to their position in the District or due to the resources available. In those instances, prior to participating in the decision or transaction or rendering the services, the employees shall disclose any interest they have that may be benefited from the decision, transaction, or services in writing to the Vice President of Administrative Services for College employees or a Director of Accounting Services for District Office employees, and obtain their written approval. Additional controls, such as periodic review, shall be undertaken to prevent or detect irregularities.
- 7.3 The selection of educational materials by faculty in the context of a course they teach is not covered under this District Policy.

## 8.0 Additional Provisions for National Science Foundation (NSF) Grants

8.1 Prior to submitting any NSF grant application and annually during the term of any NSF grant, each “investigator” shall disclose to the Director of Accounting Services all significant financial interests of the investigator (including those of the investigator’s spouse and dependent children):

- 8.1.1 that would reasonably appear to be affected by the research or educational activities funded or proposed for funding by NSF; or
- 8.1.2 in entities whose financial interests would reasonably appear to be affected by such activities.

This disclosure must be updated as reportable significant financial interests are obtained.

8.2 The term “investigator” means the principal investigator, co-principal investigators/co-project directors, and any other person at the District/College who is responsible for the design, conduct, or reporting of research or educational activities funded or proposed for funding by NSF.

8.3 The term “significant financial interest” means anything of monetary value, including, but not limited to: salary or other payments for services (e.g., consulting fees or honoraria); equity interest (e.g., stocks, stock options, or other ownership interests); and intellectual property rights (e.g., patents, copyrights, and royalties from such rights).

8.3.1 The term “significant financial interests” does not include:

8.3.1.1 salary, royalties, or other remuneration from the Los Rios Community College District;

8.3.1.2 income from seminars, lectures, or teaching engagements sponsored by public or non-profit entities;

8.3.1.3 income from service on advisory committees or review panels for public or nonprofit entities;

8.3.1.4 an equity interest that, when aggregated for the investigator and the investigator’s spouse and dependent children, meets both of the following tests: does not exceed \$10,000 in value as determined through reference to public prices or other reasonable measures of fair market value, and does not represent more than a 5% ownership interest in any single entity; or

8.3.1.5 salary, royalties, or other payments that, when aggregated for the investigator and the investigator’s spouse and dependent children, are not expected to exceed \$10,000 during the twelve-month period.

- 8.4 Annually, The Director of Accounting Services shall review financial disclosures, determine whether a conflict of interest exists, and determine what conditions or restrictions, if any, should be imposed by the District to manage, reduce or eliminate such conflict of interest. A conflict of interest exists when the reviewer(s) reasonably determines that a significant financial interest could directly and significantly affect the design, conduct, or reporting of NSF-funded research or educational activities. The Director of Accounting Services shall keep NSF's Office of the General Counsel appropriately informed if the District finds that it is unable to satisfactorily manage a conflict of interest.
- 8.5 Examples of conditions or restrictions that might be imposed to manage, reduce or eliminate conflicts of interest include, but are not limited to:
- 8.5.1 public disclosure of significant financial interests;
  - 8.5.2 monitoring of research by independent reviewers;
  - 8.5.3 modification of the research plan;
  - 8.5.4 disqualification from participation in the portion of the NSF-funded research that would be affected by significant financial interests;
  - 8.5.5 divestiture of significant financial interests; or
  - 8.5.6 severance of relationships that create conflicts.
- 8.6 If the Director of Accounting Services determines that imposing conditions or restrictions would be either ineffective or inequitable, and that the potential negative impacts that may arise from a significant financial interest are outweighed by interests of scientific progress, technology transfer, or the public health and welfare, then the Director of Accounting Services may allow the research to go forward without imposing such conditions or restrictions.
- 8.7 The District shall maintain records of all financial disclosures and of all actions taken to resolve conflicts of interest for at least three years beyond the termination or completion of the grant to which they relate, or until the resolution of any NSF action involving those records, whichever is longer.

