Why Emphasize Laptop Security?

Laptop computers offer the convenience of mobility, but the risk of lost or stolen machines and of wrongful access to HHS data is high and climbing. The use of government-owned laptops and personally owned laptops to store HHS-related data and to access HHS networks demands attention to security precautions.

More than 1,000 laptops are stolen every day. The value of the laptops themselves is in the millions of dollars. The value of the lost data is incalculable. The FBI reports that 97 percent of stolen laptops are never recovered.

HHS policies and guidelines hold you responsible for your government-owned laptop and its data, and for government-owned data on personally owned computers. However you should never put your personal safety at risk to protect a laptop. The suggestions in this brochure will help you protect your laptop, its information, and HHS networks.

How to Prevent Theft or Loss

1. Do not leave your laptop unattended in an unsecured environment—even for a few seconds. When considering precautions, remember that thieves look for easy targets.

2. In the office, store the laptop in a locked drawer and lock your door. (This stops casual thieves, but won't block people who have passkeys.)

3. Consider attaching a security cable, and wrap the cable around an unmovable, unbreakable object, such as a pipe. Chair or table legs can be used, but they can be broken apart. Dismantling them; however, would slow down a thief.

4. Most laptops come with a socket that can be attached to a security cable. If yours doesn't, your cable may come with an adhesive-backed attachment that will fasten the cable to the laptop. On the cable itself, a cylinder lock is stronger than a combination lock. While cable cutters could easily slice through the wire cables, from a thief's perspective, they are conspicuous.

5. Instead of using a laptop carrying case—especially one with the manufacturer's name on the outside—consider putting the laptop in a **padded** case, then in a backpack, briefcase, or other ordinary-looking holder.

6. Batteries, power cords, and other peripherals are often overlooked. They should also be secured.

7. Remove and securely store accessory cards, such as modems and wireless devices. They are easily stolen.

8. At the airport security X-ray machine, do not put your laptop on the belt until you see a clear path to the end. One thief can distract you by setting off the metal-detector, while another spirits away your computer. Charge the battery before you travel, so airport security agents can tell instantly that it is a working computer, instead of a suspicious package.

9. Do not leave a laptop in a hotel room. If you must, use a cable lock or an alarm on the laptop. Put it in a drawer or, at least, out of sight. Put out the "Do-Not-Disturb" sign when you leave.

10. Before travel, check on a country's laptop policy. Some do not allow them in.

11. Never leave a laptop visible in a vehicle. Cover it with something, such as a blanket, or put it in the trunk. Do not leave laptops in vehicles for extended periods. Winter lows can freeze and split LCD screens. Summer temperatures can melt components.

12. Think about additional security devices, such as laptop alarms and hard-drive locks. Remember that while they work, they add bulk and cost, and delay your use of the computer. Some machines come with fingerprint readers.

How to Protect Your Data

1. Use a log-in password that is not easily guessed. Make it at least 8 characters long and composed of upper- and lower-case letters, numbers, and symbols such as "#" and "&."

2. Immediately change the default password on new laptops.

3. Password requirements can be found in the *HHS Rules of Behavior*.

4. Never set the log-in dialog box to remember your password.

5. Use a password-protected screen saver that comes on after several minutes of inactivity.

6. Keep antivirus and spyware programs up-to-date, and use them.

7. Keep operating-system and application software patched with the latest security fixes.

8. Back up your data to a location other than the laptop hard drive. Keep CDs and floppy disks separate from your laptop.

9. Disable the infrared port. Laptops can read other laptops' data from across a conference table. Cover the infrared port with black electrical tape.

HHS Requirements

1. In accordance with the *HHS Information Security Program Policy on Warning Banners*, HHS-owned laptops must display a Department-approved warning banner.

2. Exercise proper and authorized use of HHS laptop equipment to avoid limitations on equipment use or disciplinary actions

3. Immediately report a lost or stolen laptop to your OPDIV IRT, the ITSC Help Desk, and to Physical Security Personnel immediately.

4. Discuss with your supervisor the data that was stored on the laptop and the access controls that were in place.

5. Become familiar with the *HHS Malicious code protection policy*.

6. Those who access the HHS network remotely must follow the HHS Information Security Program Policy concerning Remote Access and Dial-In under the Network Security section of the policy.

7. All laptop computers must be configured with encryption software that provides both whole disk encryption as well as a FIPS 140-2 certified encryption library

Resources to Contact for Help

ITSC Help Desk: 866-699-4872

HHS IT Security Information and Policies
Web: http://www.hhs.gov/ocio/policy/index.html

Secure One HHS:
Web: http://intranet.hhs.gov/infosec/

Secure One Support
Email: SecureOne.HHS@hhs.gov
Phone: 202-205-9581

HHS Security and Privacy Awareness Day
Protecting You and Your Family

Department of Health and Human Services (HHS)

Laptop Computer Security

Department of Health and Human Services (HHS)

May 2, 2007

U.S. Department of Health and Human Services

SECURE ONE HHS