POLICY 08:13:12
DATA ACCESS MANAGEMENT

I. Purpose

The purpose of this policy is to define the requirements for providing and revoking access to restricted and confidential college data to protect its security and integrity.

II. Scope and Applicability

This policy applies to all individuals who are provided an account or other access to confidential or restricted college data. By accessing college data, the user of the account agrees to comply with Policy 08:04:05 Information Technology Resources and 08:13:01 Information Technology Acceptable Use.

This policy applies to all computing resources and accounts owned and/or provided by the College and used for college-related activities that support the mission, goals and purposes of the College. Please also refer to Tennessee Board of Regents Policy No. Policy 1:08:00:00 and 1.08.03.00 (formerly G-051 & G-052).

III. Definitions

Confidential Data - Confidential data is not protected by state or federal law. However, its loss or unauthorized use could impair the college functions, cause significant financial or reputational loss or possibly lead to legal liability. The full definition and identification of confidential data can be found in Policy 08:13:13 Data Classification.

Data custodian - A data custodian is an administrator of a Pellissippi State office or division, or his or her designee, who may make data within their charge available to others for the use and support of college functions. A data custodian is responsible for the accuracy and completeness of data files in their areas and ensures the protection requirements are met before granting access to the data. The full definition and identification of data owner at the college can be found in the Data Standards Manual linked from the Institutional Effectiveness, Assessment and Planning site.

Data user - A member of the college community that has access to college data, and thus is entrusted with the protection of that data.

Principle of Least Privilege - Limiting access rights for users to the bare minimum permissions they need to perform their work.

Restricted Data - Restricted Data is defined as data, in any format, that is regulated by law or contract. The full definition and identification of restricted data can be found in Policy 08:13:13 Data Classification.

IV. Policy

Pellissippi State Community College will ensure the confidentiality, integrity, and availability of technology and data through the development and implementation of compliance standards which address security requirements and expectations for acceptable access to confidential and restricted data. These standards will follow industry-defined best practices in securing technology and data.

All systems and files that contain confidential or sensitive information must have a data custodian for each source; each department must identify all sources of confidential/sensitive information and assign a data custodian. The data custodian and the user share the responsibility of preventing unauthorized access to PSCC information systems. The data custodian will analyze user roles and determine the level of access required to perform a job function. The level of authorized access must be based on the principle of least privilege.

Access to applications and college information is granted based on an individual's relationship with the College and the individual's job responsibilities. Managing user account access is a continual process and vital to the security of information systems. Only authorized users should be allowed access to grant, review, deactivate, update, and/or terminate account access to information systems.

Managers will notify Information Services of internal personnel changes in job function, status, referral privileges, and/or affiliation. Human Resources will notify Information Services of all terminations and personnel transfers to different departments. Accounts will be disabled and/or deleted in accordance with Policy 08:13:02 Computer Accounts.

Access to an information system must be reviewed regularly. User authorization shall be reviewed and revised by the data custodian. At a minimum, the data custodian must review user access to the information system every twelve (12) months and address issues.

College employees and external parties may request access to College data (both quantitative and qualitative) in support of the College mission and goals. In order to be considered, data requests must adhere to all relevant state and federal laws (i.e.: FERPA, HIPAA) in their use and dissemination of data. For all external data requests and internal requests requiring confidentiality, only anonymized/de-identified data will be utilized and disseminated, unless approved by the president. All external data requestors must also complete a Confidential Data Request provided by the vice president of Information Services.

V. Enforcement

Failure to comply with this policy may result in temporary or permanent denial of access to computer or information technologies, or in some cases may result in college disciplinary action or legal action. Possible violations of this policy, other campus policies or illegal activity may have other disciplinary actions taken as listed in Pellissippi State Policy 08:13:01 Information Technology Acceptable Use. Disciplinary actions will conform with other college policies and may result in a disciplinary review conducted by the vice president of Student Affairs, or designee, in matters involving alleged violations by students, or by the director of Human Resources in matters involving employees of the College.

Reviewed/Recommended: President's Council, November 24, 2014
Approved: L. Anthony Wise, Jr., President, November 24, 2014
Reviewed/Recommended: President's Council, September 9, 2019
Approved: President L. Anthony Wise Jr., September 9, 2019