Catalina Foothills School District

Remote Access Requirements

Purpose:

This document is intended to define optimal business practices for granting remote access to Catalina Foothills School District (CFSD) approved vendors. Many CFSD resources (E-mail, Google Drive, Frontline, etc.) are available to the public and secured by traditional means: secure website; user names; complex passwords. There will be times when access to CFSD internal resources is required by approved vendors.

Scope:

These guidelines apply to CFSD approved vendors. Before remote access is granted, all other avenues of providing the necessary information or access should be explored.. An approved vendor requesting remote access must agree to the CFSD Vendor Access Requirements and adhere to all guidelines contained therein.

Guidelines:

Remote access to internal resources will be granted using one of two methods: Virtual Private Network (VPN) client, and direct connection which takes place over Port 443. Access via Virtual Private Network client is only granted to specific user accounts that have met the criteria in the Scope of this document. A Cisco VPN client will be installed on the client machine, and instructions for use will be provided. When access is no longer required, the Educational Technology Department will disable the user account or remove membership in the VPN access group. When applicable, direct access via LogMeIn will be provided to the CFSD approved vendor.

Vendors seeking approval for access to our network need to reach out to the CFSD Systems Engineer and Network Manager with one week's notice. Upon approval, the CFSD vendor will be given access temporarily with the account being disabled at 12:00 a.m.

In order to protect the integrity of the CFSD internal network, the Educational Technology Department reserves the right to remove remote access capabilities in total or to any individual without notice.

April 2024