CPTC Procedure: Software Installation

Overview
Allowing employees to install software on company computing devices opens the College up to unnecessary security and legal exposure. Conflicting file versions can prevent programs from running. User software installation can lead to unintentional or intentional introduction of malicious software code. In addition, unlicensed software that was installed without a proper license or not in accordance with license agreements could expose the employee and/or the College to legal repercussions. Malicious software disguised as legitimate software can be used to compromise the organization's network and data. All of these are just some of the examples of problems that can be introduced when employees install software on college equipment.
Note: this procedure is a derivative of a section of the TCSG Security Guidelines. Any changes or differences in the TCSG document will supersede the CPTC procedure.

Purpose
The purpose of this procedure is to minimize the risk of loss of program functionality, loss of system stability, the exposure of sensitive information contained within Coastal Pines Technical College's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

Scope
This procedure covers all software as well as all computers, servers, tablets, smartphones, networking infrastructure devices, and other computing devices operating within Coastal Pines Technical College.

Procedural Guidance
Employees may not install software on Coastal Pines Technical College's computing devices. Software requests must first be approved by the requester's manager and then be made to the IT department or Help Desk in writing or via email. Final decision will be made by the College information security administrator (ISA) designated by TCSG. Employees may appeal to the College President to overturn the decision of the ISA.

Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

Penalties
Violations of these policies incur the same types of disciplinary measures as violations of other CPTC policies or state or federal laws, including criminal prosecution.

Responsibility
The Executive Director of Information Technology has the overall responsibility for ensuring this procedure is implemented.

Adopted: May 20, 2020
Revised: September 19, 2023