Laptop and Information Security Tips for JLab Travelers

According to FBI statistics, one out of every ten laptops will be stolen and only 3% of lost or stolen laptops are recovered. When your work duties require the use of a laptop and/or electronic equipment while traveling, it is especially important that measures are taken to protect the items from loss or theft and to protect the information on those devices. Please review the information in this bulletin and take the appropriate measures before, during, and after your trip. If you have questions about computer security, please contact Brian Hanlon (x7548) or Andy Kowalski (x6224). <u>If you can do without a laptop, don't take it!</u>

International Travel Note: Travel laptops are required for travel to sensitive countries and are available from the IT Division Help Desk. Travel laptops may also be checked out for domestic travel.

Before Your Trip

- Back up your system!!!!
- Remove any sensitive personal information (e.g. income tax files, credit card numbers, PII, 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 and anti-spyware software is installed, running, and up to date
- Make sure anti-virus signatures are up to date
- Consider moving all personal files to a removable storage device (e.g. USB memory stick)

* Note that travel laptops supplied by the IT Division are fully patched and configured with anti-virus and anti-spyware protection.

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 baggage
- Keep Hand Carry letter separate from laptop as they can be used for identification purposes if required
- Consider using a bag that doesn't look like a computer case
- Do not use any publicly available computers
- Don't leave your laptop unattended
- Don't let anyone else use your laptop
- Protect all memory media (CDs, memory sticks, etc.)
- Don't use thumb drives given to you and don't use your own thumb drive in a foreign computer —they may be compromised. If you're required to do it, assume you've been compromised; have your device cleaned as soon as you can
- Terminate connections when you're not using them
- Avoid Wi-Fi networks if you can—they're insecure

After Your Trip

- Report any unusual or suspicious computer issues
- Change your JLAB 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!

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.

Report stolen property immediately to the police in the jurisdiction where you believe the theft occurred. Follow-up by promptly reporting the loss to your supervisor, and to JLAB Security (757-269-7548 or 757-269-5822 after hours).

PROPERTY PASSES & EXPORT CONTROL

All laptops and other Government equipment must be accompanied by a property pass when traveling domestically and a Hand Carry Export Certification Letter when traveling overseas. Questions about Property Passes should be addressed to Christian Whalen (x5899).

All equipment hand carried out of the U.S. must be reviewed and documented on a Hand Carry Letter. Questions about temporary exports, contact Shauna Cannella (x5393) or Brian Hanlon (x7548).