New York State Office Of Children & Family Services

CLIENT VPN

New York State Office of Children & Family Services (OCFS) Client Virtual Private Network (VPN) Access to the Human Services Enterprise Network Request for remote access State workstations including CONNECTIONS In A Box personal computers (CIABs) and NYS Laptop computers

This offering is for VPN access using State owned computers only.

Table of Contents

Introduction

These procedures will be read and understood, including the attached MOU, before filling in the request form in order to make certain that there are no misunderstandings during this process.

The objective of this initiative is to allow District and Agency staff to access the CONNECTIONS application from remote access State workstations, including CIAB's and State Laptop computers, via the use of a Client VPN solution.

A Virtual Private Network (VPN) supplies network connectivity over any physical distance. The key feature of a VPN is its ability to use public networks like the Internet rather than rely on private leased lines. VPN technologies implement restricted-access networks that utilize the same cabling and routers as a public network, and they do so without sacrificing features or basic security.

The connectivity provided by an ISP (Internet Service Provider) must be in place before submitting the request for the Client VPN solution.

Client VPN access utilizes a client to allow the user to access all applications that he or she has been granted access to, and would be able to access using a networked computer. The installation includes a firewall.

Request for VPN Submission Procedure

Initiation Process

All Local Districts, and Voluntary Agencies that currently have a Bailment Agreement with the State (OCFS), may be given access to the Client VPN Offering. The Offering Document is located on the OCFS Internet Web Site <http://www.ocfs.State.ny.us/>.

Submission Requirements

The ISP must be installed and operational before submitting the VPN request.

The Agency has determined the employee's job duties require remote access to the Human Services Enterprise Network and all agency permissions have been satisfied. Submission of this request form signifies that the employee to be granted VPN Access acknowledges understanding of the HSEN Acceptable Use Policy and agrees to be in compliance and to install and maintain recommended Antivirus and Firewall Software to safeguard the HSEN network from virus attacks, and, if a Voluntary Agency, to be in compliance with the Agencies bailment agreement with the New York State Office of Children and Family Services. It is the Agency's responsibility to submit this form to delete VPN access for individuals when they longer require access or have been terminated.

Submission Process

The requester for the organization should e-mail the VPN form to **comctrup@dfa.State.ny.us.** The requester **must** indicate on the form the machine name/serial number of each State workstation, CIAB computer or State laptop they will use – these usually begin with a "W" followed by the serial number.

The Office of Children and Family Services (OCFS) and The Office for Technology's OFT) Customer Networking Solutions will process the request and a response will be sent directly to the authorized submitter for ADD requests.

Authorizing Individuals will be notified when ADD and DELETE requests are completed. Organizational submitters and authorizing individuals may email **comctrup@dfa.State.ny.us** to check on the status of their requests.

The access granted through this process is applicable only to specified remote access State owned workstations, including CIAB's and NYS owned laptops.

The submission of this request indicates that the employee has read and agrees to the ***Remote Access Acceptable Use Memo of Understanding*** delineating the employee's responsibilities for use, and the software requirements for the user's remote access State workstation, CIAB, or State laptop in this document and on the VPN request form. The instructions for obtaining and installing the Office Of Children and Family Services VPN Client software will be sent to the user when the request has been processed.

Further questions can be referred to the Enterprise Help Desk at **1-800-697-1323**.

Client VPN Dual Connection

For security reasons, when the State workstation is used to connect to the HSEN using VPN, the following precautions need to be taken:

Avoid using the laptop's modem to dial out while connected to the HSEN via the VPN. By avoiding dual connectivity, you lessen the chances that Internet viruses or cyber attacks could promulgate past the laptop.

It is also important to have the most current security patches and anti virus signatures resident on your laptop. You should make a habit of using the VPN connection to the HSEN at least once a week. The laptop will be updated automatically within 15 minutes after you have logged onto the network.

Funding

The cost of the ISP for the VPN access will be the sole responsibility of the requesting Agency.

Remote Access Acceptable Use Memo of Understanding

I. Introduction

It is the Office of Children and Family Services policy to ensure that authorized individuals that conduct official State business from remote locations via State-owned PCs or Laptop computers be provided viable remote access to the NYS Human Services Enterprise Network.

Connection to the global Internet exists to facilitate the official work of OCFS and affiliated District and Agency staff serviced by the NYS Human Services Enterprise Network, both internally and through remote access to that network. Remote access connections and services through the Internet are provided for employees and persons legitimately affiliated with OCFS for the efficient exchange of information and the completion of assigned responsibilities consistent with OCFS' statutory purposes. The use of these remote access connections and services by any Agency employee or Agency contract employee authorized by OCFS must be consistent with this Acceptable Use Memo of Understanding and all relevant security policies.

II. Principles of Acceptable Use

Remote access users of the NYS Human Services Enterprise Network who are authorized by OCFS are required:

- To respect the privacy of other users; for example, users shall not intentionally seek information on, obtain copies of, or modify files or data, belonging to other users, unless explicit permission to do so has been obtained.

- To respect the legal protection provided to programs and data by copyright and license.

