

Laptop & Information Security Tips for PPPL Travelers

According to FBI statistics, one out of every ten laptops will be stolen within the first twelve months of purchase, and 90% of them will never be recovered. PPPL employees and collaborators often travel in the course of their work. It is especially important that we take measures to protect all computers and electronic equipment from loss or theft and protect the information on those devices while traveling. Please review the information in this bulletin and take the appropriate measures before, during, and after your trip. If you have questions about computer or information security, please contact Jim Hirsch (x3388) or Steve Baumgartner (x2820).

Before Your Trip

- Back up your system!!!
- Remove any sensitive personal information (e.g. income tax files, credit card numbers, etc.)
- Be sure that all vendor operating system and security patches are installed
- Install all patches to Microsoft Office products(*this is very important*)
- Install patches to all third party software packages
- Make sure anti-virus software is installed, running, and up to date
- Make sure anti-virus signatures are up to date
- Make sure anti-spyware software is installed, running, and up to date
- Consider moving all personal files to a removable storage device (e.g. USB memory stick)

During Your Trip

- Keep your laptop and other electronic equipment with you at all times
- Don't put laptops or electronic equipment in your checked luggage
- Consider using a bag that doesn't look like a computer case
- Do not use any publicly available computers
- Avoid wireless networks as much as possible
- Use our Virtual Private Network (VPN) service when connecting to PPPL to check email, etc., the VPN is available at <http://vpn.pppl.gov>
- Don't leave your laptop unattended
- Don't let anyone else use your laptop
- Protect all memory media (floppies, CDs, memory sticks, etc.)
- Be aware that many foreign internet service providers (ISPs) are monitored

After your Trip

- Report any unusual or suspicious computer issues
- Change your PPPL account password
- Change any other passwords that were used
- Run a full anti-virus scan
- Run a full spyware scan

Use Common Sense

Common sense can go a long way in protecting your privacy. Be aware of your surroundings and tone down your volume when you're discussing business (or personal) matters on your mobile phone. Take simple measures to protect your hardware, such as keeping your laptop with you or locking your computer bag in the trunk rather than leaving it inside the car.

All incidents of loss or theft of information technology must be reported immediately to Property Administration (x2724 or x2882, the PPPL Helpdesk (x2275 or helpdesk@pppl.gov) and the Cyber Security Officer (x3388 or cyberadmin@pppl.gov).

PROPERTY PASSES *All laptops and other Government equipment must be accompanied by a valid property pass during travel.* Laboratory Procedure MC-007 outlines the requirements for property passes. Questions about property passes should be addressed to Chris Canal (x2724) or Fran Cargill (x3396).

NOTE: International Property Passes are required for foreign travel. In addition, laptops must be appropriately documented as a Temporary Export during foreign travel. This information is available on the Material Services Web Page at: <http://material-control.pppl.gov/>