TEXAS A&M INTERNATIONAL UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.32 Personal Devices on University Networks (BYOD)

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

Procedure Statement and Reason for Procedure

TAMIU has the responsibility of safeguarding information entrusted to it. With the proliferation of smart devices in the consumer market, the workplace has seen a steady increase in their use among employees. By providing mobility, employees find the practicality of navigating and performing work-related tasks while using their devices essential to productivity. If accessing TAMIU sensitive data, the device must be secured by following specific policies.

This SAP establishes a TAMIU-wide process for safeguarding TAMIU Information Resources on user-owned devices (BYOD – bring your own device). It applies to all users of 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. Personal Devices on TAMIU Networks (BYOD)

    1.1 By connecting a non-TAMIU owned device, the individual user is responsible for any TAMIU information residing on the device and any potentially accessible information resulting from stored credentials in the personal computing device.

        1.1.1 If a lost or stolen device is believed to contain TAMIU data, the user must notify the Office of Information Technology (OIT) and the University Police Department (UPD) as soon as possible. UPD is available 24 hours a day, 365 days a year.

1.1.2 If a lost or stolen device is believed to contain (or has the potential to contain) confidential information as defined in *TAMIU SAP 29.01.99.L1.31, Information Classification*, the device may be completely wiped at the discretion of OIT. A complete wipe would mean the total erasure of TAMIU and personal data.

1.1.3 The use of an employee device for State business purposes may require the employee to surrender information contained on the device to respond to open records requests.

1.1.4 Email synchronization will be supported through encryption-enabled protocols.

1.1.5 A strong password or PIN should be set on personal devices utilizing email synchronization.

1.1.6 All remote access to confidential information with personal computing devices should utilize encryption techniques that secure wireless transmission (e.g., VPN, SSL, etc.)

1.1.7 Personal devices are not supported by OIT. Users should contact the device manufacturer or their carrier for operating system or hardware-related issues.

1.1.8 Personal devices must follow the same TAMIU rules and standard administrative procedures as TAMIU-owned devices.

1.1.9 At TAMIU's discretion, personal devices may be blocked from accessing certain websites during work hours/while connected to the TAMIU network.

1.1.10 At TAMIU's discretion, personal devices may be blocked from accessing all or part of TAMIU Information Resources.

1.1.11 TAMIU reserves the right to monitor the location of the personal computing devices containing TAMIU data. While on TAMIU premises, TAMIU may record time and position of the personal computing device.

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