HELPFUL TIPS

- Ask yourself “Is it really necessary that I transport this sensitive information?” If the answer is no, then do not copy the information.

- Encrypt files or the full disk. By encrypting files or using full disk encryption, you reduce the risk of unauthorized individuals viewing sensitive data.

- Use strong passwords on all your devices, such as a minimum of eight characters and a mix of special symbols, letters and numbers. Never use the same password for multiple devices or accounts.

- Be sure all critical information is backed up. Portable devices should not be the only place important information is stored.

- Store your portable devices securely. When not in use, store portable devices out of sight and, whenever possible, in a locked drawer or file cabinet.

- It takes only a few seconds to secure your computer and help protect it from unauthorized access. Lock down your computer every time you leave your desk.

- Set up a screen-saver that will lock your computer after a pre-set amount of time and require a password to log back in.

- If your computer is used by more than one person, you may want to create individual accounts, with unique login and passwords for each user.

- Choose a strong password. A good password should always include upper and lowercase letters, numbers, and at least one special character. Do not set the option that allows a computer to remember any password.

- Do not engage in inappropriate conduct, such as cyberbullying, cyberstalking or rude and offensive behavior.

- Do not do something in cyberspace that you would consider wrong or illegal in everyday life.

- Do not impersonate someone else. It is wrong to create sites, pages, or posts that seem to come from someone else.

- Adhere to copyright restrictions when downloading material from the Internet.

- Do not use someone else’s password or other identifying information.
Multi-State Information Sharing and Analysis Center

For more information please visit:
www.msisac.org

http://security.cuny.edu