Travis County Technology & Security Policies

Encryption Policy

Policy #: TC-ITS-160 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.5 **Effective Date**: May 30, 2015

Accountability & Responsibility

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

Purpose

The purpose is to implement a security measure to encrypt sensitive information in transit whenever deemed appropriate and the information is not improperly modified without detection.

Policy

Travis County will evaluate the need for and use of encryption to maintain the confidentiality and integrity of sensitive information, including but not limited to, ePHI, PII, or CJI, being transmitted over a network.
ePHI, PII, or CJI and other sensitive electronic information should be encrypted to avoid unauthorized disclosure and access. Encryption may also be utilized in combination with other access controls where indicated by risk analysis.

Procedure(s)

General

1. Travis County will identify systems that require ePHI, PII, or CJI and other sensitive electronic information to be encrypted.
2. Travis County will identify members of the workforce who require encryption capabilities.
3. Travis County will review the viability of securing ePHI, PII, or CJI and other sensitive electronic information on critical databases, file servers, and on mobile devices such as laptops, smartphones, and portable flash drives.
4. Travis County key length requirements will be reviewed and upgraded as technology allows. All keys generated should be securely escrowed.
5. Travis County will evaluate encryption capabilities of products and systems to ensure proper functionality.

Transmissions

1. To appropriately guard against unauthorized access to or modification of ePHI, PII, or CJI and other sensitive information that is being transmitted from Travis County networks to a network outside of such networks must use an encryption mechanism between the sending and receiving entities to ensure that such transmissions are not easily intercepted and interpreted by parties other than the intended recipient.

2. When transmitting sensitive information via removable media, including but not limited to, CDROM, memory cards, magnetic tape and removable hard drives, the sending party must use an encryption mechanism to protect against unauthorized access or modification.

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	Combined Encryption Policy: HIPAA (309) into this policy. Renamed from Encryption and Decryption policy to Encryption Policy.	ITS Policy Committee	07/06/2016
1.2	Combined Transmission Security Policy (318) into Transmission section first item.	ITS Policy Committee	09/09/2016
1.3	Merged Integrity Controls Policy (311) into this policy. Updated #5 in policy from test to evaluate.	ITS Policy Committee	09/28/2016
1.4	Updated name of CIO	Randy Lott	12/18/2017
1.5	Updated policy number from 308 to 160 and updated approver's title.	Joyce Miller	11/20/2019