Pacific Lutheran University

Instructions for Travel with University-Owned Laptop Computers

Help Desk: 253-535-7525

Important Information about Security:

To assist in protecting this laptop, please connect it to the PLU campus network once a week between Wednesday-Friday for a minimum of 4 hours. This will ensure that the operating system and software has updated patches and anti-virus updates. In addition, we ask that you log on to the network **before** leaving campus for an extended time away to ensure that your university-owned laptop has been updated. You will need to be logged on to the PLU network a minimum of 2 hours for the updates to install and may require a reboot during that time to retrieve an additional set of security updates.

Do **not** store personal information of students, employees or university affiliates, including **names** in combination with **SSN numbers or driver's license/Washington State ID numbers** on this computer or other portable storage devices when either the name or numbers are unencrypted. Washington State has a law (SB-6043) that addresses breaches of security that compromise personal information. You may view details of this law on the following web site: **http://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010**

NOTE: You can transport digital information pertaining to University business in the above mentioned categories **only** with prior authorization from a PLU Vice President, in coordination with the Associate Provost for Information & Technology Services. For more information, please refer to the PLU Administrative System Policy found at: **http://www.plu.edu/helpdesk/policies/administrative-systems.php**

University Laptop Instructions

This University-owned laptop has been assigned to you for use in and support of PLU's academic programs. It is your responsibility to ensure the safety of this laptop and any University data on it. Protecting this University asset will help prevent theft and/or loss. **Please keep this document with the laptop computer**. If this is a shared department laptop, please remove any files you have created upon your return to campus and deliver this laptop to your department's administrative assistant.

If you will be away from campus more than 2 weeks, contact the Help Desk at ext. 7525 for additional information on updating your laptop and providing for unexpected hardware problems.

To provide for the physical safety of the equipment:

- Avoid using a bag with computer identification on it.
- Do not leave the laptop in visible or public places such as a car. Keep the laptop with you at all times. If you must set the computer down when in public places such as airports, hotels or restaurants, hold the laptop between your feet or place it against your leg so that you know it is there. Thieves may try to distract you by bumping into you or otherwise diverting your attention from your personal belongings.
- Never leave passwords in your carrying case.

To avoid the loss of critical data while away:

- Back up your files before you go. Save files to a network storage device before leaving campus.
- Remove any unnecessary data and ensure that you have no sensitive contact, research, or personal data on the computer.
- Only take with you the items that are necessary (e.g., laptops, tablets, cell phones, etc.). If you can do without the item, we recommend leaving it at home.

PLU strongly discourages the storage of sensitive data on portable media, including laptops, PDAs, flash memory, and external hard drives. Nor does the University provide or support any particular software for the encryption of data on portable media. Where exceptional or compelling need exists, however, PLU will work with individuals on a case-by-case basis to secure a solution for safeguarding critical data in these environments.

When you return from your trip:

- Change your passwords. This will insure that if an account was compromised while you were away, they would no longer have access.
- Schedule an appointment with the Help Desk soon after your return to drop off the laptop and have the device scanned for malware and viruses.

Updated 9/2013