## 1.0 Definitions

- 1.1 For the purpose of these Los Rios Community College District Policies and Administrative Regulations, terms shall be defined as follows:
  - 1.1.1 “Access” means to gain entry to, instruct, or communicate with the logical, arithmetical, or memo function resources of a computer, computer system, or computer network.
  - 1.1.2 “Administrative Computing” means all computer equipment, software, services, policies, and procedures which are in place to support all computing except direct instructional use (classroom, video, Internet, or other methods). Administrative Computing includes, but is not limited to systems which serve the following functions, internal Business/Accounting, Human Resources/Personnel, Student Administration/Records, electronic-mail/calendaring, general Internet/intranet use, Desktop office systems, file sharing/printing, and all other general productivity systems. Participation in Administrative Computing systems is applicable to Los Rios Management, Faculty, Classified Staff, Students, Contractors, and Consultants.
  - 1.1.3 “Administrator” means a District employee, or a contractor or vendor authorized by a District employee to provide access to the Systems.
  - 1.1.4 “Computer contaminant” means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, bypass security programs, modify, destroy, record, or transmit data, or in some other fashion alter the normal operation of the computer, computer system, or computer network.
  - 1.1.5 “Computer network” means any system which provides communications between one or more computer systems and input/output devices including, but not limited to, personal computers, servers, display terminals and printers.
  - 1.1.6 “Computer program or software” means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system or computer network to perform specified functions.
  - 1.1.7 “Computer services” includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

- 1.1.8 “Computer system” or “System” means any computers, network, and/or associated facilities which includes hardware, software, data stored or accessible electronically, and documents and manuals available to support the usage and/or operation and maintenance of the System leased or owned by the District and associated facilities, including those located on the college campuses, outreach centers, the District Office, Facilities Management, and other offsite facilities whether wholly or partly operated by the District, as a computer system designed, intended or used for administrative purposes.
- 1.1.9 “Data” means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit, or presented on a display device.
- 1.1.10 “Injury” means any unauthorized alteration, deletion, damage or destruction of a computer system, computer network, computer program, or data caused by the access.
- 1.1.11 “Supporting documentation” includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.
- 1.1.12 “User” includes any District employee, student, contractor, vendor or other person who uses the Systems.
- 1.1.13 “Victim expenditure” means any expenditure reasonably and necessarily incurred by the owner/lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

## 1.0 Statement of Responsibilities

- 1.1 This regulation shall apply to all users of the Los Rios Community College District Systems.
- 1.2 Users must not share their account with others. With a few exceptions, accounts shall be issued to individuals for specific purposes and are not to be shared, unless otherwise approved by an Administrator.
- 1.3 Users must use computing facilities and services only for District business.
  - 1.3.1 Accounts must not be used for private consulting or sold to other individuals.
  - 1.3.2 Computing and/or networking resources must not be used for direct personal financial gain (except for appropriate contract and external accounts) or to provide free resources for unauthorized purposes.
- 1.4 Users must not attempt to interfere with the normal operation of the system.
- 1.5 Users must not attempt to encroach on others' use of computing and/or networking facilities or to deprive them of resources.
- 1.6 Users must not attempt to subvert the restrictions associated with their computer accounts.
- 1.7 Users must not attempt unauthorized access of computer installations outside the District computers or networking facilities.
- 1.8 Use of the Systems is a privilege that shall not be abused. Users shall be held to a high standard of professional behavior by complying with all Policies and Administrative Regulations relating to the Systems' use. The following are examples of unethical and inappropriate use.
  - 1.8.1 Transmitting unsolicited information which contains obscene, indecent, lewd or lascivious material or other material which explicitly or implicitly refers to sexual conduct;
  - 1.8.2 Transmitting unsolicited information which contains profane language or panders to bigotry, sexism, or other forms of discrimination;
  - 1.8.3 Communicating any information concerning any password, identifying code, personal identification number or other confidential information without the permission of its owner or the controlling authority of the computer facility to which it belongs;
  - 1.8.4 Creating, modifying, executing or retransmitting any computer program or instructions intended to gain unauthorized access to, or make unauthorized use of a computer facility;

