TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

Tuskegee University
Office of Information Technology
Mobile Device Acceptable Use Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to use a private or Tuskegee University provided mobile device that can access the University's electronic resources. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

Laptop/notebook
Tablet computers such as iPads
Mobile/cellular phones
Smartphones
PDAs

Any mobile device capable of storing data and connecting to an unmanaged network. The goal of this policy is to protect the integrity and confidential data that resides within Tuskegee University's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to the University's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Tuskegee University's direct control to backup, store, and otherwise access data of any type must adhere to a Tuskegee University defined processes for doing so.

Applicability

This policy applies to all Tuskegee University Faculty, full and part-time Staff, Contractors and other agents who utilize either Tuskegee-owned or personally-owned mobile device to access, store, back up, relocate or access any resources or information. Such access to the University's resources or information is a privilege, not a right. Consequently, employment at Tuskegee University does not automatically guarantee the initial and ongoing ability to use these devices to gain access to the University networks and information.

The policy addresses the following threats:

Loss - Devices used to transfer or transport work-related files could be lost or stolen.
Theft - Sensitive University data is deliberately stolen and/or sold by an employee.
Copyright - Software copied onto a mobile device could violate licensing.
Malware - Viruses, Trojans, Worms, Spyware and other threats could be introduced via a

mobile device.

Compliance - Loss or theft of financial and/or personal and confidential information/data could. expose the college to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of the office of the CIO. Unauthorized and unmanaged use of mobile devices to back up, store, and otherwise access any University related information/data is strictly forbidden. This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the Tuskegee University network.

Policy and Appropriate Use

It is the responsibility of any Faculty or Staff member of Tuskegee University who uses a mobile device to access resources, to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct University business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

Access Control

1. The office of the CIO reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to the Tuskegee University network infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the University's systems, data, students, staff and faculty at risk.

2. Prior to initial use on the Tuskegee network or related infrastructure, all mobile devices must be registered with IT and such device have mobile management software installed on it. The IT will maintain a list of approved mobile devices and related software applications and utilities as needed. Devices that are not on this list may not be connected to the University's network infrastructure. Although IT currently allows only listed devices to be connected to network infrastructure, it reserves the right to update this list in the future.

3. End users who wish to connect such devices to non-college network infrastructure to gain access to college data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT department such as updated software, anti-virus software, and personal firewalls. Tuskegee data is not to be accessed on any hardware that fails to meet Tuskegee University's established IT security standards.

All mobile devices attempting to connect to the Tuskegee University network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by the IT department. Devices that have not been previously approved by IT, are not in compliance with IT's security policies, or represent any threat to the Tuskegee computer network or data, will not be allowed to connect. Laptop computers or personal PCs may only access the Tuskegee computer network using a Virtual Private Network (VPN) connection that is authorized by their supervisor.

Security

1. Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password. See the Tuskegee University password policy for additional details. Employees agree to never disclose their passwords to anyone.

2. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain University data. Any off-site computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by the IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

3. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Tuskegee University's overarching security policy.

4. Faculty, Staff, contractors and Vendors will follow all Tuskegee University-sanctioned data removal procedures to permanently erase only Tuskegee- specific data from such devices once their use is no longer required.

5. In the event of a lost or stolen mobile device it is incumbent on the user to report this to IT immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re- provisioning.

6. Faculty, Staff, Contractors and Vendors will make no modifications of any kind to Tuskegee-owned and installed hardware or software without the approval of the Office of the CIO. This includes, but is not limited to, any reconfiguration of the mobile device.

7. The Office of the CIO reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the Tuskegee computer network.

Organizational Protocol

The Office of the CIO can and will establish audit trails relating to Tuskegee-owned data and these will be accessed and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to the Tuskegee University's networks may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains Tuskegee University's highest priority.

Policy Non-Compliance

Failure to comply with the Mobile Device Acceptable Use Policy may, at the full discretion of the University, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.