@SFUSDdot
Department of Technology

Department of Technology
601 McAllister Street
San Francisco, CA 94102
415.241.6476

Description

The San Francisco Unified School District (SFUSD) Virtual Private Network (VPN) service provides access to secure District systems for users outside of SFUSD's on-site network. VPN is intended for use only by SFUSD employees or authorized contractors in roles/positions that require off-site access.

Requires VPN if outside of SFUSD's Network	Accessible without VPN
● GoFAST ● PERCii ● stubs-admin.sfusd.edu (admin access) ● File Servers (shared file folders) ● PeopleSoft (testing environment ONLY) ● City of San Francisco's eMerge system (SFUSD HR staff requiring access) ● Other specifically identified systems ● Synergy, Student Information System (SIS) if accessing outside of the US.	● SFUSD Employee Email ● Google Services: Docs, Sheets, Slides, etc. ● Services supporting Google authentication ● Zendesk, SFUSD Service Request System ● SFUSD Employee Website (www.sfusd.edu) ● EMPowerSF ● stubs.sfusd.edu (historical paystubs) ● Special Education Information System (SEIS)

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 employees or authorized contractors must be approved by a district office Head of Department or Site Administrator for VPN service as well as the SFUSD Head of Technology or designee. The Head of Department 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.

All VPN users are required to use the district's two-factor authentication (2FA) as a condition of our cyber insurance provider.

By signing this VPN Request Form, both requester and user acknowledge that the computer used for VPN access will be a de facto extension of the SFUSD's network and 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 (AUP).

- Continued on next page -

Virtual Private Network Service (VPN) Policy and Request Form

Procedure

1. (1) Complete the checklist and associated requirements on the final page of this document.
2. (2) Sign and date the form.
3. (3) Obtain the signature of your Head of Department or Site Administrator.
4. (4) Scan the completed form and attach it to a Service Request ticket at help.sfusd.edu.
5. (5) You will receive a notification of approval or rejection.
6. (6) If approved, VPN software will need to be installed by the requesting user:
    - You will be emailed information to your SFUSD email account about how to install and configure VPN software along with instructions for activating 2FA, if not already in place.

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) form must accompany this VPN account request. All non-employees with VPN access are required to use the District's two-factor authentication (2FA)

- Continued on next page -

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 be a current SFUSD employee with an active district email account.
□ SFUSD employees must have an SFUSD-provided device for VPN access.
□ The device that will be used must meet current SFUSD standards and include critical security software (antivirus, anti-theft, content filtering).
□ User must have District two-factor active on their account

Non-Employees

□ Must have an approved "Technology Acceptable Use and Security Policy: Non-Employee" form on file.
□ User must have District two-factor active on their account

Describe the reason for your request and the system(s)/data you require access to:

Approvals

VPN Requestor (User) Information			
Print Full Name of Requestor (User)		SFUSD Employee	NO
Work Location or External Organization			
SFUSD-issued Username		SFUSD Employee ID#	
Requestor's Signature		Date Signed	
Dept. Head or Site Administrator			
Print Name		Duration of Access	From: To:
Signature		Date Signed	
Department of Technology Approval			
Head of Technology or Designee Signature		Date Signed	

Submit a scan or PDF of this completed signature page with a technology service request at help.sfusd.edu