- To protect data from unauthorized use or disclosure as required by State and federal laws and agency regulations.

- To respect the integrity of computing systems: for example, users shall not use or develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.

- To safeguard their accounts and passwords. Any user changes of password must follow published guidelines for good passwords. Accounts and passwords are assigned to single users and are not to be shared with any other person without authorization.

- Users are expected to report any observations of attempted security violations to their LAN administrator. Following is the Logon banner for the OCFS network:

"**Warning:** The Office of Children and Family Services (OCFS) computer system (the system) is the property of the State of New York and the client specific or other statutorily protected data accessed through it has been deemed confidential by the State of New York. Access to this system is limited to authorized persons and entities. Access to data maintained by other governmental agencies also may be available through the system. Access to such data also is limited to authorized persons and entities. Unauthorized access to the system, or unauthorized release of any data accessible through the system, may result in civil liability and or criminal prosecution. If you suspect unauthorized activity has or is occurring, or if you have questions as to what is authorized, please e-mail the OCFS Acceptable Use Committee at acceptable.use@dfa.State.ny.us. You have no right to privacy in any information you enter or receive through the system. Your use of this system constitutes your express consent for the State, and other authorized persons and entities to access, intercept, read, forward, copy of reuse any material you enter into or receive through the system for any authorized purpose.

III. Unacceptable Use

It is not acceptable to use NYS Human Services Enterprise Network remote access:

- For activities unrelated to the Agency's business objectives and processes;
- For activities unrelated to official assignments and/or job responsibilities;
- For any illegal purpose;
- To transmit threatening, obscene or harassing materials or correspondence;
- To access any Internet sites on commercial connections without using required VPN software on the HSEN via requested access policies;
- Without all necessary security and VPN software enabled and up-to-date.
- For unauthorized distribution of NYS data and information;
- To interfere with or disrupt network users, services or equipment;
- For private purposes such as marketing or business transactions;
- For solicitation for religious and political causes;
- For unauthorized not-for-profit business activities;
- For private advertising of products or services; and
- For any activity meant to foster personal gain.

Any use must be in accordance with OCFS Policies and Procedures

IV. Agency Rights

Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et Seq), notice is hereby given that there are NO facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and user access requests, and will monitor messages as necessary to assure efficient performance and appropriate use. Messages relating to or in support of illegal activities will be reported to the appropriate authorities. The Agencies reserve the right to log network use and monitor file server space

utilization by users and assumes no responsibility or liability for files deleted due to violation of file server space allotments. OCFS reserves the right to remove a user account from the network. OCFS will not be responsible for any damages. This includes the loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors, or omissions. Use of any information obtained is at the user's risk.

OCFS make no warranties, either expressed or implied, with regard to software obtained from this system. OCFS reserves the right to change their policies and rules at any time. OCFS makes no warranties (expressed or implied) with respect to remote access services, and it specifically assumes no liabilities/responsibilities for:

- The content of any advice or information received by a user outside NYS or any costs or charges incurred as a result of seeking or accepting such advice;

- Any costs, liabilities or damages caused by the way the user chooses to use his/her Agency's remote access;

- Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the Agencies. OCFS' remote access services are provided on an as is, as available basis.

- Any damage to equipment while accessing the NYS Human Services Enterprise Network remotely. This includes but is not limited to hardware, software, deletion/loss of personal files, virus damage, etc.

- Any 3rd party (commercial) connectivity solutions not ordered/supported by OFT-CNS. This includes bandwidth, connection support, and support of 3rd party data communications equipment installed by vendors outside of OFT-CNS control.

V. Enforcement and Violations

The approval of a request for VPN access for Remote Access State workstations including CONNECTIONS In A Box (CIAB) personal computers or State laptop computers only grants access through State owned equipment. It does not grant any access through Local District or Voluntary Agency or personally owned equipment.

This policy is intended to be illustrative of the range of acceptable and unacceptable uses of the remote access connections and services and is not necessarily exhaustive. Questions about specific uses related to security issues not enumerated in this policy Statement and reports of specific unacceptable uses should be directed in writing to the Information Security Officer at the ocfs.sm.it.remote.access mailbox. Other questions about appropriate use should be directed to your supervisor.

Alleged breaches by Agency staff should be brought to the attention of the employee's Office and Division Head for further action. The Information Security Officer, Legal Affairs, and Public Information Offices will be made aware of breaches of security to

consider further disciplinary action. This Agency will review alleged violations of the Remote Access Acceptable Use Memo of Understanding on a case-by-case basis.

Employees should be made aware that breaches of security and computer abuse are subject to civil liability and criminal penalties. For example if a client establishes that he/she suffered economic loss because of the wrongful disclosure of his/her name or program status to a third party, he/she may seek to recover the loss from the Agency, a district, or the worker. If it is established that a worker making a disclosure knew that the disclosure was inappropriate, there would likely be no recovery against the Agency or the district, but the worker could be held liable for the economic loss and for punitive damages, could be terminated from employment, and could be prosecuted for the crime of Official Misconduct.

Link:

Client VPN Form and Instructions:

http://www.oft.State.ny.us/forms/VPNRequestForm.doc