Coast Community College District
BOARD POLICY
Chapter 3
General Institution

BP 3901 Electronic Information Security

References

BP 3720 Computer and Network Use
BP/AP 5040 Student Records, Directory Information, and Student Privacy
BP 6960 Identify Theft Preventions
California Information Practices Act, Civil Code §§ 1798 *et. seq.*

The District retains selective information in electronic form on employees, students, contractors, and other individuals who conduct business with the District. Certain types of information, if divulged publicly or to unauthorized individuals, could result in significant harm including financial loss, reputation damage, loss of credit standing, or other problems requiring extensive time and effort by the District to address. To protect electronic information, state and federal laws restrict how certain types of information can be stored, displayed, or transmitted through electronic networks and in information technology systems. Furthermore, some laws require disclosure when certain information is compromised or when information systems have been breached.

The District and its employees have an ethical and legal obligation to take necessary steps to protect the confidentiality, integrity, and accessibility of information that is stored electronically by the District. Additionally, the District recognizes its responsibilities to correct errors in electronic information, and to issue proper notifications of improper disclosures of personal information, including employee and student records.

The Board directs the Chancellor or designee to develop and implement procedures that will:

1. Enforce applicable federal and state laws, including those laws and regulations that are specific to electronic information security as well as those that apply to the protection of personal information, including employee and student records.

2. Employ best practices to safeguard the storage and transit of personal information across the District's information systems and digital networks.

3. Delineate processes for expeditiously investigating suspected breaches, thefts of computing systems, or inadvertent disclosures of personal information contained in District information technology systems. These processes shall also describe the appropriate follow-on actions to take to limit damage, secure compromised systems, and notify affected persons.

4. Employ best practices to ensure the on-going accessibility of the District's information systems including the Information Technology aspects of the District's Business Continuity and Disaster Recovery activities.

Adopted October 18, 2016
Reviewed June 21, 2023