New York State Office Of Children & Family Services

New York State Office of Children & Family Services (OCFS) is Offering Secure Socket Layer (SSL) Virtual Private Network (VPN) Access to Approved OCFS Applications and Webstar for use with Local District and Agency's Non - State Owned PCs.

Table of Contents

1. Introduction

This document, including the attached *"Remote Access Acceptable Use Memo of Understanding*" (MOU), will be read and understood by the Local Security Administrator and any employee whom access is requested before completing the request form in order to make certain that there are no misunderstandings during this process.

a. The objective of this initiative is to allow OCFS users with a valid HSEN ID, access to Approved OCFS Applications and Webstar from their **Non-State Owned PCs** via the use of an SSL VPN solution.
b. As additional OCFS Applications become available on SSL VPN, a notification will be distributed and updated instructions and access requirements will be posted to the OCFS Web Site.
c. A Secure Socket Layer (SSL) Virtual Private Network (VPN) is the most widely deployed security protocol in the world. As such, it has undergone extensive scrutiny and has yet to be degraded by any known weakness. This does not mean it is guaranteed secure for the future, but it does mean that many of the brightest minds in cryptography and mathematics have been unable to find any holes in its cryptographic armor.
d. The key features of an SSL VPN is its ability to use public networks like the Internet rather than rely on private leased lines, and provide the highest level of Security needed for New York State's data.
e. SSL 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 security with SSL.
g. The connectivity of a **High Speed ISP (Internet Service Provider) must be in place and operational before submitting the request for SSL VPN access**. The Local District or Agency is responsible for arranging with the ISP for the amount of bandwidth needed based on the local usage.

2. SSL VPN Access Submission Procedure

a) Qualifications to Participate in SSL VPN Offering:

1) **SSL VPN Supports Win ME/2000/XP on Non-State Owned Equipment**.
2) OCFS users with valid HSEN IDs are eligible to request access to SSL VPN for Non-State Owned PCs
3) **The High Speed ISP must be installed and operational before submitting the SSL VPN request.**
4) **The SSL VPN Offering Document and request form are located on the OCFS Internet Web Site < (http://www.ocfs.state.ny.us/main/vpn/sslvpn/) >.**

b) Submission Requirements

1) The District or Agency has determined that an employee's job duties require remote access to Approved OCFS Applications and Webstar and all agency permissions have been satisfied.
2) Submission of this request form by the Local Security Administrator signifies:
   - The employee has a Valid HSEN user ID prior to requesting SSL VPN access.
   - That the Local District or Agency who is requesting SSL VPN Access for any employee acknowledges understanding of OFT Policy *"User Responsibilities when using OFT IT Systems".*
   - The Local District or Agency agrees to be in compliance with all OCFS policies, and to install and maintain required Antivirus and Firewall Software to protect the integrity of the network.
   - That it is the Local District or Agency's responsibility to submit the SSL VPN request form to delete SSL VPN access for individuals when they no longer require access for any reason.

c) Submission Process

1) The Local Security Administrator for the organization must e-mail the SSL VPN form, listing individuals for each site separately, requesting SSL VPN to **comctrup@ocfs.state.ny.us.**
2) The Office of Children and Family Services (OCFS) will process the request and a response will be sent directly to the Local Security Administrator for ADD requests.
3) The Local Security Administrator will be notified when ADD and DELETE requests are completed.
4) The Local Security Administrator that submitted the ADD or DELETE SSL VPN requests may email **comctrup@ocfs.state.ny.us** to check on the status of their requests.

5) The response to the Local Security Administrator will include**:**
   - Notification that the Users and their HSEN ID's have been registered with the SSL VPN Server.
   - A set of instructions will be included for installing the Office Of Children and Family Services SSL VPN CONNECTIONS Citrix Program Neighborhood (PN) Agent.
   - Instructions for Logging on to CONNECTIONS and Webstar.

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

d) Funding

1) The cost of the High Speed ISP for the SSL VPN access will be the sole responsibility of the requesting Local District or Agency.

2) The SSL VPN will be provided by OCFS.

3. SSL VPN Request Form Instructions:

⓪ Enter the name of the Local District or Agency requesting SSL VPN Access to be added or deleted.
① Enter the three-character Agency code assigned.
② Enter the Site name assigned to the location where the employees are located.
③ Enter the date of the request.
④ Enter the Last Name of the Local Security Administrator requesting SSL VPN access to be added or deleted.
⑤ Enter the First Name of the Local Security Administrator requesting SSL VPN access to be added or deleted.
⑥ Enter the HSEN ID of the Local Security Administrator requesting SSL VPN access to be added or deleted.
⑦ ***High Speed ISP must be installed and operational before the SSL VPN request is submitted.***
⑧ Provide the name of your ISP
⑨ Provide the contact information for your ISP.

