Security Awareness Message- JULY 2011

Protecting Your Portable Device and OCFS Information

- It is your responsibility to protect the physical security of your portable device and OCFS Information at all times.
- The security and confidentiality of OCFS' Information is governed by various federal and state regulatory and statutory requirements.
- Your portable device must never be left unattended unless it is physically secured, and you must make certain that only authorized personnel have access to your portable devices, and the information stored on them.
- Do not view, discuss or process confidential information where it can be seen or heard by unauthorized persons.
- Unless approved by OCFS, do not download any software or connect personally-owned equipment (printers, scanners, wireless devices, flash drives, etc.) to your OCFS-owned portable device.
- In order to receive the latest security updates, connect your laptop or portable device to the HSEN for a minimum of two hours each month, preferably overnight.
- Treat your OCFS issued laptop or portable device like cash; never leave it unattended in a public location, in plain sight in your car or other unsecured area, and use a locking device, where possible.
- Use only authorized WiFi networks. Use a virtual private network (VPN) and avoid using unsecured WiFi when connecting to the HSEN.
- Always use a strong password to log on to, your portable device and log off or lock your laptop or portable device when it is not in use. Do not share your password with anyone.
- Report any loss or theft of your OCFS laptop or portable device to the police and submit the OCFS 4440 Lost/Stolen report form to your supervisor and LAN Administrator immediately.
- An Office for Technology (OFT) approved encryption package is required for all OCFS laptops and portable devices. OCFS requires all information stored on portable devices, including portable media (such as USB drives) and data in transit to the network to be encrypted. If you are unsure whether your portable device is configured with encryption, please contact your local LAN administrator.
- Specifically OCFS encryption requirements apply to: All OCFS owned Laptop computers and Portable Devices, USB drives, CDs/DVDs, Personal Digital Assistants (PDAs) and Smartphones and any other approve device.
- E-mail containing confidential information must not be transmitted via the internet (outside the HSEN) unless an OCFS approved encryption method is used.
- Confidential information must never be stored on an unencrypted device.
- Do not use your encrypted device to store confidential information. You should make certain you upload confidential information as soon as possible and then delete that information from the portable device.
- Send questions, or report suspicious activity, to OCFS Information Security Officer by email at Acceptable.use@OCFS.state.ny.us