A. Install on agency computers only that software which is licensed to or owned by the agency and the license covers installation on the employee's specific computer.

B. Copy software only if authorized by the specific license agreement governing that software.

C. Install on agency computers only software which has a business or computer maintenance purpose.

D. Maintain documentation, original media, or other forms of evidence necessary to demonstrate that software installed on agency computers is properly licensed for the specific machines on which it is installed. For example, documentation or media could be stored in a binder, pocket file folder, zip lock bag, or other such storage device, and kept in the immediate vicinity of the computer. IT support personnel reserve the right to remove any unlicensed software from any computer system. If such action is taken, the support person will notify the employee and respective supervisor.

14.0 INFORMATION RESOURCES PROJECT MANAGEMENT

14.1 Information technology projects must utilize project management practices in accordance with Texas Administrative code Ch. 216, Subch. C, Project Management Practices for Institutions of Higher Education and AgriLife Research Project Management Framework.

14.2 Projects that meet the state's definition of a major information technology project will be reported to the state in accordance with Texas Administrative code Ch. 216, Subch. C, Project Management Practices for Institutions of Higher Education.

DEFINITIONS

Owner of an information resource—A person responsible for a business function and for determining controls and access to information resources supporting that business function. For example, the owner is typically the unit head, director, or their designee.

Custodian of an information resource—A person responsible for implementing owner defined controls and access to an information resource. Custodians may include state employees, vendors, and any third party acting as an agent of, or otherwise on behalf of the state entity. For example, the custodian is typically an IT manager or resource.

User of an information resource—An individual or automated application authorized to access an information resource in accordance with the owner defined controls and access rules.

Confidential data—Data that is excluded from disclosure under requirements from federal or state law. This can include, but is not limited to: personnel records, health records, financial records, address information, student education records, credit card, social security, or drivers' license numbers.

Sensitive data—Sensitive data may be subject to disclosure or release under the Texas Public Information Act, however the agency has decided that the data must have the same or equivalent level of protection as confidential data. Examples of sensitive data include: operational information, personnel records, information security procedures, and internal communications.

Mission critical—Data, which if access to was unavailable, an essential mission of TAMU, the agency, or department would not be able to be continued, and or would cause a significant financial loss to be incurred, would cause institutional embarrassment to take place, would cause an inability to comply with federal regulations or legal obligation, or could cause a possible closure of an agency or University department.

Portable computing device—Any device other than a desktop computer that can store data, access the Internet or AgriLife networks, email systems or applications. Examples include notebook computers, internet enabled phones, net book computers, and portable memory devices such as USB drives and memory sticks.

RELATED STATUTES, POLICIES, OR REQUIREMENTS

1 Texas Administrative Code Ch. 202, *Information Security Standards*

1 Texas Administrative Code Ch. 206, *State Websites*

1 Texas Administrative Code Ch. 213, *Electronic and Information Resources*

A&M System Policy 29.01, *Information Resources*

A&M System Regulation 10.02.01, *Fraud, Waste, and Abuse*

A&M System Regulation 29.01.03, *Information Security*

Copyright Law of the United States

A&M System Regulation 29.01.02, *Use of Licensed Software*

AgriLife Form AG-415*, Employee Acknowledgment*

CONTACT OFFICE

For interpretation or clarification, please contact AgriLife Information Technology at 979-985-5737.

REVISION HISTORY

Approved: July 3, 1998
Revised: August 25, 2003
February 10, 2005
September 13, 2007
March 31, 2010
August 1, 2011
August 24, 2012
September 12, 2014
January 23, 2017
August 22, 2018
February 5, 2020

Next Scheduled Review: February 5, 2025