SAN FRANCISCO
DEPARTMENT OF
TECHNOLOGY

VPN Access 75-6005

Revision History

Date	Version	Author	Comments
03/5/13	1	David Geller	
10/14/16	2	David German	Reformat/Paired with City Remote Access Policy
12/29/16	2.1	David German	Edits with Thompson, Bailess, Voje, Muhirwe

1. Overview

The purpose of this policy is to provide guidelines for Remote Access Virtual Private Network (VPN) connections to the City and County of San Francisco (CCSF) Department of Technology (DT) network.

Use of the VPN service at CCSF comes with responsibilities for both departments and users. All other policies covering the authorized use of CCSF computing resources are still in effect when those resources are accessed from remote locations, as are all regulations (e.g., HIPAA) which protect the confidentiality and integrity of information entrusted to CCSF's stewardship.

2. Purpose

The objective of the VPN access policy is to maintain a secure environment for accessing City and County of San Francisco computer systems remotely.

3. Scope

This policy applies to all CCSF employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing the VPN to access CCSF FiberWan. This policy applies to all implementations of VPN that allow direct access to the CCSF resources from outside the CCSF network.

4. Policy

This policy covers all VPN users, equipment utilized by the VPN, and all CCSF resources accessed through the VPN tunnel. Device access to the City FiberWan is only allowed through VPN software approved and administered by DT.

5. VPN User Account Guidelines

- VPN access is for users (staff and consultants) who need access to CCSF computing resources that are not otherwise available from outside City-wide networks.
- New VPN accounts, or changes to existing accounts, must be requested via DT service request by departmental IT administrators on behalf of the employee's manager.
- Service requests may be submitted by email or directly through the DT Service Portal and must include all required forms, including user acceptance signatures, as attachments to the email or ServiceNow ticket.

VPN access for third parties (e.g., consultants and support personnel) to perform tasks specifically noted in their SOW and MOU on CCSF systems must be requested by a CCSF Manager through their

department IT administrator. In addition, the third party must complete and sign a non-disclosure agreement with CCSF. Please see links below for specific VPN user request types:

- ✓ Contractor VPN
- ✓ Group VPN
- ✓ User VPN

- Users shall access CCSF networks through only one VPN group. If, in unique circumstances, additional access is required the Local IT Administrator must justify the use of additional profiles with explanation of the different projects and access requirements of each. VPN users that access multiple groups without Local IT Administrator justification and DT permission will result in immediate disabling of that VPN User's account.
- VPN access can be terminated by user's manager, system data owner, departmental IT administrator, City Cyber Security Team (if compromise of credentials is suspected), Department of Human Resources – in case of separation, or by the user's request.
- Contractors will be given the most least privileged access that allows them to complete their tasks.
- Contractor's accounts automatically expire after 90 days, or at the end of the supporting contract, whichever is shorter. Contracts lasting longer than one year will require annual resubmission of the VPN user access form.
- IAM, AD and VPN user and group passwords expire after 90 days.
- Accounts that have been inactive for 90 days will be disabled. After an additional 90 days (180 total days since last activity) the accounts will be deleted. Departments may request these limits be extended annually through written request.
- Departments are required to keep an updated list of VPN groups and users. DT may request a list of these groups and users at any time to ensure alignment with accounts in the VPN access control lists.
- DT support is only for City purchased equipment. Personal equipment using approved VPN software must be supported by the equipment owner.

6. Roles and Responsibilities

6.1 DT Responsibilities

- VPN access to the City FiberWan will be set up and managed only by the Department of Technology.
- DT reserves the right to monitor for unauthorized VPNs and disable access of those devices performing non-sanctioned VPN service.
- All network activity during a VPN session is subject to CCSF computing policies and may be monitored for compliance.
- DT will provide the VPN client software and instructions for installing the software.

6.2 User Responsibilities

- Only VPN client software distributed by DT may be used to connect to the CCSF VPN. Approved users can download the VPN client and installation instructions from DT.

- Departmental IT administrators are responsible for the installation of the VPN software.
- Users with VPN privileges shall ensure that only authorized users can access computing resources located on the CCSF network.
- All computers, including personal computers that are connected to the CCSF network via VPN or any other technology must have:
    - Up-to-date virus-scanning software with current virus definitions installed
    - All relevant security patches installed
    - Available firewall enabled
    - No infection of viruses, worms, or other malware

7. Related Standards, Policies and Processes

- DHR Telecommute Policy (In Draft)
- Alternative Work Schedule Policy (In Draft)

8. Approvals

Role	Name & Title	Signature	Date
Responsible	Joe Voje - CISO	DocuSigned by: Joe Voje	January 26, 2017 | 11:18
Sponsor	Bryant Bailess - PMO Deputy Director	DocuSigned by: Bryant Bailess	January 31, 2017 | 8:59
Sponsor	Saul Melara – Operations Deputy Director	DocuSigned by:	February 7, 2017 | 5:19
Sponsor	Ken Bukowski - City CIO	DocuSigned by: Kenneth Bukowski	February 7, 2017 | 7:48

THIS POLICY TO BE REVIEWED ANNUALLY AT THE END OF THE FISCAL YEAR