EL PASO COMMUNITY COLLEGE PROCEDURE

For information, contact Institutional
Effectiveness: (915) 831-6740

CS-1 **Security of Centralized Computerized Administrative Data**

APPROVED: November 3, 1994 **REVISED**: September 1, 1995
Year of last review: 2021
AUTHORIZING BOARD POLICY: CS

Classification: Institutional
Responsible Vice President or Associate Vice President: Vice President of Information Technology/Chief Information Officer
Designated Contact: Director of Records Management

OBJECTIVE: To provide security control guidelines for centralized computerized administrative data.

PROCEDURE: To aid in securing all computerized administrative data stored at Information Technology (IT) central data processing facility from unauthorized access, the following guidelines have been developed.

I. The Director of Information Technology or designated representative will be responsible for securing all centralized computerized administrative data.

A. Data is defined as data necessary to support the administration of the District and supported by IT.

B. Data not meeting this definition must be secured by the appropriate area whether or not it is stored at the central site.

II. Access to the administrative data will be controlled on an individual password basis.

A. Passwords will be established and provided to each individual by IT.

B. Authorization for access to administrative data will be approved on an individual basis by the Vice President of the administratively responsible organization of the data.

C. This authorization will be in writing or sent through Email and will include relevant elements deemed necessary by IT.

III. When access, has be authorized, IT will provide the individual with the initial password(s) and will notify the Vice President of the authorizing organization(s) of this action.

IV. IT will maintain an overall security review to ensure all violations and attempted penetrations are identified. Appropriate action will be taken to preclude and eliminate any attempted breaches of security.

V. Authorizing organizations will inform IT of all changes in access authorization, i.e., employee terminations, new hires, changes in access level requirements.

VI. Each individual authorized access will be responsible for safeguarding their password(s) from disclosure and/or use by other individuals. Passwords should not be maintained in any written form.