- 1.8.5 Creating, modifying, executing or retransmitting any computer program instructions intended to obscure the true identity of the sender of electronic mail or electronic messages, collectively referred to as "messages" including, but not limited to, forgery of messages and/or alteration of system and/or user data used to identify the sender of messages;
- 1.8.6 Accessing or intentionally destroying software or licensed software in a computer facility without the permission of the owner of such software or licensed software or the authority of the facility;
- 1.8.7 Making unauthorized copies of licensed software;
- 1.8.8 Communicating any credit card number or other financial account number without the written permission of its owner;
- 1.8.9 Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose;
- 1.8.10 Using the computer facilities in a manner inconsistent with the District's contractual obligations to suppliers of computer facilities or with any published District policy.
- 1.8.11 Using the Internet to gain unauthorized access to any computer;
- 1.8.12 Using computer facilities for work done on behalf of a commercial firm;
- 1.8.13 Copying a file from another computer user's account or any recording media without permission;
- 1.8.14 Copying copyrighted computer software for use on another computer without permission;
- 1.8.15 Unplugging or reconfiguring computer equipment to make it unusable or difficult to use;
- 1.8.16 Engaging in personal attacks: writing bullying, intimidating, threatening or harassing entries;
- 1.8.17 Making threats (directed towards others or yourself) without expecting the recipients of those threats, the college, and the police to consider them real; and
- 1.8.18 Displaying sexually explicit or sexually harassing images or text in a public computer facility or location that can potentially be in view of other individuals.

Adm. Regulation Revised: 9/27/10

Adm. Regulation Reviewed:

Board Policy: [P-8831](#)

Employee's  
Copy

## 1.0 Programs and Files

- 1.1 Generally, the Los Rios Community College District will not examine electronic mail or material except in the following circumstances:
  - 1.1.1 Investigating a potential violation of the law or District Policies, Administrative Regulations or guidelines;
  - 1.1.2 Disc capacities are exceeded, and user's mail storage is a contributing factor;
  - 1.1.3 Performing any necessary maintenance of the System;
  - 1.1.4 Forwarding a misdelivered message;
  - 1.1.5 Closing an account which contains unread mail;
  - 1.1.6 The Chancellor determines that examination is necessary.
- 1.2 Absent reasonable cause, users shall be notified that electronic mail was examined by a system administrator.
- 1.3 The District reserves the right to access all information stored on District computers. When performing maintenance, every effort will be made to insure the privacy of user's files. However, if violations are discovered, they will be reported immediately to the appropriate District/College official(s).

---

LRCCD

Adm. Regulation Adopted: 1/24/00  
Adm. Regulation Revised: 9/27/10; 1/25/16  
Adm. Regulation Reviewed: 1/25/16  
Board Policy: [P-8851](#)

## 1.0 This Administrative Regulation is intended to guarantee, to the extent possible, the security and integrity of the Systems

- 1.1 The Systems are owned by the Los Rios Community College District and are to be used for District-related activities only. If faculty, staff or students bring personally-owned equipment into the District environment, they will be required to adhere to existing District and College policy as use of their equipment may affect the work of others.
- 1.2 Informational access to resources connected to local, national and/or international networks may be permitted, as a courtesy to others on the network, as long as their use does not adversely affect campus use and such access provides benefit to the District.
- 1.3 Users shall recognize their responsibility in the process of maintaining security of District computing and networking resources.

## 2.0 District Information Security Officer

- 2.1 The District's Vice Chancellor, Education and Technology shall be the District's Information Security Officer (ISO). The District ISO, in conjunction with the District Office Information Technology Department (District IT Department), is responsible for implementing the Information Security Policy and Regulation. The District ISO with the assistance of the District's Internal Auditors shall:
  - 2.1.1 Ensure the Information Security District Policy and Administrative Regulation is updated on a regular basis and published as appropriate.
  - 2.1.2 Ensure appropriate training is provided to data owners, data custodians, network and system administrators, and users.
    - 2.1.2.1 Data owners are the person or persons responsible for creating data that is resident on the Systems;
    - 2.1.2.2 Data custodians are the persons responsible for administering the infrastructure to store and transmit data on the Systems;
    - 2.1.2.3 Data users include any District employee, student, contractor, vendor or other person who uses the Systems;
    - 2.1.2.4 The terms *system* and *network* administrator as used in this Administrative Regulation are generic and pertain to any person who performs those duties, not just those with that title or primary job duty.
  - 2.1.3 Ensure each College and the District Office appoints a person responsible for security implementation, incident response, periodic user access reviews, and distribution of information security policies and education, (e.g. information about virus infection risks).

