Andrew M. Cuomo
Governor

NEW YORK STATE
OFFICE OF CHILDREN & FAMILY SERVICES
52 WASHINGTON STREET
RENSSELAER, NY 12144

Gladys Carrión, Esq.
Commissioner

Administrative Directive

Transmittal:	13-OCFS-ADM-01
To:	Commissioners of Social Services Executive Directors of Voluntary Authorized Agencies
Issuing Division/Office:	OCFS-Executive
Date:	February 6, 2013
Subject:	**Portable Device Security and Remote Access Guidance**
Suggested Distribution:	Directors of Social Services Voluntary Agency Supervisors Child Protective Services Supervisors Child Welfare Supervisors Security Coordinators CONNECTIONS Implementation Coordinators All users of portable devices
Contact Person(s):	Information Security Office (518) 473-9254; acceptable.use@ocfs.state.ny.us
Attachments:	No
Attachment Available Online:	n/a

Filing References

Previous ADMs/INFs	**Releases Cancelled**	**Dept. Regs.**	**Soc. Serv. Law & Other Legal Ref.**	**Manual Ref.**	**Misc. Ref.**
11-OCFS-ADM-08 State Issued OCFS and OTDA IT Equipment		18 NYCRR Part 466.6			Cyber Security Policy P03-002 Version 3.4 Information Security Policy Revision Date: July 30, 2010 Thomas Smith, Director NY New York

I. Purpose

The purpose of this Administrative Directive (ADM) is to provide guidance and information for Local Departments of Social Services (LDSS) and authorized Voluntary Agency staff using state-owned portable devices, including but not limited to laptops, netbooks, tablet computers, smartphones and personal digital assistants, or using a non-state-owned, or personally owned, device (referred to collectively as portable devices) when accessing the Office of Children and Family Services' (OCFS's) data or applications. This ADM will assist LDSSs and other authorized users in protecting the confidentiality, integrity and availability of OCFS information. This directive is not intended to supersede pre-existing agreements for the use of state Virtual Private Network (VPN) devices, or through non-state- owned, Secure Sockets Layer / Virtual Private Network (SSL/VPN) devices, but is meant to reinforce existing policy and, where necessary, provide up-to-date security directives to meet the evolving cyber-security requirements. Required technical, administrative and physical measures to protect the security of portable devices issued by OCFS, as well as when users remotely access OCFS's applications from a non-state-owned or personally owned device, are set forth herein.

II. Background

Portable devices are increasingly used to store, transmit or access OCFS's confidential information for official and approved purposes. When used for such purposes, users must exercise due diligence and are responsible for maintaining the physical security of these devices, and are also responsible for the security and integrity of all information transmitted or stored on them. Portable devices must not be used to store or transmit confidential information unless approved and suitable protective measures, including but not limited to encryption, are present, enabled and used. Devices used to access OCFS telecommunications, Internet, or e-mail services or equipment must not be used for any illegal, disruptive, unethical or unprofessional activities; for personal gain; or for any purpose that would jeopardize the legitimate interests of the state.

III. Program Implications

Portable devices storing or accessing OCFS's confidential information present a unique security threat due to their small size and portability. They can be easily lost, misplaced, or stolen. Besides the cost of the device itself, the loss or theft of a portable device places at risk the confidentiality of the device's contents and information. The unauthorized disclosure of confidential information could cause great harm to the children and families we serve, and cause significant damage to the credibility and reputations of LDSSs, Voluntary Agencies and OCFS.

IV. Required Action

This ADM must be distributed to all persons assigned or with access to OCFS-issued portable devices, or who access OCFS's applications and data from a non-state-owned or personally owned portable device.

Compliance with this ADM is mandatory, and OCFS will take all appropriate measures to protect the security and confidentiality of its information assets. Any non-compliance with this ADM may result in disciplinary action, up to and including termination, and/or possible prosecution under applicable local/state and federal laws.

State-Issued or LDSS/VA-Issued Portable Devices:

Physical Security of Portable Devices:

Users of state-issued portable devices are responsible for the physical security of their portable device at all times, and must secure their state-issued portable device(s) when not in their physical possession. Users must make every effort to see that only authorized personnel have access to state-issued portable devices.

