Security Information for Remote Access to State Applications from Non-State Owned or Personally Owned Devices

Introduction and Background

The purpose of this document is to provide users with terms and conditions when remotely accessing Office of Children and Family Services' (OCFS's) applications from a non-state owned or personally owned device in order to maintain the confidentiality, integrity and availability of information. Any OCFS employee, local district, agency or contract employee accessing an OCFS application is required under existing policy to adhere to all applicable Federal and State statutory and regulatory confidentiality requirements. The information contained in this document, along with all referenced information, is not intended to replace or supersede any information contained in existing Office for Technology (OFT), Office of Children and Family Services (OCFS) and Office of Information Technology Services (ITS) Remote Access Acceptable Use documents or other agreements such as the Remote Access Acceptable Use Memorandum of Understanding.

Anyone attempting to access any OCFS application with a personally owned or non-state owned device should be familiar with the terms and conditions contained in the log-on banner for each application, information in this document, and other documents referenced herein. As indicated in the OCFS and OFT log-on banners, OCFS systems are for official business and only for authorized use, and the user's activities are subject to monitoring. Users have no expectation of privacy. The log-on banner is presented during the authentication process, and applies regardless of the method or manner used to access the OCFS application.

OCFS allows authorized users to access OCFS-approved applications and information assets, including Webstar, and NYSeMail with personally-owned or non-state owned devices so long as they use published remote access links, and not connect directly to the HSEN network. Remote access connections and services by any OCFS, local district/agency or contract employee must be consistent with all relevant OCFS policies. Users are responsible for maintaining the confidentiality of password and account information, and are responsible for any activities that occur under their credentials. Further, users must: (a) immediately notify OCFS of any unauthorized use of password or account information, or any other breach of security; and (b) make certain devices are password protected; and (c) make certain that they logout from their account at the end of each session.

Users shall not store any Personal, Private, or Sensitive Information (PPSI) or other confidential information on any personally-owned devices, or on portable storage or web services, except as approved by the OCFS Information Security Officer (ISO).

User responsibilities when accessing OCFS and other NYS applications from personally-owned or non-state owned devices are as follows:

Any costs to procure and/or maintain non-state owned devices used to access OCFS and other NYS applications will not be borne by NYS and are the sole responsibility of the user or in some cases the local district or agency that employs the user. If an authorized user elects to use his/her own computer or portable device to access a state application, that user or local district or agency is responsible for making certain that the equipment is compatible with the state application, and is solely responsible for the purchasing, servicing, and maintenance costs associated with any non-state owned or personally-owned equipment. The state will not reimburse employees for such costs, nor will the state provide technical support for any personally-owned equipment. OCFS is not responsible for compensation, including overtime or carrier charges for work outside of normal work locations using a personally-owned or non-state owned device.

OCFS may revoke access to agency resources and services from a personally-owned or non-state owned device should the agency determine that the access presents a risk to the agency's mission.

Minimal Requirements:

1. In order to access OCFS applications from the Internet, users must have an Internet Service Provider (ISP) with high speed connectivity, properly installed and configured, with appropriate security patches. The connectivity, bandwidth, airtime charges and/or data communications equipment is the responsibility of the user, local district or agency, and is not the responsibility of OCFS.
2. Users must have installed and maintain up to date anti-virus protection and firewall software on his or her device, wherever possible.
3. Users must take all appropriate measures to make certain that the device they are using to access an OCFS application is virus free and will not pose a security risk to OCFS information.
4. The user shall physically protect the device when it is being used to access OCFS assets.
5. The user shall provide an appropriate level of protection of the credentials used to access OCFS systems. Software may be used to manage credentials and automatically enter them for the user, but such software must provide an appropriate level of security for the credentials (e.g. a password must be entered before the program will give access to the credentials), and the program must use an appropriate encryption method to protect the credentials from unauthorized access. In particular, the 'auto-complete' functionality, or similar found in most modern web browsers, should not be used to store logon credentials and automatically type them in for the user without a password prompt.
6. To access State Email systems remotely, users must only utilize the Outlook Web Access (OWA) in order to protect against confidential materials being accidently stored on a non-state owned or personally owned device.
7. The user's browser history should be cleared regularly to avoid storage of transient files related to a current session of an OCFS web application, as well as any confidential materials that may remain in the web browser history.

All OCFS confidential information transmitted or stored must be encrypted in accordance with NYS Office of Cyber Security Cryptographic Standard (http://www.dhses.ny.gov/ocs/resources/documents/Cyber-Security-Standard-S10-006-V1.1-Cryptographic-Controls.pdf) using Federal Information Processing Standard (FIPS) approved algorithms.

OCFS make no warranties (expressed or implied) with respect to remote access services, and it specifically assumes no liabilities/responsibilities for:

- Any costs, liabilities or damages caused by the user's remote access to OCFS applications.
- Any consequences of service interruptions or changes, regardless of whether these interruptions were within the control of OCFS, OFT or ITS. OCFS, OFT or ITS provides remote access services on an "as is, where available" basis.
- Any damage to equipment while accessing remotely. This includes, but is not limited, to hardware, software, deletion/loss of personal files, or virus damage.
- Any third party (commercial) connectivity charges not authorized, ordered or supported by OFT or ITS. This includes bandwidth, connection support, and support of third party data communications equipment installed by vendors outside of OFT control.

This information is intended to be illustrative of the range of acceptable and unacceptable uses of remote access connections and services, and is not necessarily exhaustive. See the OCFS Telecommunications and Computer Use Policy (PPM 1900.00) for additional terms and conditions. Questions about specific security issues not enumerated herein or for reports of unacceptable use should be directed in writing to the OCFS Information Security Officer at acceptable.use@ocfs.state.ny.us. Other questions about appropriate use should be directed to your supervisor.

Any alleged security incidents or breaches by users should be brought to the attention of your supervisor for further action. OCFS must be notified of any suspected breaches of security as quickly as possible so that they can investigate and secure the application, and address requirements and other potential consequences of a breach. OCFS will review each suspected violation or breach on a case-by case basis.

WARNING: Breaches of confidentiality, security and computer abuse may be subject to civil liability and/or criminal penalties, as well as disciplinary action, including possible termination.