- 2.1.4 Respond to internal and external complaints and/or queries about real or perceived non-compliance with the District's Information Security Policy and Administrative Regulation.
- 2.2 Each manager is responsible for establishing procedures to implement the provisions of this District Policy and Administrative Regulation within their areas of responsibility, and for monitoring compliance.

### 3.0 Data Classification Policy

- 3.1 It is essential that all District data be protected. Different categories of data require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. There are three primary categories of data in the District's Systems:
  - 3.1.1 High Risk Data – High Risk data is information for which the law prohibits unauthorized disclosure and requires notification of the affected parties if unauthorized disclosure occurs. Data covered by federal and state identity theft prevention laws, such as the Information Practices Act of 1977 (Civ. Code, § 1798, et seq.), Health Insurance Portability and Accountability Act (10 U.S.C., § 1320d-2), the Financial Information Privacy Act, (Fin. Code, §§ 4050, et seq.), or other laws are in this category. Any electronic record of a Social Security number, driver license number, or California Identification Card number, medical information, health insurance account number, or bank/credit account number (with any required access password) when associated with other data that in any way identifies a person falls in this category. A user name or email address, in combination with a password or security question and answer that would permit access to a District online account also falls in this category. Data in this category requires the highest degree of care to safeguard it from unauthorized use and/or disclosure.
    - 3.1.1.1 Other data may need to be treated as High Risk because it would cause severe damage to the District if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.
  - 3.1.2 Confidential Data – Confidential data is information not meeting the criteria of High Risk Data, but subject to other legal privacy requirements, such as FERPA (20 U.S.C., § 1232g), the privacy clause of the California Constitution (Cal. Const., Art. 1, § 1), the California Student Records Act (Ed. Code, §§ 76200, et seq.), and the attorney-client or other legally recognized privilege. Confidential data can also include data that would not expose the District to financial or other liability if disclosed without authorization, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements for this type of data.

- 3.1.3 Unrestricted Data – Unrestricted data is information that may be released or shared on an as needed basis. Examples of this data would be schedules of classes, or other publicly available information.
- 3.2 All District data shall be categorized in one of the three categories set forth in section 3.1 and protected according to the requirements set for each category. The data category and its corresponding level of protection should be consistent when the data is replicated and as it flows through the District
- 3.2.1 Managers must ensure that all data collected or stored by persons in their operating unit is properly classified. Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.
- 3.2.2 No District-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification. (All District computers are connected to the internet unless specific effort has been taken to eliminate such connections.)
- 3.2.3 Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.
- 3.2.4 High Risk data must be encrypted during transmission over insecure channels (all network connections should be considered insecure unless the District IT Department has provided specific guidance otherwise).
- 3.2.5 High Risk data, when stored on portable computers or storage devices, shall be encrypted on the disk to prevent access without knowledge of a password.
- 3.2.6 Confidential data should be encrypted during transmission over insecure channels.
- 3.2.7 All data necessary for the efficient operation of the District should be backed up, and the backups tested periodically, as part of a documented, regular process.
- 3.2.8 Backups of data must be handled with the same security precautions as the data itself. When Systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

#### 4.0 Required Information Security Practices

- 4.1 The following information security practices are mandatory:

- 4.1.1 The District shall use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the District's data, network and system resources.
- 4.1.2 Security reviews of servers, firewalls, routers and monitoring platforms shall be conducted on a regular basis. These reviews shall include user and access privileges, monitoring access logs and results of intrusion detection software, where it has been installed.
- 4.1.3 All collection and use of High Risk data is forbidden except when required in performance of assigned duties. Collection, storage and use of High Risk data must be approved by management. No High Risk data shall be transported off site without proper authorization. Where reasonable alternatives exist or can be created in lieu of the use or creation of High Risk data, those alternatives shall be used.
- 4.1.4 All workstations shall be configured such that after a few minutes of inactivity (not to exceed 30) they shall automatically enter screen saver mode and require a password to resume work.
- 4.1.5 Servers, desktop computers, or portable computers storing data including Social Security numbers, driver license numbers, credit card numbers, or other financial account information linked to names must be reported to the District IT Department. At least two times each year, vulnerability scans shall be run against these identified machines.
- 4.1.6 Computers storing High Risk Data shall require a password for access and shall be configured to go into password protected screensaver mode within a reasonable time of non-operation. Encryption is required for High Risk data stored on portable computers and portable storage devices (e.g. USB flash storage or external drives.)
- 4.1.7 Application development that is intended to store, manipulate, or transfer High Risk data must occur in a secure development environment, and to the extent any development or testing occurs outside the secure development environment must use data with all High Risk elements removed or fictionalized during the development and testing process.
- 4.1.8 An employee, data owner, data custodian, network and system administrator or user shall immediately notify the District ISO if that person becomes aware that High Risk or Confidential data has been lost, stolen, compromised, or disclosed to an unauthorized person.
- 4.1.9 When outsourcing application support for applications that store High Risk or Confidential data, asset protection and escrow arrangements in the event of third party failure should be included in the contractual language. Asset protection refers to a process where the agencies agree upon ownership and the classification of information, and documents the process for safeguarding each asset to protect against data loss, data theft, or unauthorized access to data. Escrow arrangements provide for access

and use of the application source code in the event the vendor goes out of business or otherwise is unable to continue to support the application.

4.1.10 Critical technology (i.e. remote access technologies, wireless technologies, removable electronic media, laptops, tablets, PDAs, email, and internet usage) with access to credit card processing devices/networks, must have the following usage policies established:

- 4.1.10.1 Explicit approval by management.
- 4.1.10.2 Authentication for use of the technology.
- 4.1.10.3 Log of all devices and personnel with access.
- 4.1.10.4 Acceptable uses of technologies defined and documented.
- 4.1.10.5 Acceptable network locations for the technologies defined and documented.
- 4.1.10.6 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.
- 4.1.10.7 Activation of remote access technologies for vendors and business partners only when needed and immediate deactivation after use.

## 5.0 Recommended Information Security Practices

5.1 The following information security practices are strongly recommended, but not required:

- 5.1.1 Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis. A regular basis, at a minimum, includes testing annually, but the sensitivity of the information secured may require that these tests be done more often.
- 5.1.2 Education should be provided to District faculty and staff to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual, network administrator, system administrator, data custodian, and users.
- 5.1.3 Use of existing data stores is preferred over development of new data stores containing High Risk or Confidential data. Creation of any computer file or database that contains High Risk or Confidential data must be approved in advance by a College or District manager. Such approved data stores will be identified and communicated to District IT Department in order that the computer(s) storing such data may be monitored to assure proper configuration to reduce the chance of intrusion by unauthorized users. Sufficient information about the data to be collected and stored and the proposed use of the data must be

communicated to District IT Department to support analysis of possible use of existing data stores to meet the work requirements.

