Remote Access Policy

Policy #: TC-ITS-210 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.8 **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 define how Travis County controls Remote Access to the County's information systems and networks in order to prevent unauthorized use.

In order to protect the network and data infrastructure of the County, all Travis County-owned computers have the ability to connect to the County's network via a remote access solution. This solution provides protection to the computer and its Internet connection by using the County's firewall and give the user the ability to access sensitive internal resources while on a public Internet connection.

This service is intended to extend the work environment for mobile employees beyond the physical boundaries of the campus in order to provide a more flexible working environment. However, in order to provide this level of flexibility, it is necessary to take appropriate security precautions.

Scope

This policy applies to all Travis County employees, contractors, and any other agents who remotely connect to the County's computing resources, other than those available on the public Internet.

This policy also applies to all devices which are used by authorized individuals for remote access, whether personally-owned, County-issued or otherwise obtained. These devices include but are not limited to workstations, laptops, tablets, smartphones, and any other computing device which is capable of communicating on the County's network.

Responsibilities

All individuals that utilize Travis County remote services are responsible for protecting remote access methods, devices and credentials assigned to them. Users are responsible for maintaining the security of computers and devices used to remotely access County resources.

The County Executive, Technology & Operations (CETO) is responsible for approval of remote access methods and resources and implementing systems and specifications to facilitate unit compliance with this policy

Definitions

Remote access is defined as any external connection by a device/host (County issued or privately owned) to Travis County's internal data network to access computing resources owned, managed or maintained by Travis County. Multifactor Authentication (MFA) involves combining more than one authentication type and generally provides a stronger assurance of the person's identity. Combining only two of the types is called two-factor authentication (2FA).

Policy Statements

The Travis County remote access infrastructure must follow these guidelines:

1. It is the responsibility of Travis County employees, contractors, vendors, and agents with remote access privileges to Travis County corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Travis County.
2. Secure remote access must be strictly controlled by using Multi-factor Authentication (MFA) and strong passwords. Please refer to TC-ITS-200, Password Management Policy.

3. Only approved remote access solutions may be used to connect to Travis County. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Travis County production network must obtain prior approval from the Chief Information Security Officer (CISO).
4. Members of the workforce using an active remote access solution must ensure that unauthorized users are not allowed access to Travis County internal networks.
5. At no time is a remote user to connect Travis County's network to any other network or device beyond the initial device making the connection. This includes, but is not limited to split tunneling, dual homing, or otherwise re-routing County traffic beyond the intended endpoint.
6. While connected to Travis County computing resources, remote access users are required to follow County policies at all times, including the Acceptable Use Policy regardless of the device and location.
7. All remote devices as set forth in the scope of this document must have appropriate security protections enabled. These protections include but are not limited to, the use of anti-virus software with the latest virus definitions installed, all appropriate operating system security patches applied and a personal firewall installed where available.

Exceptions

All requests for any exception to this policy must be formally assessed, approved and documented by the Chief Information Security Officer (CISO). Approved exceptions must be periodically reviewed by the Information Security Office.

The exception will be granted for a period of no more than one year from the time the exception is granted. At the end of the year, the exception will be reviewed and either terminated or renewed for another period. Requests for exception may be revoked in the event of a security incident or policy violation using established incident response procedures.

Enforcement

Failure to comply with this policy may result in disciplinary action. Access may be revoked at any time for reasons including non-compliance with security policies.

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 VPN Policy (404) into this policy.	ITS Policy Committee	09/09/2016
1.2	Changed wording on #8 regarding dual or split tunneling to be allowed only if approved.	ITS Policy Committee	9/23/2016
1.3	Updated name of CIO	Randy Lott	12/18/2017
1.4	Draft to include scope, exceptions, updated policy statements and important sections.	Paul Knight	2/27/2019
1.5	Removed two policy statements to be included into the Acceptable Use Policy instead. Updated policy number from 317 to 210.	ITS Policy Committee	3/8/2019
1.6	Added language that requires MFA externally and only applications that are centrally-managed and use AD can be allowed.	Joyce Miller	9/23/2019
1.7	Updated title for policy approver	Brandon Rogers	11/07/2019
1.8	Renumbered from 317 to 210	Joyce Miller	11/20/2019