

TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

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 the University network are followed. 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.

TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

Organizational Protocol

The Office of the CIO can and will establish audit trails relating to Tuskegee 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 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.