Staff utilizing portable devices should exercise caution in public, and not bring unwarranted attention to the fact that a portable device is in their possession. Staff that are required to enter data into their portable device in a public area should be aware of their surroundings and, when dictating notes or discussing a client matter, be aware of those persons that may be able to overhear their conversation. Staff must take reasonable precautions to prevent onlookers from seeing information entered into or stored on their portable device.

State-issued portable devices may never be left unattended unless the workspace or portable devices have been secured.

1. When left unattended, staff should secure their portable device:

   a. with a cable lock, if feasible; or

   b. in a secure workspace or secured enclosure, such as a locked cabinet, desk drawer or vehicle.

2. When using the cable lock, it must be secured:

   a. to an immovable object or furniture of such size to prevent removing the portable device from the area with the object or furniture still attached; and

   b. in such a way that the cable lock cannot be removed without unlocking it (e.g., by slipping the locking cable under a desk leg).

Note: When working from home with a state-issued portable device, cable locks are not required, but highly recommended. However, when leaving your home, make certain that you properly secure your state-issued portable device.

Technical Controls

1. Technical controls provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for the systems or applications.
2. Information on technical controls specific to portable device security are provided below in the following areas:

   - Access Control and Network Security
   - Encryption and Wi-Fi Network Security

Access Controls and Network Security

1. Personal Identification Numbers (PINs) and passwords are used to limit access to state-issued portable devices and defend against unauthorized use. All state-issued portable devices must be configured so that a password or PIN is required to log-on to the portable device, per OCFS guidance for state-issued and non-state-owned (Local District and Voluntary Agency owned) devices.

2. Never share passwords or store the password with the portable device.

3. Laptop and other designated portable device users must leave their portable device connected to the Human Services Enterprise Network (HSEN) for at least 2 hours each month, and preferably overnight, in order to download and install the latest security updates. Note: Some portable devices, such as personally owned devices, are not permitted to connect to the HSEN network and may only connect to OCFS applications and data using Web services.

4. Users must take reasonable measures to make sure that portable devices connecting to Web services are free from malware.

5. Portable device users must never connect personally owned equipment (printers, scanners, wireless devices, flash drives, etc.) to a state-issued portable device unless approved by the Information Security Officer (ISO).

6. Users must not download unapproved software to a state-owned portable device.

7. Users must not upload or store confidential information to any third party source without prior written ISO approval.

Encryption

“Encryption” is a technology that renders plain text and files indecipherable to unauthorized parties, except through use of an encryption key.

1. **All OCFS confidential information stored on a state- or LDSS/VA-issued portable device must be encrypted.**
2. Laptop users must shut down their laptop, rather than placing it in sleep mode. This provides added security when the laptop is equipped with whole disk encryption.
3. Users must verify their device is encrypted prior to storing or transmitting any confidential information. Under no circumstances should confidential information be kept on a USB flash drive unless either the flash drive or the file containing the confidential information is encrypted using an OCFS-approved encryption method.

Portable devices that do not have encryption enabled may under no circumstances be used to store or transmit confidential information.

Personally Owned Devices:

With the approval of the LDSS or Voluntary Agency, an authorized user may elect to use a personally owned computer or portable device to access an OCFS application. In this circumstance, any costs associated for purchasing, servicing, and maintaining such personally owned equipment is the responsibility of that user. OCFS will not reimburse LDSS or Voluntary Agency employees for such costs, nor will OCFS provide technical support for any personally owned equipment. Staff must make certain that the personally owned equipment is compatible with the state application(s) being accessed.

OCFS may revoke access to its resources and services from a personally owned device should OCFS determine that the access presents a risk to OCFS.

Remote Access Minimum Requirements:

1. To remotely access OCFS applications from the Internet, users must have an Internet Service Provider (ISP) with high speed connectivity. User’s personally-owned device must be properly configured and have all appropriate security patches. The connectivity, bandwidth, airtime charges and/or data communications equipment is the responsibility of the user, LDSS or agency, and not OCFS.

2. Any device capable of supporting anti-virus and firewall software must have up-to-date anti-virus protection and firewall software configured to provide real time protection for the device.

3. The user must take all appropriate measures to make certain that the device used to access an OCFS application is virus-free and will not pose a security risk to OCFS information.

4. Access to the portable device must be password protected if it will be used to access OCFS systems. Password management 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, may not be used to store log-on credentials and automatically type them in for the user without a password prompt. It is also strongly recommended that personal devices that access OCFS applications and data also utilize a complex password, where feasible.

