JULY 2012 SECURITY AWARENESS MESSAGE

Physical Security and Secure Storage of Data and Documents

Reasonable steps must be taken to prevent and minimize the risk of access to Personal, Private and Sensitive Information (PPSI) by unauthorized persons.

- Do not store confidential information or PPSI in the open, whether in hard copy, or in electronic form. Remember there may be individuals with no need to know, such as cleaning staff, or other vendors, that enter the floor after hours!
- Store hard copies in locked drawers or cabinets. Boxes that contain confidential information need to be returned to a secure location at the end of the day, even if work is not complete!- **Clean Desk Principle**
- Pick up faxes, scans, and printed documents **right away**.
- **Always** lock your computer when you are away from it.
- Store confidential information in the application when at all possible.
- Store confidential information in protected drives, such as your H drive, where only you or those you designate can access. Do not store confidential information on your 'C' Drive (hard drive or desktop).
- Keep antivirus and other security updates up to date. Plug in portable devices to the network regularly to keep your computer secure.
- Make sure you portable device is encrypted. Do not store any confidential information on an unencrypted portable device.
- **All confidential information must be encrypted when stored on removable media, such as CDs and USB drives,** be properly labeled if they contain confidential information, and securely stored when not in use. No confidential information may be stored on unencrypted USB drives.
- Upload confidential information from your encrypted portable device as soon as possible and then delete it from your portable device.
- **Do not** allow unauthorized individuals to enter your floor without an approved purpose.
- **Do not** allow shoulder surfing where unauthorized individuals could see your work.
- **Do not** discuss confidential information where unauthorized individuals may overhear your conversation.
- See 18 NYCRR 357.5 which sets forth specific procedures for storing, using individually identifiable information and limiting internal access using a "need to know" standard.
- Confidential information, when no longer required to be maintained under State Archiving Records Administration (SARA) or by other requirements, must be securely destroyed in accordance with OCFS policy. When you are disposing confidential information that has been printed, it must be put into locked bins for secure disposal, or it must be cross cut shredded. **Never** place confidential information into regular trash baskets!