



# Travis County Technology & Security Policies

## Data Backup Policy

**Policy #:** TC-ITS-130  
**Version #:** 1.3

**Approved By:** Paul Hopingardner, County Executive, Technology & Operations  
**Effective Date:** May 30, 2015

### Accountability & Responsibility

This policy is governed by the accountability and responsibility section found [here](#).

### Purpose

The purpose is to establish and implement procedures to create and maintain retrievable exact copies of sensitive information and ensure appropriate secure storage in the event of equipment failure or damage.

### Policy

Travis County will create and maintain exact, retrievable copies of sensitive information and ensure that backup media is periodically tested to ensure suitable quality and reliable data restoration.

Travis County will ensure that sensitive information is backed up to disk, tape, other storage technologies, or a combination of those technologies on a regular basis to minimize the loss of data in the event of an incident or disaster.

### Procedure(s)

In developing the backup schedule, the Chief Information Officer (CIO), or their designee, will consider factors such as the following:

- What data (systems, files, directories, and folders) should be backed up
- How frequently data should be backed up
- Who is responsible/authorized to retrieve the media
- Test the copy of the data to make sure the copy of the data is exact and retrievable

A backup schedule should include incremental backups and should include transportation to and storage at a third-party vendor off-site secure location.

### 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	Merged Data Backup and Storage Policy (203)	ITS Security Policy Group	08/19/2016
1.2	Updated name of CIO	Randy Lott	12/18/2017
1.3	Updated policy number from 110 to 130 and updated approver's title.	Joyce Miller	11/20/2019