Chapter 135. Information Technology and Systems[1]

Contents:

Subchapter A. General Provisions of Chapter

135.001 Authority 1
135.002 Intent of Chapter 1
135.003 Application 1
135.004 Effective Date 1
135.005 Definitions 1
135.006 Information Systems Technology Standards Document and Demonstrations 2
(135.007 - 135.013 Reserved for Expansion) 3

Subchapter B. Information Technology Security Policies Program

135.014 Intent of Subchapter B 3
135.015 Information Systems Security Policies 3
135.016 Information Systems Security Designee 3

Subchapter A. General Provisions of Chapter

135.001 Authority

The Travis County Commissioners Court adopts this chapter under the authority of the laws of the State of Texas.

135.002 Intent of Chapter

The purpose of Chapter 135 is to provide policies for management of certain information technology and systems.

135.003 Application

This chapter applies to all Information Systems managed by the Chief Information Officer. It does not apply to Information Systems managed by an Elected Official outside of the Commissioners Court unless that Elected Official adopts this chapter in writing.

135.004 Effective Date

This chapter becomes effective on the date the Commissioners Court adopts it.

135.005 Definitions

In this chapter:

[1] Chapter 35 was adopted by Travis County Commissioners Court on May 3, 2016, Item #19, and renumbered June 1, 2018 (approved May 15, 2018 Item 7).

(1) "Chief Information Officer" means the department head of the Travis County Information Technology Services Department.

(2) “Information Systems” means an interconnected set of information resources under the same direct management control that shares common functionality. It includes hardware, software, information, data, applications, communications, and people.

(3) “Information Systems Security” means the protection of Information Systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

(4) “Information Systems Security Policies” means policies that maximize to the greatest practical extent the County’s Information Systems Security in a manner that minimally complies with all State and Federal rules and regulations related to Information Systems Security for the County.

(5) “Information Systems Standards Document” means a document that provides a baseline that an Elected Official or County Department will use to establish and review its Information Systems architecture for the purposes of an Information Systems procurement, to the extent that such Information Systems are managed by the Chief Information Officer. The document will contain minimum technical requirements an Elected Official or County Department’s Information Systems will possess to be compatible with Information Systems managed by the Chief Information Officer.

135.006 Information Systems Standards Document and Demonstrations

(a) The Information Technology Services Department (ITS) will solicit input from all Elected Officials and County Departments in advance of identifying appropriate technological standards for Information Systems and prepare the Information Systems Standards Document no later than February 28 of each year. An Elected Official or County Department may challenge the document’s contents but must bring the challenge to the Commissioners Court no later than the fourth regularly scheduled Commissioners Court meeting following the date of the document’s publication.

(b) An Elected Official or County Department may arrange for any demonstration or trial use of computer hardware, software, or other technical products and services. An Elected Official or County Department may not, however, install or implement any trial Information Systems, without written approval from the Chief Information Officer or the officer’s designee, to the extent such demonstration or trial use will use Information Systems managed by the Chief Information Officer.

(135.007 - 135.013 Reserved for Expansion)

Subchapter B. Information Technology Security Policies Program

135.014 Intent of Subchapter B

The County is exposed to certain security risks while leveraging Information Systems to efficiently and effectively conduct the County's business. The Commissioners Court has determined that it is in the best interests of County and its residents to establish and maintain Information Systems Security Policies that provide a framework within which the County establishes required levels of Information Systems Security and define security accountability, network and system service, incident handling and response, and acceptable use and security training.

135.015 Information Systems Security Policies

Subject to applicable budgetary restrictions, the Chief Information Office will create and implement the Information Systems Security Policies.

135.016 Information Systems Security Designee

If a State or Federal rule or regulation requires a County Employee to be designated as being responsible for County Information Systems Security or any part of it, the Chief Information Officer is so designated for the Information Security Systems that the Chief Information Officer manages. The Chief Information Officer may also serve as the designee for any Elected Official or County Department that wishes to designate the Chief Information Officer in this capacity.