

April 2006

Laptop Security

If your laptop were lost or stolen today, would your sensitive information be compromised?
Did you make it easier for the thief to access your information by using the “save password” function?
Could YOU be the next media headline involving an information security breach?

The loss of a laptop can cause irreparable harm to the organization and the laptop owner. Laptops must be secured and used responsibly to prevent compromise of personal and sensitive information.

Laptop Security - Top 10 lists:

1. If you must leave a laptop unattended, lock it to an unmovable or extremely heavy object using a security cable or use an anti-theft device such as a laptop motion sensor and alarm.
2. Engrave the laptop with personal details to deter thieves.
3. Carry the laptop in a bag that is not obvious to thieves.
4. Lock down your operating system - Implement proper security configuration controls and employ a virus scanner, antispysware, firewall protection and use a “power-on” password.
5. Patches - Keep all security patches up to date.
6. Protect sensitive information - Sensitive files must be stored using encryption. School of Medicine policy requires that Protected Health Information (PHI) on laptops be encrypted with an approved encryption tool.
7. Password compromise - Do not save passwords in files, web browsers, VPN clients or any other insecure software. If you must store passwords, use an encrypted password management tool.
8. Protect your flash drives - If you use one, make sure it is a protected model that requires either a password or a fingerprint for access.
9. Lock down unwanted ports - USB ports in laptops should be disabled when not in use to prevent unauthorized users from transferring information using USB drives. Another option is to use a 3rd party utility to password protect the port.
10. Backups - Data on the laptop should be backed up on a regular basis. The campus has a contract with Iron Mountain to provide an easy, inexpensive way to automatically backup your laptop.

If you need assistance updating virus definitions, using encryption or any other security features, please contact OIS client services.