



Travis County Technology & Security Policies

Multi-Factor Authentication Policy

Policy #: TC-ITS-186
Version #: 1.2

Approved By: Paul Hopingardner, County Executive, Technology & Operations
Effective Date: November 26, 2019

Accountability & Responsibility

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

Purpose

The purpose of this policy is to define requirements for multi-factor authentication. These standards are designed to minimize the potential security exposure to Travis County resources from damages which may result from unauthorized use. Multi-factor authentication adds a layer of security which helps deter the use of compromised credentials. Multi-factor authentication is recognized as an industry best practice in preventing unauthorized access to an institution's enterprise accounts, financial, operational, and academic systems.

Scope

This policy applies to all authentication administered throughout the Travis County network, whether centrally managed by Information Technology Services (ITS), managed by a designated technology service provider, or departmentally managed. This policy applies to all individuals and entities who are authorized to access the County's network's information systems and data.

Definitions

Multi-factor Authentication (MFA) involves combining more than one authentication type and generally provides a stronger assurance of the person's identity.

Two-factor authentication is combining only two authentication types (2FA).

Policy

Travis County has implemented multi-factor authentication for access to controlled and confidential data. Please refer to TC-ITS-402, Data Classification Policy.

Any user that is designated a system administrator, has privileged access to Travis County technology, or otherwise meets the criteria of high risk as assigned by the Chief Information Security Officer (CISO) shall also be required to enroll in multi-factor authentication and may not be eligible for exemption from this policy.

Exemption

Travis County users that wish to apply for exemption from the multi-factor authentication policy have to provide justification to the CISO.

Not all requests will be granted unless there is an individual need that supersedes the needs of the protection of the Travis County data and its technology systems.

Important

Any technology system connected to the Travis County network must apply the appropriate authentication and access controls to prevent unauthorized access to the County's administrative, operations and systems and data.

Those users, system owners and administrators that are noncompliant with this policy are subject to being prevented from connecting to systems that require multi-factor authentication, thereby potentially impacting their ability to perform work functions and access their own employee-related records.



Travis County Technology & Security Policies

Policy Revision			
Version	Purpose/Changes	Editor	Date
1.0	Travis County Information Technology Services Information Security Policies Draft Creation	Paul Knight	February 22, 2019
1.1	Reviewed by ITS Policy Committee.	ITS Policy Committee	April 5, 2019
1.2	Update of name and title of approver	Brandon Rogers	November 7, 2019