

1.0 Security

- 1.1 Information security is an area of utmost concern and importance to the Los Rios Community College District. Given the rapid pace of technological change, the decentralization of computing, and the proliferation of computers, networks and users of varying capabilities, it is essential that these systems be protected from misuse and unauthorized access. This Policy and corresponding Administrative Regulation are established to help maintain the security of District Systems and to inform all users of their rights and responsibilities relative to computer security awareness.
- 1.2 Storage of District data on the District's Systems and transfer of data across its internal network supports efficient work processes. Commensurate with that efficiency is the need for the appropriate security measures. Protection of confidential information is a primary goal of the District and should be achieved in all aspects of data collection and use.
- 1.3 This Information Security Policy (Policy) recognizes that not all communities within the District are the same and that data are used differently by various operating units within the District. This Policy, however, applies to all operating units within the District. While all confidential information shall be handled and stored in a manner that will protect the privacy of students, faculty and staff of the District, this Policy addresses requirements for confidential information stored and transmitted in electronic form on computers and computer networks. For purposes of this Policy and accompanying Administrative Regulation, operating units include each separate department at each of the Colleges and the District Office (for example, Financial Aid, Admissions and Records, each of the academic departments, Human Resources, Business Services, General Services, the Los Rios Police Department, etc.).
- 1.4 Each operating unit within the District shall apply this Policy to meet information confidentiality and data security needs. The Policy is written to incorporate current technological advances. The technology installed at some operating units may limit immediate compliance with the Policy. Instances of non-compliance shall be reviewed with and approved by the Associate Vice Chancellor of Information Technology or the Dean of the Department responsible for Information Technology at each campus.

2.0 Purpose

- 2.1 Information security means protection of the District's data, applications, networks, and computer systems from misuse and unauthorized access, alteration, or destruction.
- 2.2 The purpose of this Information Security Policy and Regulation is:
 - 2.2.1 To establish a District-wide approach to information security.

- 2.2.2 To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of District data, applications, networks and computer systems.
- 2.2.3 To define mechanisms that protect the reputation of the District and allow the District to satisfy its responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- 2.2.4 To prescribe an effective mechanism to respond to external and internal complaints and queries about real or perceived non-compliance with this Policy.

3.0 Administrative Regulations

- 3.1 The Chancellor shall adopt administrative regulations regarding security.

LRCCD

Policy Adopted: 4/5/00
Policy Revised: 5/16/07; 12/15/10
Policy Reviewed:
Adm. Regulation: [R-8871](#)