Software Licensing Policy

Summary

To help fulfill its mission, Columbus State University utilizes a large variety of software packages. Faculty, staff, and students have access to campus-wide packages such as word processors, as well as specialized departmental applications.

U.S. law expressly forbids unauthorized duplication or use of copyrighted software. Enforcing those laws protects the integrity and reputation of CSU.

Purpose

This purpose of this policy is to ensure that all software installed on campus is appropriately licensed and used in accordance with individual license agreements.

Policy

- CSU must purchase valid licenses for all software installed on university computers and UITS must approve those purchases.
- Users may not install personal software on CSU computers. CSU must own the license.
- Users may not install CSU software on personally owned computers, unless allowed in the license agreement.
- Users may not duplicate copyrighted software unless otherwise provided for in the license agreement, and for backup and archival purposes.
- Users may request the installation of Freeware and Shareware as it relates to their job function.
- CSU must maintain an asset inventory and provide a secure repository for all media, licenses, and other documentation.

Procedures and Responsibilities

- User should submit an eQuest request for all software purchases, including upgrades.
- Upon delivery, the user should submit an eQuest request for installation. Users may not install the software themselves.
- UITS is responsible for installing the software and depositing the media, licenses, and other documentation in a secured fireproof cabinet.
- To ensure compliance, UITS is responsible for conducting periodic, random assessments of CSU software and computers.
- Users are accountable for any unlicensed software found on their computers.

Related USG Policy

4.1 (IT Handbook) Technology Procurement Approval Process & 5.1 (IT Handbook) USG Information Security Program & 5.4 (IT Handbook) USG Information Asset Management and Protection Standards

Last Update

2/4/2014

Responsible Authority

Chief Information Security Officer