Catalina Foothills School District

Vendor Guidelines

Purpose:

This document is intended to define optimal business practices for third party vendors accessing resources on the Catalina Foothills School District (CFSD) network. It is the desire of CFSD to have consistent rules available so that vendors, CFSD departments, and CFSD schools understand what is required and why these practices must be followed. It is necessary to safeguard CFSD from damages which may result from unauthorized or inappropriate use of the CFSD network. Damages include the loss of sensitive or confidential data, intellectual property, compromise of the CFSD network, or damage to critical CFSD network infrastructure.

Scope:

It is the responsibility of CFSD vendors, contractors, and subcontractors with access to CFSD resources to exercise due care in properly securing CFSD resources. Additionally, it is the responsibility of CFSD vendors, contractors, and subcontractors with access to CFSD resources to ensure that proper safeguards are observed when using vendor devices on CFSD networks.

These guidelines apply to all CFSD vendors, contractors, or subcontractors with a CFSD-owned or personally-owned device used to connect to the CFSD network. They also apply to any connections used to perform work on behalf of CFSD.

Guidelines:

CFSD vendor devices used to administer CFSD resources must be properly secured with strong passwords, antivirus (if applicable), and stored in a restricted physical space whenever possible. At no time should any CFSD vendor provide, release, share, or distribute data or information deemed confidential by CFSD. Any vendor software installed on the CFSD network must be documented and communicated to the Educational Technology Department. This includes remote access software that may permit the vendor to enter the network from an external location. Installed software should be legally obtained and verification of licensing should be included with documentation.

April 2024

At no time should any CFSD vendor provide their access credentials to any other entity without the express consent of the Educational Technology Department. Vendor passwords should conform to the general password strength requirements defined in the Catalina Foothills School District Password Guidelines. Secure storage of passwords and procedural documents used for accessing CFSD resources is required. Any changes made on the CFSD network or to CFSD applications are documented and communicated to the Educational Technology Department. If a vendor believes that the security of devices has been compromised, they must alert the Educational Technology Department immediately. This would include any compromises that may have occurred from external entities, but also from internal parties, such as CFSD staff.

Any user accounts used to administer CFSD resources should be created for vendor use only and be separate from the default administrator accounts. Vendors requiring physical access to network ports must request access three (3) business days before access is required. The Educational Technology Department may refuse the request or require additional information before access is granted. Vendors requesting access to a CFSD wireless network must request access three (3) business days before access is required. The Educational Technology Department may refuse the request or require additional information before access is granted. Subcontractors used by vendors and requiring access to CFSD resources will be communicated to the Educational Technology Department three (3) business days before access is required.

Requests for remote access to internal CFSD resources must be in accordance with the Catalina Foothills School District Remote Access Guidelines document. In order to protect the integrity of the Catalina Foothills School District network, the Educational Technology Department reserves the right to terminate vendor access at any time without notice.

Acknowledgement

I acknowledge that I have read this document and will make every effort to comply with these guidelines.

Name (Print)	Company
Signature	Date