Pine Technical College

Policy and Procedure

Policy Number: 126
Date: April 5, 2010
Revision Date:
Division/Department: Administration
Author(s): Alison Holland

Subject: Data Integrity

Authorities: Bureau of Labor and Statistics Data Integrity Guidelines

Purpose: Ensure that the quality of the data produced is the highest quality and that staff are aware of the legal responsibilities a public body has for such high standards.

Policy:
The following guidelines must be followed by all Pine Technical College (PTC) program offices and PTC employees to ensure the integrity of information maintained and disseminated by PTC.

PTC information quality guidelines define "Integrity" as the security of information—protection of the information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification.

Confidential nature of PTC records

Data collected or maintained by PTC under a pledge of confidentiality shall be treated in a manner that will assure that individually identifiable data will be used only for statistical purposes and will be accessible only to authorized persons.

Authorized persons include only those individuals who are responsible for collecting, processing, or using the data in furtherance of statistical purposes or for the other stated purposes for which the data were collected. Authorized persons are authorized access to only those data that are integral to the program on which they work, and only to the extent required to perform their duties.

When non-PTC employees are granted access to confidential PTC data or Privacy Act data, they must be notified of their responsibility for taking specific actions to protect the data from unauthorized disclosure. The vehicle for providing this notification is the written contract or other agreement that authorizes them to receive the data. Accordingly, if a commercial contract, cooperative agreement, inter-agency agreement, letter of agreement, memorandum of understanding, or other agreement provides a non-PTC employee access to PTC confidential data or Privacy Act data, it must contain appropriate provisions to safeguard the data from

unauthorized disclosure. The authorization document will state the purpose for which the data will be used and that all persons with access to the data will follow PTC Policy 313 (Student Data Privacy) and will sign PTC's Affidavit for Non-Disclosure. These provisions are required whether the data are accessed on or off PTC premises. They also are required when access to the data may be incidental to the work conducted under the contract or other agreement (such as in systems development projects, survey mail-out processing, etc.).

Data collection

The integrity of PTC data collection process requires that all survey information be sound and complete. Data must be obtained from the appropriate college official or respondent and the data entries must accurately report the data and responses they provided. The administrative aspects of the data collection process, such as work time reported and travel voucher entries, must be factually reported. Therefore, employees must not deliberately misrepresent the source of the data, the method of data collection, the data received from respondents, or entries on administrative reporting forms.

Procedure:

Procedures for safeguarding confidential information

Department managers are responsible for implementing procedural and physical safeguards to protect confidential information from disclosure or misuse within their offices, including:

- Where appropriate and necessary, preparing written procedures for the handling and disposal of confidential data. Ensuring that all employees within their organizations are familiar with and understand these procedures.
- Ensuring that new employees are informed about the different types of confidential data maintained in their work areas and the special precautions that are to be taken with their use, storage, and disposal.
- Developing data collection instruments and collection methodology.
- Ensuring that commercial contracts, cooperative and inter-agency agreements, letters of agreement, and affidavit, which give non-PTC employees access to confidential data, contain the proper confidentiality- and security-related clauses.

Responsibilities:
All PTC employees are responsible for following the rules of conduct in the handling of personal information contained in the records covered under the Privacy Act of 1974.

Dissemination of news and data releases

Public information documents require manager-level approval. PTC offices also are required to consult the college President before instituting an automated process to disseminate news releases or other products to the public.

Data security

PTC and MnSCU have established appropriate computer security measures to safeguard PTC's data processing environment against destruction or corruption of data or systems, unauthorized disclosure of data, and loss of service. These security measures are part of an overall management control process that includes information technology (IT) security. The PTC Chief Information Officer is assigned overall responsibility for directing the application of such controls.

Dissemination:
This policy will be included in new staff hiring packet. Standard dissemination also applies.

Reviewed by Campus Roundtable: April 19, 2010; May 17, 2010

Reviewed by Faculty Shared Governance: N/A

Reviewed by Managers Meeting: N/A

Approved: May 17, 2010