Memorandum

Date: October 31, 2006

To: All University Faculty and Staff Members

From: G.P. "Bud" Peterson, Chancellor University of Colorado at Boulder

Subject: Essential Guidelines for Protecting Private Information

In carrying out the work of the university, we are required to deal with private information (such as Social Security numbers, credit card information, educational records, health information, etc.) of our students and their parents, alumni and donors, faculty and staff, research associates, vendors, and health-care patients, among others. The imperatives of respecting privacy and guarding personal information are clear, but the ever-increasing use of electronic information brings new challenges to ensuring security.

Reports of inadvertent breaches of electronic security are all too common, both at the university and beyond. Many of these breaches involve desktop workstations and portable hardware, such as laptops, personal digital assistants and flash drives. Even the smallest spreadsheet or database is at risk. The loss, theft or compromise of private information seriously undermines public confidence and trust in the university and can result in significant fines and/or sanctions for the institution and individuals.

Therefore, storing private information on desktop workstations and/or portable computing devices is no longer allowed, except in approved applications. Below are the most essential guidelines to follow when dealing with any sort of private information:

1) Do not store private information on a workstation or mobile computing device. Information of this sort must be stored only on computing systems monitored by trained electronic data security professionals.
2) Should you have a business need for storing private information on a workstation or mobile device, you must a) get written justification from the appropriate departmental authority, and b) consult with the IT Service Center to implement safeguards to protect the device from loss, theft or unauthorized access. Please review the CU-Boulder Private Data Security Standards http://www.colorado.edu/its/docs/policies/ucbprivate.html for initial guidance. In addition, the IT Security Office may also be able to identify viable alternatives to the local storage of private information.
3) If the business need no longer exists or if the information is no longer in use, immediately remove all private information from your workstations and mobile devices. Because the process of "deleting" files rarely removes data completely from a device, please contact the IT Service Center for assistance.

If you have any questions or need additional assistance, you can reach IT Service Center at (303) 735-6637 Monday to Friday, 8:00 a.m. - 7 p.m.

Carbon Copy:

Bobby Schnabel, Vice Provost for Academic and Campus Technology and CIO
Dennis Maloney, Executive Director of Information Technology Services
Jack McCoy, Assistant Vice President and Information Security Officer
Dan Jones, Campus IT Security Director
Jim Dillon, IT Audit Manager