TEXAS A&M **INTERNATIONAL** UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.20 Authorized Software/Hardware

First Approved: March 28, 2013
Revised: June 22, 2017
Next Scheduled Review: June 22, 2022

Procedure Statement and Reason for Procedure

End-user license agreements are used by software and/or hardware and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable laws. More importantly, installation of any software and/or use of any hardware must have a justifiable business purpose and must be properly licensed.

The purpose of this SAP is to establish the procedures for licensed software and hardware use on Texas A&M International University (TAMIU) Information Resources. It applies to all individuals who use TAMIU Information Resources. This SAP supplements *TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities* and *TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources*.

Procedures and Responsibilities

1. Requirements

1.1 All software or hardware installed on TAMIU-owned or operated computer systems and networks must be appropriately licensed.

1.1.1 Software and hardware must be used in accordance with licenses agreement, contract agreements, and applicable copyright laws. Those installing or authorizing the installation of such should be familiar with the term of such agreements and laws. Where feasible, such agreements should be maintained in the department that operates the hardware or the system on which the software is installed.

1.1.2 In cases where this is not feasible, individuals or departments should maintain sufficient documentation (e.g., End User License Agreements, purchase receipts, etc.) to validate that the software or hardware is appropriately licensed.

1.2 Third party copyrighted information or software that TAMIU does not have specific approval to store and/or use must not be stored on TAMIU systems or networks. System administrators will remove such information or software/hardware unless proof of authorization from the rightful owner(s) is provided.

1.3 In instances where the department is the owner-custodian or custodian of the system hosting the software or hardware, the department is responsible for ensuring compliance with this SAP.

1.4 The use of limited-license software is tracked and protected to control unauthorized copying and distribution. OIT will randomly perform scans to ensure license compliance and that only approved software or hardware exists.

1.5 Software or hardware purchased with personal funds may not be installed on TAMIU computers or networks without prior authorization from OIT.

1.6 Software or hardware purchased with TAMIU funds may not be installed on non-TAMIU systems or networks without prior authorization from OIT.

1.7 TAMIU provides site licensing for certain software (e.g., Microsoft Office, MS operating systems, STATA, etc.) Limited licensed software purchased by TAMIU departments will be installed once the license is provided.

1.8 All files downloaded from the Internet must be scanned for viruses using the approved OIT virus detection software.

1.9 Privately purchased, shareware, or freeware software will not be installed until proof of ownership is supplied and a review is performed. If the software is deemed a security risk or duplicates the functionality of an existing, approved software or hardware, the software will not be installed. The use of peer-to-peer software is not approved without prior permission from OIT. For a current list of TAMIU's authorized and supported software, please refer to the OIT website at: http://oit.tamiu.edu.

Related Statutes, Policies, Regulations, or Rules

Texas Administrative Code 202, Subchapter C – Information Security Standards for Institutions of Higher Education

TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources

TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities

Appendix

References:
Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Office of Information Technology, 956-326-2310