



MEMORANDUM

To: Deans, Vice Presidents, Directors, and Senior Business Officers

From: Robert Johnson
Associate Senior Vice President, Financial and Business Services

Laura La Corte
Associate Senior Vice President, Compliance

Date: April 22, 2009

Subject: Encryption Requirements for Newly Purchased Laptops and
Mobile Storage Devices

In order to ensure the integrity of university data, USC requires all laptops and mobile storage devices that are paid for with university funds and/or used for USC business purposes to be encrypted. As an additional security measure, we strongly encourage you to avoid storing any sensitive data on such equipment altogether.

Laptops and mobile storage devices purchased on or after April 22, 2009 must be either a) delivered with built-in encryption (preferred) or b) accompanied by a software-based encryption solution for subsequent installation. All encryption solutions purchased separately must be installed before the instrument may be used to store or access university data. This policy applies to laptops and mobile storage devices purchased from all sources of university funds, including sponsored project accounts, and applies to laptops and mobile storage devices used for business purposes but purchased with personal money.

Contract suppliers have been informed of this policy and have agreed to review orders and to ship only laptops and mobile storage devices with encryption solutions whenever the instrument is paid via a university purchase order. Contract suppliers of laptops and mobile storage devices are posted in a list on the following web page:

- www.usc.edu/purchasing/secureyourlaptop

Employees who purchase new laptops and mobile storage devices via a non-contracted vendor (e.g. Costco, Best Buy, Frys, etc.) or via a contract supplier using a credit card must provide proof that the instrument was purchased with an encryption solution. Proof must be provided as an attachment to a) a reimbursement request (if Travel Card or personal funds were used) or b) a Procurement Card receipt. Reimbursement requests absent of proof will not be processed.

Purchasing Services will no longer recommend specific secured models, as described in a procedural memo issued in April 2008. Instead, departments can select the laptop and mobile storage device most appropriate for the business need and subsequently make arrangements to ensure the instrument is encrypted.

The Information Security Office will be working with the Information Security Liaisons, Information Technology Services (ITS), and others on a separate program to secure existing laptop computers.

Questions about information security should be directed to the Information Security Office at (213) 743-4900 or www.usc.edu/admin/compliance/infosec. Questions about purchasing laptops or mobile storage devices should be directed to Tae Kim, Senior Buyer, in Purchasing Services at (213) 740-9792 or kim.tae@usc.edu.

cc:

Robert Abeles, Interim Senior Vice President and Chief Financial Officer
Todd Dickey, Senior Vice President, Administration
Robert Wood, Chief Information Security Officer
Clare Hansen-Shinnerl, Assistant Vice President of Business Services