This selection will apply to all persons on this form.

- ⓿ Select either Added or Deleted. All persons on the form must have the same request status of either ‘Added’ or ‘Deleted’.
- ❶ This box is checked when the LDSS/Agency Local Security Administrator has reviewed the form and is in agreement that the persons named should have access. ***Use this box only when requesting to add SSL VPN access.***
- ❷ Enter the phone number of the site requesting SSL VPN access be added or deleted.
- ❸ Enter the Address of the site requesting SSL VPN access be added or deleted.
- ❹ The Process and e-mail address for submitting the SSL VPN Access Request.
- ❺ Enter All Users, Last name, First name and HSEN User Id for whom access addition or deletion to SSL VPN is requested. (Use another form for additional users)

OCFS-4827 (Rev. 7/2005)(Sample)

NEW YORK STATE
OFFICE OF CHILDREN AND FAMILY SERIVCES

SSL VPN REQUEST FOR ACCESS TO APPROVED OCFS APPLICATIONS
For Local District and Agency Use on Non-State Owned PC's

AGENCY NAME: ⓪	AGENCY CODE: ①	SITE NAME: ②	DATE OF REQUEST: ③
LOCAL SECURITY ADMINISTRATOR'S LAST NAME: ④	LOCAL SECUREITY ADMINISTRATOR'S FIRST NAME: ⑤	LOCAL SECURITY ADMINISTRATOR'S HSEN ID: ⑥	

⑦ ***HIGH SPEED ISP MUST BE INSTALLED AND OPERATIONAL BEFORE THE SSL VPN REQUEST IS SUBMITTED.***

PLEASE PROVIDE ISP NAME: ⑧	PLEASE PROVIDE ISP CONTACT INFORMATION: ⑨

ACCESS IS TO BE ⓿ ☐ ADDED **OR** ☐ DELETED

Submission of this request form signifies that the Local district or agency and employee to be granted SSL VPN Access acknowledges understanding of the Remote Access Acceptable Use Memo of Understanding (MOU) and agrees to be in compliance with all OCFS Policies. The Local District/Agency is responsible for maintaining the required Antivirus and Firewall Software to safeguard the HSEN network. It is the Local District's responsibility to submit this form to delete SSL VPN access for individuals who no longer require access for any reason.

PLEASE "X" THE FOLLOWING ONLY ON REQUESTS TO ADD SSL VPN ACCESS:

☐ ❶ The Local District/Agency's Local Security Administrator has determined the employee's job duties require remote access to the SSL VPN Approved OCFS Applications and all permissions have been satisfied.

The Local District or Agency site(s) is/are responsible for having their ISP commercial connectivity installed, working, configured, and security patches applied along with any necessary data communications equipment if using multiple Non State owned PC's. The connectivity, bandwidth, and/or data communications equipment is the responsibility of the local district or agency and is not the responsibility of OCFS or OFT/CNS or supported by OFT/CNS.

SITE PHONE NUMBER: ❷	SITE ADDRESS: ❸

FORM SUBMISSION ❹

The Local Security Administrator for the organization will e-mail the completed form to comctrup@ocfs.state.ny.us

OCFS will process the request and will send a response directly to the Local Security Administrator for **ADD** requests. Local Security Administrator's will be notified when **ADD** and **DELETE** requests are completed. The Local Security Administrator's may e-mail comctrup@ocfs.state.ny.us to check on the status of their requests.

The response to the Local Security Administrator will include a set of instructions for installing the Office of Children and Family Services PN Agent. Instructions on how to log on to Approved Applications will be included. Further questions for support of the SSL VPN can be referred to the **Enterprise Help Desk at:**

1-800-697-1323

OCFS-4827 (Rev. 7/2005)(Sample) ❺

NEW YORK STATE
OFFICE OF CHILDREN AND FAMILY SERIVCES

SSL VPN REQUEST FOR ACCESS TO APPROVED OCFS APPLICATIONS
For Local District and Agency Use on Non-State Owned PC's

Enter employee's Name & HSEN ID requiring access to or deletion from SSL VPN:

NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:
NAME:	HSEN:	NAME:	HSEN:

4. Remote Access Acceptable Use Memo of Understanding

Introduction

It is the Policy of Office of Children and Family Services (OCFS) to allow authorized individuals who require the ability to conduct official State business from remote locations via privately owned computers viable remote access to OCFS Approved Applications and Webstar. This is consistent with the Office for Technology Customer Networking Solutions Bureau's Policy.