5. To access the OCFS e-mail system remotely, users must only utilize the Outlook Web Access (OWA) to protect against confidential materials being accidently stored on a personally owned device through use of third party e-mail systems, such as Yahoo or Google.

6. When accessing non-Citrix-based OCFS applications, (i.e. other than CONNECTIONS and ASAP) through the Internet with a personal device, copies of confidential data viewed in the application may be retained on the devices. To mitigate this, the user should clear the browser's history/cache immediately after viewing confidential information to comply with OCFS's requirement that such information not be stored on personally owned devices. Information about how to clean the cache on a personal device will be available through the vendor of the device or the help function of the Web browser.

Users may not store any of OCFS's confidential information on any personally owned devices, or on portable storage or Web services, except as approved by the OCFS Information Security Officer.

Wi-Fi Network Security:

Users must not transmit or access confidential information over a Wi-Fi connection unless the website utilized provides an SSL-protected Webpage to enter or access OCFS's information, or users connect using an OCFS-approved VPN solution. An SSL Web connection can be identified on a protected page by looking for "https://" in the address bar of the Web browser. Many Web browsers may also display an icon of a "lock" on the status bar of the Web browser. To verify the security status of the website, click on the "lock" icon found in the address bar of the Web browser.

A VPN connection, which encrypts internet traffic through a secure tunnel, providing the required level of data security, can also be utilized. Note: Users must not access the HSEN or OCFS applications using Wi-Fi networks they are not authorized to access. When using a wireless connection to connect to an OCFS application, all confidential information must be encrypted in accordance with the New York State Office of Cyber Security Cryptographic Standard, and connection must be made using a secure socket layer protocol

(See http://www.dhses.ny.gov/ocs/resources/documents/Cyber-Security-Standard-S10-006-V1.1-Cryptographic-Controls.pdf).

Reducing Data Exposure:

A state-issued or approved non-state-owned portable device must never be used as the sole repository for confidential case information, or to transmit unencrypted confidential information. The portable device could be lost, stolen, or accidentally damaged and any confidential case information stored on it could be lost or compromised. Confidential case information must be transmitted to the HSEN as soon as practicable, and not permanently stored on the portable device. Users should delete confidential information, such as personally identifiable case information, on any state-issued or non-state-owned portable device after this information has been transferred to the HSEN.

Any exceptions to this ADM must be approved in writing by the OCFS Information Security Office (ISO).

Any staff member that identifies or suspects a security incident or violation of this ADM must report any such incidents or suspected violations to the OCFS ISO for investigation.

Lost or Stolen Procedures:

If a state-issued portable device is lost or stolen, the loss must be reported immediately to the police, your supervisor, LAN Administrator, and the OCFS ISO and Management Services. Report any OCFS-issued lost or stolen equipment to OCFS ISO and Management Services, by completing and sending the OCFS-4440 Lost or Stolen Equipment Form as follows:

Email: OCFS-4440 Lost or Stolen Equipment Form to comctrup@ocfs.ny.gov

and ocfs.sm.oms.telecommunications@ocfs.ny.gov.

If a non-state-owned device is lost or stolen and contains OCFS confidential data, it should be reported to the OCFS ISO via email at

acceptable.use@ocfs.ny.gov

immediately, stating what type of device was lost or stolen, and whether confidential information was stored on the device, so that an assessment of the encryption status can be completed, along with notifying the owner of the device.

With certain portable devices, once reported lost or stolen, OCFS may be able to disable the device, lock the device, or completely erase its contents remotely.

Forms

OCFS 4440-Lost or Stolen Equipment Form

Forms are located on the OCFS Intranet at:

http://ocfs.state.nyenet/it/forms.asp

Forms shall be submitted via e-mail to:

comctrup@ocfs.ny.gov

and ocfs.sm.oms.telecommunications@ocfs.ny.gov

V. Systems Implications

None.

VI. Additional Information

Questions regarding this ADM may be submitted by e-mail to the OCFS ISO at

acceptable.use@ocfs.ny.gov

VII. Effective Date

Immediately.

s/s Sheila Poole

Issued By:
Name: Sheila Poole
Title: Executive Deputy Commissioner
Division/Office: OCFS