June 25, 2007

To: Business Services Staff

Re: Business Services Data Security Requirements

I want to thank everyone for your continued efforts to ensure the protection of University data against breaches and unlawful use. There is an ongoing, heightened sense of priority that we need to place on this endeavor given that our customers and the University entrust that we will exhibit due diligence in the securing, handling and storage of this data. Because of this, I want to take the opportunity to update and restate the expectations that I sent to you in 2005 regarding the appropriate security and handling of the University's restricted and personally identifiable data. The following expectations continue to be in effect and all supervisors must be certain their staff are aware of these.

1. Restricted or personally identifiable data about employees, students, customers or anyone otherwise affiliated with Purdue may not be stored on workstation hard drives, laptops, tablet PCs, CD's, floppy disks, or other external devices such as pin drives or any other media subject to confiscation, infiltration or compromise. Restricted or personally identifiable data include but are not limited to SSN, credit card information, and other identification information like birthdates, maiden names, etc. If there is an exceptional business requirement to save such data on a CD, you must obtain approval from your director or department head and all data security and handling guidelines must be followed.

2. Be familiar with the intent and impact of the IN SSN Breach and Notification Laws that were enacted in July, 2006. Given the nature of our business, many of you work with restricted or personally identifiable data and need to understand your responsibility under these laws. You will find my memo dated May 19, 2006 regarding these laws and more information on "personally identifiable data" on the Business Services Security page at:

   http://www.purdue.edu/business/Security/pdf/SSNNotification_BreachLawsMemo.pdf

3. Restricted or personally identifiable data may not be transmitted via email or email attachments unless a mechanism for protection (i.e. encryption) has been utilized. In addition, this data should not be sent to yourself for use on a computer at home or stored on your home computer. Please contact your computer support area if you need additional information on encryption.

4. All data, electronic files and electronic documents must not be stored on your hard drive, including "temp" and "OLK" directories. Each staff member is to do a monthly scan on your workstation and if such files are identified, they should be removed immediately. Please contact your technical support if you need assistance in this process. If you are supported by the HR/Financial Zone, you can find the instructions on how to scan your workstation at this URL:

http://www.purdue.edu/hrfzone/FAQs/SensitiveData.html

Computers supported by the Human Resource/Financial Zone have a log off script to delete the temporary files from the C:\Temp folder, Microsoft Office temporary folders, the SAPGui cache folder, and the Internet Temp folder. If you (or a program installed on your computer) have created any other new temp folders on your hard drive that could contain Business Services data, you are responsible for deleting the data from those areas.

5. Queries or programs may not be created or executed against any data set, warehouse or other repository that includes Social Security Numbers (SSN) without express written permission from your Director.

6. All electronic data, documents and files must be stored in a secured location within file services (aka LAN) for your department. Electronic data, documents or files containing restricted or personally identifiable information must be stored in a limited, secure directory within file services.

7. Restricted or personally identifiable data printed on paper forms, reports or documents must be stored in secured locations (i.e. locked filing drawers or cabinets).

8. Your computer workstation is property of the University and is to be used for University business purposes only. Your computer should not be used to visit websites that are not required for Purdue business purposes. Exceptions to this practice should be discussed with and approved by your director or department head. Your computer workstation is not to be used for computer games and you should not download games or any other software to your workstation from the web or e-mail attachment. These practices could permit computer viruses to enter the Purdue network.

9. When you are away from your workstation, your computer must be locked to help prevent unauthorized access. At the end of the work day, shut down your computer. Note: Employees not supported by the Human Resource/Financial Zone should check with their own computing support staff on the appropriate procedure to close their computers at the end of the day. Some zones would prefer the user to LOG OFF in order to do nightly upgrades.

Any violation of these standards and expectations will result in disciplinary action, which could include termination of employment.

Additional information, including the appropriate handling and disposal of information can be found at:

Purdue University SecurePurdue:
http://www.purdue.edu/securePurdue/
Security Requirements for Handling Information:
http://www.itap.purdue.edu/security/procedures/dataHandling.cfm

HR and Financial Restricted Data Types:
http://www.purdue.edu/Business/Security/Training/Restricted%20Data.html
Securing protected information:
http://www.purdue.edu/bscompt/doc/SecProtInfo.doc
Data Confidentiality:
http://www.purdue.edu/securepurdue/standards/dataConfident.cfm
Data Classifications:
http://www.itap.purdue.edu/security/procedures/dataClassif.cfm
Information on the IN Breach and Notification Laws:
http://www.purdue.edu/securePurdue/breach/

If you have any questions regarding this information, please call Business Services Computing at 47265 and you will be directed to the appropriate person.

Sincerely,

s/ James S. Almond

James S. Almond
Vice President for
Business Services and
Assistant Treasurer