Texas A&M University System Standard - Authorized Software

Standard Statement

This standard is intended to inform System Offices (SO) computer users of the rules for authorized software on SO information resources.

Definitions

Information Resources (IR) - the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Software - a computer program, which provides the instructions which enable the computer hardware to work. System software, such as Windows or MacOS, operate the machine itself, and applications software, such as spreadsheet or word processing programs, provide specific functionality.

Information Resource Owner - an entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Responsibility

1. GENERAL

   Authorized software, also called licensed software, is any software that is acceptable for use within the SO. Software licensed for use at the SO has end-user license agreements which inform employees and agents of their responsibilities as end users regarding authorized use of the software. This procedure is intended to inform SO computer users of the requirements for authorized software on SO information resources.

   Non-compliance with copyright laws regarding software is subject to significant civil and criminal penalties imposed by federal and state laws. These penalties are applicable to the SO and/or an individual. Violation of this standard is subject to SO disciplinary action as well.

2. APPLICABILITY

This Standard Administrative Procedure (standard) applies to all SO information resources.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*. The intended audience is users of SO information resources.

3. STANDARDS

3.1 All software installed on SO owned or operated computer systems used by SO employees and agents in the conduct of SO business must be appropriately licensed.

3.1.1 For software having a licensing agreement, persons installing, or authorizing the installation of software should be familiar with the terms of the agreement. Where feasible, the licensing agreement should be maintained in the department that operates the system on which the software is installed or through a license management agreement with a third party (e.g., SELL).

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

3.2 No software may be copied or installed by any SO employee or agent unless the licensing agreement specifically grants such a procedure.

3.3 Each department will be asked to report the status of their compliance as part of the annual risk assessment process (refer to Rule 29.01.99.S1).

3.4 For instances in which the department is the owner-custodian or custodian of the system hosting the software, the department is responsible for ensuring compliance with this standard.

Supplements

System Policy 07.01, Ethics
System Regulation 29.01.02, Use of Licensed Commercial Software
SO Rule 29.01.99.S1, Security of Electronic Information Resources
SO Rule 29.01.99.S2, Rules for Responsible Computing

Contact Office

Contact The Texas A&M University System Chief Information Officer for interpretation or clarification of this standard.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer