SUBJECT:  Information Systems Security Planning
EFFECTIVE DATE:  June 1, 2020
BOARD POLICY REFERENCE: CS

PURPOSE
Develop policies and procedures for security planning.

PROCESS
Security Planning Policy and Procedures (PL-01)
The College District:

A. Develops, documents, and disseminates to information system owners:
   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management
   commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security planning policy and associated security
   planning controls; and
B. Reviews and updates the current:
   1. Security planning policy biennially; and
   2. Security planning procedures annually.

Security Planning Policy
The CISO must direct and coordinate the creation of a security plan protecting the information system
assets of the College District. The plan must address the information systems’ identification and classification,
owners, automated protection tools, network security, minimum levels of system security settings, security audit
process and frequency. In addition:

Security Plan (PL-02)
The College District:

A. Develops a security plan for the information system that:
   1. Is consistent with the organization’s enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business
   processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or
   connections to other information systems;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for meeting those requirements including a
   rationale for the tailoring and supplementation decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
B. Distributes copies of the security plan and communicates subsequent changes to the plan to information system owners
C. Reviews the security plan for the information system annually;
D. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
E. Protects the security plan from unauthorized disclosure and modification.

Rules of Behavior (PL-04)

The College District:

A. Establishes and makes readily available to individuals requiring access to the information system, the rules describing their responsibilities and expected behavior with regard to information and information system usage;
B. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
C. Reviews and updates the rules of behavior biennially; and
D. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.