Mobile Devices Policy

Policy #: TC-ITS-185 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.4 **Effective Date**: May 30, 2015

Accountability & Responsibility

This policy is governed by the accountability and responsibility section found here.

Purpose

The purpose of this policy is to address the appropriate protection of sensitive electronic information (SEI) when it is stored, transferred, or accessed on mobile devices such as the following: laptops, smartphones (devices with operating systems), tablets, or removable media (USB flash drives, memory cards, floppy disks, CDs, DVDs, and so on). This policy is not intended to address non-classified data.

Policy

It is the policy of Travis County to implement reasonable safeguards while using mobile devices. These safeguards relate to protecting confidential information, equipment security, and security of data.

Procedure(s)

General Guidance

Cell phone conversations **(Confidential Information)**

- All mobile and portable device users must hold SEI in confidence and in accordance with the HIPAA Privacy Rule, HIPAA Security Rule, the HITECH Act, CJIS, Texas State Law, as well as the terms of the Employee Confidentiality Agreement, and all Travis County policies and procedures.
- Protected SEI and other confidential information may only be read, taken, used, copied, or discussed in conjunction with the direct performance of the user's duties.
- Any violation of this policy or unauthorized use or disclosure of patient information will result in Travis County taking appropriate HR and/or legal action against the user.

Security of the Equipment

- Mobile and removable devices must be serviced on a timely basis. An employee must never attempt to repair any device or authorize repairs by any third party.
- Stolen or misplaced Travis County or third-party owned mobile devices which access the Travis County network must be reported immediately to the ITS Service Desk. All passwords will immediately be changed to prevent unauthorized access.

Security of Data

- It is the responsibility of the employee to adhere to all Travis County policies and procedures regarding the appropriate access, use, storage, and disposal of SEI on devices.
- Regular backups should be performed on devices to ensure information is protected from device failure. Questions regarding appropriate backup processes and technology should be forwarded to the ITS Service Desk.
- SEI residing on a device must be encrypted and password-protected where appropriate.

Policy Revision

Version	Purpose/Changes	Editor	Date
1.0	Travis County Information Technology Services Information Security Policies Creation	Randy Lott	05/30/2015
1.1	Removed "In order to access Travis County-owned information systems and services on a mobile device, only Travis County approved Mobile Device Management (MDM) or Enterprise Mobile Management (EMM) software must be installed on any mobile device" from Policy section. Remove from Security of Data section:	ITS Policy Committee	05/03/2016

Version	Purpose/Changes	Editor	Date
	• All information contained in the MDM/EMM software that is present on a mobile device is the property of Travis County and may be wiped without permission or notice by the Travis County ITS department. • Stolen or misplaced devices will have all information and contents in the MDM/EMM software wiped from the device's storage areas.		
1.2	Removed "It is the employee's responsibility to ensure that the media used to back up a device is secured, protected and disposed of according to established policies." from Security of Data.	ITS Policy Committee	7/15/2016
1.3	Updated name of CIO	Randy Lott	12/18/2017
1.4	Updated policy number from 314 to 185 and updated approver's title.	Joyce Miller	11/20/2019