Computer Use and Responsibilities

Information Technology

Purpose

This document outlines requirements for computer use and responsibilities of the employee in order to protect University information resources. These requirements must be followed as documented to protect University systems and data from unauthorized access or misuse. Please refer to the TAMU Standard Administrative Procedure SAP 29.01.03.M0.02 Rules for Responsible Computing and SAP 29.01.03.M1.17 Information Resources – Privacy.

Scope

This document covers all full-time and part-time employees, contract workers, consultants, temporary workers, and other personnel granted access to University systems, networks, software, and/or data.

Protecting University Data

As an employee of the University you need to be aware of the types of data that you need to protect. Misuse or exposure of this data can lead to damage to the University's reputation, loss of funding and fines.

Some types of data you need to protect are (but not limited to):

- Social Security Numbers
- Credit Card Numbers
- Student Records (Any combination of data that allows identification of student – Grades, DOB…)
- Protected Health Information (Any health related information, medical conditions, diagnoses…)
- Controlled Research Information

Always follow the rule: **If in doubt, protect it.**

Equipment

Equipment covered by this document includes (but is not limited to):

- Desktops, laptops, and tablet computers
- Smartphones (defined as any cellular telephone that connects to the internet via Wi-Fi or a mobile provider network)
- Flash, memory, and/or thumb drives
- External hard disks

University Issued Computing Devices

All employees will be assigned a University issued computing device(s) for use in carrying out University business. It is ***RECOMMENDED*** that the University issued device(s) will be used for ***ALL*** University business. These devices will have information security software installed to allow the University to ensure the device and data on the device are protected to the best ability of the available protection methods.

ALL portable devices will be encrypted.

These devices will, where permitted by the computing device:

- Be added to the TAMUG Domain
- Have the current University approved and supplied end point protection software installed
- Have Administrative Rights removed to stop malware from being able to control the device
- Be encrypted if it is a portable device or desktop that contains sensitive information
- Have end point patch and remote management agent installed
- Have sensitive information scanning software installed

Privacy (Information Resources – Privacy SAP 29.01.03.M1.17)

The University has the right to examine information on information resources which are under the control or custody of the University. The general right to privacy is extended to the electronic environment to the extent possible.

However, there should be no expectation of privacy beyond that which is expressly provided by applicable privacy laws. Privacy is limited by the Texas Public Information Act, administrative review, computer system administration, and audits.

University Supplied Software

Subject to software specific Licensing Agreements, ***University Supplied Software*** will only be installed on University issued devices.

User Responsibilities

The employee (all full-time and part-time employees, contract workers, consultants, temporary workers, and other personnel granted access to University systems, networks, software, and/or data) is responsible for any and all University data saved to their University issued device.

- The employee should not attempt to change or disable any security settings applied to the device by the Information Technology department.
- In the event that a user believes a University issued device that is authorized to connect to the University's resources, systems, or networks might be compromised, they must immediately notify the Information Technology department in writing of the potential security risk.
- If a user loses or misplaces a University issued device that is authorized to connect to the University's resources, systems, or networks, they must immediately notify the Information Technology department in writing of the potential security risk.
- Whenever an employee decommissions, prepares to return, or otherwise ceases using a University issued device, the employee must notify the Information Technology department that the device will no longer be used to connect to University resources, systems, or networks.