## 1. Overview

Remote access to our corporate network is essential to maintain our productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Campbell County policy, we must mitigate these external risks to the best of our ability.

## 2. Purpose

The purpose of this policy is to define rules and requirements for connecting to Campbell County's network from any host. These rules and requirements are designed to minimize the potential exposure to Campbell County from damages which may result from unauthorized use of Campbell County resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Campbell County internal systems, and fines or other financial liabilities incurred as a result of those losses.

## 3. Scope

This policy applies to all Campbell County employees, contractors, vendors and agents with a Campbell County-owned or personally-owned computer or workstation used to connect to the Campbell County network. This policy applies to remote access connections used to do work on behalf of Campbell County, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Campbell County networks.

## 4. Policy

It is the responsibility of Campbell County employees, contractors, vendors and agents with remote access privileges to Campbell County's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Campbell County.

General access to the Internet for recreational use through the Campbell County network is strictly limited to Campbell County employees, contractors, vendors and agents (hereafter referred to as “Authorized Users”). When accessing the Campbell County network from a personal computer, Authorized Users are responsible for preventing access to any Campbell County computer resources or data by non-Authorized Users. Performance of illegal activities through the Campbell County network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use Campbell County networks to access the Internet for outside business interests.

For additional information regarding Campbell County's remote access connection options, including how to obtain a remote access login, troubleshooting, etc., contact the Helpdesk at (434) 332-9866 or (434) 332-9536 or helpdesk@co.campbell.va.us.

### 4.1 Requirements

*4.1.1* Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the *Password Construction Guidelines.*

4.1.2 Authorized Users shall protect their login and password, even from family members.

4.1.3 While using a Campbell County-owned computer to remotely connect to Campbell County's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4 Use of external resources to conduct Campbell County business must be approved in advance by the Information Technology Department and the appropriate department head or supervisor.

4.1.5 All hosts that are connected to Campbell County internal networks via remote access technologies must use the most up-to-date anti-virus software (Sentinel One for Campbell County owned devices), this includes personal computers.

4.1.6 Personal equipment used to connect to Campbell County's networks must meet the ownership of Campbell County, Vendor Company, or authorized device (with permission and knowledge of IT Department) for remote access.

## 5. Policy Compliance

### 5.1 Compliance Measurement

The Information Technology Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, firewall logs, internal and external audits, and will provide feedback to the policy owner and appropriate business unit manager.

### 5.2 Exceptions

Any exception to the policy must be approved by the Information Technology Department and the Director in advance.

### 5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 6 Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Campbell County's network:

- *Acceptable Use Policy*
- *Password Construction Guidelines*

## 7 Revision History

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| August 2018 | Jonathan Pingilley | Adopted from SANs Security Policy Project |
| January 2025 | Jonthan Pingilley<br>Jodi Crews | Updated areas to reflect new technologies and policies |