OCFS Security Guidelines

Safe Computing Practices

- **Be responsible—**Download *only* authorized, work-related executables or documents from the Internet that are from trusted sources ***and*** that your LAN/Security Administrator has approved. *Never* use commercial e-mail accounts (such as AOL, Hotmail or Yahoo), Instant Messaging, chat rooms or other third-party services on a state computer without prior *written* authorization.
- **Be professional**—*Never* use state e-mail services for prohibited activities, including (but not limited to): sharing jokes or any other non-work-related materials; transmitting illegal, offensive or threatening items; and soliciting for unauthorized causes or activities. In addition to being prohibited, these unnecessary electronic transmissions crowd network bandwidth and occupy server capacity needed for legitimate business purposes.
- **Be alert** and *immediately* report any suspected virus infection or other system compromise to your LAN/Security Administrator *and* to the OCFS Information Security Officer (Jo Shrader). Proper reporting speeds reaction, recovery and damage control. Be sure you know who your LAN/Security Administrator is *before* you need to contact him/her.
- **Be consistent** in complying with the same safety procedures when using remote access or transporting files between PCs via a floppy disk or CD. If you move disks between your home and work PCs, make sure you have up-to-date anti-virus software on your home PC and regularly scan disks and CDs. Viruses can easily be brought into the state network through a laptop, home PC or storage media.
- **Be suspicious** of e-mail you weren't expecting, even if it's from someone you know. Computer viruses often send e-mails to all contacts in an unsuspecting sender's address book. *Before* you open the e-mail, call the source to verify that s/he intentionally sent the e-mail.

- ***NEVER* run/download/forward unsolicited files** (e.g., executables, documents, spreadsheets). Any programs that run or execute on your PC must be virus-checked and approved by your LAN/Security Administrator first. *Never* open *any* file with a double file extension (e.g., iamavirus.txt.vbs).
- ***NEVER* forward virus warnings to *anyone*** Contact your LAN/Security Administrator to determine how to proceed. (If your LAN/Security Administrator is not available, contact the Help Desk.) Forwarding these items increases risk and creates additional network traffic.
- ***NEVER* attempt to test system weaknesses or vulnerabilities** unless you are specifically authorized to do so.
- ***ALWAYS* leave your PC powered on (being sure to log off, as appropriate)** This will ensure that your PC will receive security patches. Click on **Start > Shut Down > Restart** to log off and restart your computer *without* leaving it powered off.

Anti-virus software helps protect against computer viruses, but does NOT replace conscious, consistent adherence to established safety procedures.

If you think your computer may have been exposed to a virus, DON'T PANIC! Contact your LAN/Security Administrator IMMEDIATELY.

OCFS Security Guidelines

Protecting Your Password

- **Make it difficult**
  Select a password that is easy for you to remember, but difficult for others to guess. Don't be stingy—make your password as long as possible (at least 8 characters and up to a maximum of 13 characters), in order to help reduce the likelihood of allowing someone to guess it. You cannot use all or part of your logon ID in your password, nor can you reuse any of your last 13 passwords.
- **Mix it up**
  Your OCFS password *must* contain *at least* one uppercase letter, one lowercase letter *and* one number. CONNECTIONS users must *never* use symbols in their passwords.
- **Keep it to yourself**
  Don't share your password with others. Never display your password; if you need to write it down, don't keep the information at your desk or anywhere it can be easily seen by others.
- **Embrace change**
  You must change your password periodically—*at least* once every 90 days. If you think your password has been compromised, *change it immediately*. (Don't forget to report the situation to your LAN/Security Administrator as soon as possible!)
- **Be yourself**
  Use *only* your logon ID and password; *never* use a current or former co-worker's ID or password.
- **Let your fingers do the walking**
  Never store passwords in macros or automatic log-on features. Enter your password manually every time.

Your unique User ID and password not only provide you with "keys" to access the OCFS network (including CONNECTIONS, as applicable), they also serve as a form of identification—linking you to your actions in the system.
YOU are responsible for actions taken with your User ID and password! Always follow established password protocols to help prevent unauthorized use of your User ID and password.

If you think your password has been compromised, change it immediately AND report the situation to your LAN/Security Administrator.

Security is everyone's responsibility!

These guidelines are advisable for *all* of your passwords.

OCFS Security Guidelines

Protecting Confidential Information

Maintain confidentiality 24/7

Protecting confidential information encompasses all spoken, handwritten, printed and electronically transmitted notes and communications. When you make case visits, be sure to keep client-identifiable casework documentation with you at all times and *never* allow unauthorized individuals to view the information. Remember that all case and system information must be used *only* for legitimate business purposes. If you must keep hard copies of confidential information at your desk, *always* lock your desk whenever you are away from it. If hard copies need to be discarded, *always* run them through a cross-cut shredder.

Don't kick this habit

It's easy to become complacent or to think, "I'll only be away from my computer for a few minutes." If you are logged on to the system, *always* lock your computer (or log off the network) by holding down the **Ctrl**+**Alt**+**Del** keys at the same time. Do this *every time* you leave your desk; this helps prevent unauthorized individuals from using your User ID and password to access the network. ***80% of security breaches are unauthorized people using an authorized user's computer, NOT hacking in from outside.***

Hit the road, but…

Be particularly careful when using portable electronic devices, such as laptop computers, Quick Pads, voice recorders and PDAs. Don't leave confidential information on these devices longer than is absolutely necessary. If the device has the ability to transmit information, avoid transmitting confidential information over wireless connections or unsecured public connections. When traveling with the device, keep it with you at all times; *never* check it into airline luggage systems.

Exercise care with voicemail and e-mail

When conducting casework or other legitimate business contacts by phone, it's inevitable that you may sometimes need to leave a voicemail message or send an e-mail to a contact. *Avoid* ever including confidential information in voicemail you leave or e-mail you send.

Don't convey confidential information where others can intercept it

Caseworkers have an obligation to preserve the confidentiality rights of the children and families with whom they work. Other staff may also have legitimate access to this information. If you must discuss confidential information on the phone, avoid areas where your conversation can be overheard. Remember that cellular phone lines are not sufficiently secure to be appropriate when discussing confidential information. *Avoid* saving confidential information to the hard drive of *any* desktop computer. Check the permission levels on your Microsoft Outlook folders; make sure you understand what each level of access means and assign permissions on a need-to-know basis *only*.

The walls have ears

Be mindful of protecting confidential information in areas where you can be easily overheard, such as in cubicle areas.

Use follow-through when faxing

If you need to transmit any confidential information via fax, call first *before* sending the fax, in order to alert the intended recipient that you are sending a fax. Be sure to call the recipient afterward, too, to verify that the fax was received *and* that it was not left on the fax machine. Avoid faxing confidential information whenever possible.

Security is everyone's responsibility.

Always follow established security protocols to help protect confidential information.