The OCFS, through the Office for Technology connection to the global Internet, exists to facilitate the official work of OCFS 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 the Agency's statutory purposes. The use of these remote access connections and services by any OCFS employee, Local District/Agency or contract employee authorized by OCFS, must be consistent with this Acceptable Use Memo of Understanding and all relevant security policies of OCFS and OFT.

The purpose of this MOU is to see that OCFS systems are used by Local District or Agency staff to support agency business functions to their fullest capacity. This MOU advises staff and management of their responsibilities and provides guidance in managing information communicated through SSL VPN.

Principles of Acceptable Use

All information, regardless of the form or format, which is created, acquired or used in support of OCFS' business activities, must only be used for official business. Information contained in OCFS applications and Local District and Agency information is an asset and must be protected from the time of its creation, through its useful life, and to its authorized disposal. It must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use.

Any OCFS employee, Local District/Agency or contract employee using SSL VPN to access an OCFS application shall adhere to all applicable Federal and State statutory and regulatory confidentiality requirements, and shall not store any confidential client information in any form of electronic media outside of the OCFS application being accessed.

As indicated on the OCFS computer logon banner, the OCFS HSEN computer system is for the Office of Children and Family Services business, or other authorized use, and that user's activities are subject to monitoring. Users should have no expectation of privacy. The logon banner is presented during the authentication process.

Any use of the SSL VPN privilege must be related to legitimate business activities and be within the individual's job assignment or responsibilities. Staff may not use SSL VPN for any illegal, disruptive, unethical or unprofessional activities, for personal gain, or for any purpose that would jeopardize the legitimate interests of the State.

NYS Human Services Enterprise Network (HSEN) remote access users 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 normally 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.
- Users shall adhere to the OCFS logon banner, which is shown below.

Warning Warning 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.

Prohibited Use

Users are prohibited from using OCFS HSEN or OFT computer services for activities including, but not limited to, the following:

- Any illegal purpose
- The creation, download, viewing, storage, copying or transmission of sexually-suggestive or sexually explicit materials
- The creation, download, viewing, storage, copying or transmission of discriminatory, threatening, harassing or other offensive images or correspondence. Such activities include but are not limited to: hate speech or material that ridicules others based upon race, creed, religion, color, sex (gender), disability, national origin, Vietnam-era veteran or military status, age, prior arrest/conviction record or sexual orientation.
- The creation, copying, transmission or retransmission of jokes or chain letters.
- Unauthorized distribution of work-related data and information
- Interfering with or disrupting network users, services or equipment
- Use of commercial purposes, in support of "for profit" activities or in support of any outside employment or business activities
- Endorsing any product or service
- Union activity not consistent with the collective bargaining agreement and/or labor management agreements
- Lobbying activity, or engaging in any prohibited partisan political activity
- Writing personal communications in a manner that could reasonably be interpreted as official State or OCFS policies
- Signing up for personal services, including but not limited to dating or horoscope services
- Visiting or engaging in conversations in "chat rooms", "bulletin boards", or similar electronic communication facilitators
- Online gambling activities
- Playing games or installing unapproved software
- Any use that could result in a security breach
- For activities unrelated to the Agency's business objectives and processes
- Any use that could generate more than a minimal additional expense to OCFS
- To access any Internet sites on commercial connections without using required SSL VPN software on the HSEN via requested access policies
- Without all necessary security and SSL VPN software enabled and up-to-date.

Any use must be in accordance with OCFS and OFT Policies and Procedures including the Telecommunications and Computer User Policy – PPM1900.00 and Customer User and Access of the Human Services Enterprise Network Policy P2003-01.

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 support efficient performance and appropriate use. Messages relating to or in support of

illegal activities will be reported to the appropriate authorities. OCFS reserves 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 and OFT reserve the right to remove a user account from the network. OCFS and OFT 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 and OFT make no warranties, either expressed or implied, with regard to software obtained from this system. OCFS and OFT reserve the right to change their policies and rules at any time. OCFS and OFT make 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 OCFS and OFT. OCFS and OFT 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, or virus damage.

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

Enforcement and Violations

The approval of a request for SSL VPN access for an employee of Local District or Agency only grants access for that employee.
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 OCFS Information Security Officer. 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. OCFS shall be apprised of all suspected breaches of security to consider further disciplinary action. OCFS will review suspected violations of the Remote Access Acceptable Use Memo of Understanding on a case-by-case basis.

Employees should be made aware that breaches of confidentiality, security and computer abuse may be subject to civil liability and/or 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, 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.