



## **Catalina Foothills Unified School District #16**

### **Remote Access Guidelines**

#### **Purpose:**

This document is intended to define optimal business practices for granting remote access to Catalina Foothills School District (CFSD) staff. Many CFSD resources (E-mail, Google Drive, Applitrack, etc.) are available to the public and secured by traditional means: secure website; user names; complex passwords. Access to CFSD internal resources is required by certain staff members and approved vendors. More stringent guidelines must be followed in order to protect the integrity of the CFSD network.

#### **Scope:**

These guidelines apply to CFSD staff members and approved vendors. Before remote access is granted, all other avenues of providing the necessary information or access should be explored.

An hourly employee for CFSD should only receive access with the express consent of the employee's supervisor. The supervisor should understand that hours worked remotely may enable the employee to work more than the 40 hour work week. The supervisor should further understand that remote access may enable the hourly employee access to the CFSD internal timeclock system, and use of the system by the employee may require additional monitoring.

An exempt employee for CFSD should only receive access with the express consent of the employee's supervisor.

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: firewall exception; Virtual Private Network (VPN) client.

A firewall exception will only be granted in the event it can be limited. Required limitations include vendor IP address/network and port(s). Preferred limitations include: specific internal host IP and port; a clearly defined instead of open ended request.

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 IT Department will disable the user account or remove membership in the VPN access group.

**Procedures:**

Any request for remote access will be made to the Network Manager or Network Systems Technician for Catalina Foothills School District. The request will be evaluated to ensure it complies with the information in this document and standard IT Department business practices.

If any request is refused, an appeal can be directed to the Director of Educational Technology.

Before any access is granted, the IT Department will utilize the internal “Network Change Request” form in order to approve and properly document important network modifications. Once approved, the Network Manager can proceed with the requested change.

**Enforcement:**

In order to protect the integrity of the Catalina Foothills School District internal network, the IT Department reserves the right to remove remote access capabilities in total or to any individual without notice.