## 6.0 Access Control Policy

- 6.1 Data shall be captured and stored in a manner that supports employees accessing the data necessary to the job function without permitting access to sensitive or confidential data unnecessary to the job function. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and maintained.
- 6.2 More than one person shall have full administrative rights to any District owned server storing or transmitting data necessary to the ongoing operation of the district. Data owners or custodians may enact more restrictive policies for end-user access to their data.
- 6.3 Access to the network and servers and Systems shall be achieved by individual and unique logins, and shall require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication. Access to the administrative network must be achieved by individual and unique logins and must require authentication. Account sharing on the administrative network is prohibited. Access to the WiFi Public network may be granted with shared logins for guests of the District attending a training, meeting, conference, or other management approved activity. Shared accounts shall not be activated for more than the duration of the event.
- 6.4 Users shall not share usernames and passwords with anyone. Users shall not write down or record their passwords in unencrypted electronic files or documents. When limited access to District-related documents or files is required specifically and solely for the proper operation of District operating units and where available technical alternatives are not feasible, exceptions are allowed under an articulated operating unit policy that is available to all affected operating unit personnel. Each such policy must be reviewed by the operating unit executive officer and submitted to the Dean of the department responsible for Information Technology or the District IT Department for approval. All users must secure their username or account, password, and system access from unauthorized use.
- 6.5 All users of Systems that contain High Risk or Confidential data must have a strong password - the definition of which will be established and documented by the District IT Department after consultation with the College community. These passwords must be changed at regularly consistent intervals with guidelines developed by the District IT Department.
- 6.6 Passwords for empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by the District IT Department.
- 6.7 Passwords must not be placed in emails unless they have been encrypted.

- 6.8 Default passwords on all Systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the strong password selection criteria when a system is installed, rebuilt, or reconfigured.
- 6.9 Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
- 6.10 Users are responsible for safe handling and storage of all District authentication devices. Authentication tokens (such as a SecureID card) should not be stored with a computer that will be used to access the District's network or system resources. If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.
- 6.11 Human Resources shall be responsible for reporting terminated employees to the District IT Department upon their termination or transfer. Access for those terminated employees shall be reviewed and adjusted as found necessary. Normally, terminated employees should have their accounts disabled immediately upon termination. Because there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the operating unit security person.
- 6.12 Transferred employee access shall be reviewed and adjusted as necessary by the new supervisor.
- 6.13 Monitoring shall be implemented on all Systems including recording logon attempts and failures, successful logons and date and time of logon and logoff. There shall be a documented procedure for reviewing system logs.
- 6.14 Activities performed as administrator or superuser must be logged where it is feasible to do so.
- 6.15 Personnel who have administrative system access shall use other less powerful accounts for performing non-administrative tasks.
- 6.16 Users who are authorized to have remote access to the network, servers, and Systems must review and adhere to the Los Rios Information Technology Remote Access Procedures.

## 7.0 All individuals employed by the District are held responsible for adhering to District procedures for system access, use and security

- 7.1 Computer and network accounts must not be made available to others or used for any purpose for which they are not authorized. Unsponsored research accounts must not be used for sponsored research or private consulting. Unauthorized attempts to modify system facilities and/or subvert the restrictions associated with computer accounts are a violation of State law.

- 7.2 Violators of the Administrative Computer Use policies are subject to the termination of their access, referral to the appropriate administrator, sanctions, disciplinary action and/or criminal prosecution depending on the severity of the violation.

## 8.0 The District is charged with maintaining overall security on the Systems and is responsible for the development and maintenance of appropriate awareness program guidelines, and procedures to assure a secure environment for the District community

- 8.1 The District's academic and administrative departments who wish to operate their own systems shall comply with these Administrative Regulations.
- 8.2 Programs and files are confidential unless they are explicitly made available to other authorized individuals. When performing system maintenance, every effort is made to insure the privacy of a user's files. However, support personnel may access files when required for the maintenance of District computing Systems and networks. All such access will be recorded and reported at an appropriate time to the District. If in doing so, violations of policy and/or procedure are discovered, they will be immediately reported to the Administrator.

## 9.0 Exceptions to Policy

- 9.1 In certain cases, compliance with specific Policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:
- 9.1.1 Required commercial or other software in use is not currently able to support the required features;
- 9.1.2 Legacy systems in use do not comply, but near-term future systems will, and are planned for;
- 9.1.3 Costs for reasonable compliance are disproportionate relative to the potential damage.
- 9.2 In such cases, operating units must develop a written explanation of the compliance issue and a plan for coming into compliance with the District's Information Security Policy in a reasonable amount of time. Explanations and plans must be submitted to the Dean of the department responsible for Information Technology at the College or the equivalent officer(s).