Virtual Private Network Service (VPN) Policy and Request Form

Department of Technology
601 McAllister Street
San Francisco, CA 94102

Description

The San Francisco Unified School District (SFUSD) Virtual Private Network (VPN) service provides access to the District's network via a user's internet provider. VPN is intended for use by SFUSD staff or authorized contractors in roles/positions that require off-site or after hours access to secured SFUSD technology systems. Users with VPN access can connect to SFUSD technology applications and services remotely that are typically only available from a District site.

Accessible without VPN	Requires VPN
• SFUSD Employee Email • Google Docs, Sheets, Slides, etc. • SFUSD Website (Public & Employee) • Synergy SIS, School Loop, Illuminate • Special Education Information System • Cornerstone P.D. Registration System • Technology/Telephone Service Request System	• Employee Information System (PeopleSoft) • Financial Information System (Peoplesoft) • Online Timeroll System • File Servers (shared file folders)

Please note that VPN access will not provide users with access to file servers and/or computers located at their school sites.

Policy and Conditions of Use

VPN service creates a secured tunnel into SFUSD's confidential and proprietary network and data systems. Because of the risk this creates, interested SFUSD technology users must be approved by a Department Head for VPN service as well as the SFUSD Chief Technology Officer. The Department Head and the user are responsible for proper use of this service to avoid loss of data, security violations, virus proliferation, and other technical matters that are outside of Department of Technology (DOT) control related to VPN services.

When using the VPN from outside of SFUSD network, the user is responsible for selecting and, if necessary, paying for connectivity through an Internet Service Provider (ISP). SFUSD does not provide Internet services from locations outside of the district. SFUSD does not provide after-hours or off-site support for VPN services.

By signing this VPN Request Form, users acknowledge that the computer used for VPN access will be a de facto extension of the SFUSD's network, and will be subject to all applicable policies, rules and regulations that apply to all SFUSD-owned equipment. This includes, but is not limited to, appropriate use, security, confidentiality, operational recovery, virus protection, etc. It is the user's responsibility to ensure that unauthorized users are not allowed to access the computer used for VPN services.

Any user found to have violated this policy may be subject to disciplinary action equivalent to the penalties of inappropriate use as stated by the SFUSD Technology Acceptable Use and Security Policy.

Rev. 3: 6/7/2016

Virtual Private Network Service (VPN) Policy and Request Form

Procedure

(1) Complete the checklist and associated requirements on the final page of this document.
(2) Sign and date the form.
(3) Obtain the signature of your Department Head or Site Administrator.
(4) Scan the completed form and email to help@sfusd.edu.
(5) You will receive a notification of approval or rejection.
(6) If approved, VPN software will need to be installed:
    - Employees: You may submit a Service Request to have the VPN software installed on your computer. Alternately, you may bring your laptop computer to the DOT Desktop Support Team Office for their weekly "Laptop Clinic" for installation. Contact the Desktop Support Team at 415-615-8900 for details on the "Laptop Clinics."
    - Non-Employees: You will be emailed information required to install and configure VPN software.

IMPORTANT: Non-employees requesting a VPN account must already have been issued an SFUSD network account (username and password). If an SFUSD network account is not yet issued, the Non-Employee SFUSD Technology Acceptable Use and Security Policy (AUP) forms and Non-Employee Access Request to Technology forms must accompany this VNP account request.

Virtual Private Network Service (VPN) Policy and Request Form

Complete and return this page to the Department of Technology as indicated at the bottom of this page. Your signature on this form confirms that you have read and agreed to abide by this VPN policy.

Requirements

Users must meet the following requirements to be considered for VPN access. Please check the appropriate boxes to confirm you understand, and have/will complete these prerequisites.

SFUSD Employees

- ☐ Must have a current, SFUSD "Technology Acceptable Use and Security Policy" on file.
- ☐ Must have an SFUSD computer (laptop or desktop) available to use for VPN access.
- ☐ The computer that will be used must meet current SFUSD standards and include critical security software (antivirus, anti-theft, content filtering). If the computer does not already have these software packages installed, the user's department or school may be responsible for purchasing the licenses (up to $80.00 cost).
- ☐ The user must read and sign the "Off Site Equipment Use Policy" for each SFUSD-owned computer that may be used offsite for VPN access.

Non-Employees

- ☐ Must have an approved SFUSD "Request for Technology Access: Non-Employee" form signed by the SFUSD employee responsible for supervising the non-employee work.
- ☐ Must have a signed "Technology Acceptable Use and Security Policy: Non-Employee" form on file.

Describe the reason for your request and the systems/data you require access to:

Approval

Requestor (User) Information				
Print Full Name of Requestor (User)			SFUSD Employee	Yes No
Work Location or Organization				
SFUSD Employees →	SFUSD Username		Employee ID#	
Requestor's Signature			Date Signed	/ /
Site Administrator/Department Head				
Print Name			Duration of Access	From: To:
Signature			Date Signed	/ /
Department of Technology Approval				
Chief Technology Officer Signature			Date Signed	/ /

Scan this completed signature page and email to **help@sfusd.edu**

Rev. 3: 6/7/2016