SAN FRANCISCO
DEPARTMENT OF
TECHNOLOGY

City and County of San Francisco Department of Technology

Technical Policies and Guidelines for Telecommuting

I. Overview

Many telecommuting employees will need access to City and County of San Francisco (City) computer systems. This document specifies the Department of Technology (DT) policies and guidelines regarding remote access to the City network, and provides remote connection instructions.

These requirements apply to all departments using remote access services. They also apply to both City-owned and personal devices used for telecommuting. Departments can include additional technical requirements based on their business and data needs, but cannot waive any of the DT requirements. Employees should check with their department management and IT personnel regarding additional department policies or requirements.

Policies governing remote access to enterprise applications such as eMerge PeopleSoft will be determined by the department owning the enterprise application.

Employees with questions should contact their departmental IT personnel, who will contact DT for further information if needed.

II. Remote Access Guide

First determine whether employees need remote access to the City network. Cloud applications such as Office 365 are available over the internet without establishing a connection to the City network. Departments whose employees require access to the City network will need to identify all applications required, including the delivery method, and request remote access.

A. Requesting Remote Access

1. Employees request and receive approval for remote access based on their department's policy and process.
2. Employees sign up for a remote access account by completing a Virtual Private Network (VPN) user request form and submitting it to the department IT representative authorized to request VPN accounts.
3. The authorized department IT representative reviews the form, updates the form with the department VPN group, and digitally signs the form.
4. The authorized IT representative submits the form to the DT Service Desk via email dtis.helpdesk@sfgov.org or directly through the DT Service Portal.
5. The DT Service Desk opens a ServiceNow request for fulfillment and responds to the requestor when complete.

The department's authorized IT representative will work with DT to determine groups of users and the VPN access required if they are not already defined.

B. Technical Requirements and Policies for Remote Access

1. Employees must have high-speed broadband internet to connect to the City network using VPN.
2. Employees need a device with an operating system supported by their department and DT.
3. Network access must be in accordance with DT's VPN policy.
4. Employees with VPN privileges must prevent unauthorized access to the City network.

C. Installing VPN Software

DT provides the VPN client software and instructions. The department's IT personnel install VPN and configure the telecommuting employee's laptop or workstation. Employees who have problems with VPN should contact department IT personnel for assistance. If the department IT personnel cannot solve the problem, they will contact DT for further analysis.

D. Remote Access Support

Employees who experience problems using VPN to connect to the City network should first determine whether their internet connection is working properly by using the web browser to go to a different website. If the employee cannot reach any website, there is a problem with the internet connection. This problem should be resolved with the Internet Service Provider. If the employee can access different websites, but not the City network, there is a problem with the City network connection. In this case, the employee should contact department IT personnel, who will provide initial support before escalating the problem to DT.

DT technical support is only available during regular business hours.