The Division of Information Technology
University Information Security Standards

Information Security Standard – Authorized Software (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

Authorized software, which also includes Software as a Service (SaaS) or any cloud-based software, approved by the Chief Information Officer (CIO).

Software licensed for use at West Texas A&M University has end-user license agreements, which protect intellectual assets and inform faculty, staff, and students of their rights and responsibilities under existing intellectual property laws. This procedure is intended to inform University computer users of the rules for authorized software on University information resources.

2. Applicability

This standard applies to all University information resources.

The purpose of this standard is to provide a set of measures that will mitigate information security risks associated with Authorized Software. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer (ISO).

The intended audience is users of University information resources.

3. Definitions

3.1 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic

data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.2 Software: A computer program, which provides the instructions, which enable the computer hardware to work. System software, such as Windows or Mac OS, operate the machine itself, and applications software, such as spreadsheet or word processing programs, provide specific functionality.

3.3 Owner of an Information Resource: an entity responsible:

(1) for a business function (Department Head); and,

(2) for determining controls and access to information resources

4. Procedures

4.1 System Regulation 21.99.10, Use of Licensed Commercial Software guides the procedures for appropriate use of authorized software for all University users of University information resources.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer