FOOTHILL-DE ANZA
Community College District

Book	Board Policy
Section	Chapter 3 - General Institution
Title	Electronic Information Security
Code	BP 3260
Status	Active
Adopted	January 20, 2009

Foothill De-Anza Community College District ("District") retains selective personal information in electronic form on employees, students, contractors and other individuals who conduct business with the district. Certain types of personal information, if divulged publicly or to unauthorized individuals, could result in significant personal damage including financial loss, loss of credit standing, or other problems requiring extensive time and effort by the affected individual(s) to address. To protect personal information, state and Federal laws restrict how certain types of personal information can be stored, displayed, or transmitted through electronic networks and in information technology systems. Furthermore, some laws require disclosure when 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 all personal information that is provided to the District.

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

1. enforce all existing federal and state laws, including those laws and regulations that are specific to electronic information security as well as apply to the protection of personal information.

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.

See Administrative Procedure 3260 Electronic Information Security Procedures

Approved 1/20/09