March 8, 2006

Memorandum

To: Managers

From: John D. Welty
           President

Subject: Confidentiality of Data

We have a challenge of growing proportions that requires the attention of each manager. Information that we have traditionally maintained in our campus files - electronic as well as paper versions - for ease of access in our normal course of business is increasingly becoming vulnerable to theft. In the wrong hands, it becomes harmful to the individuals whose privacy is violated.

The same electronic hardware that has made it so easy to store work-related information (e.g., laptops, small portable storage devices, CDs we can create ourselves) is also becoming our nemesis. In our eagerness to take care of business swiftly via email, we launch seemingly harmless electronic messages that may contain confidential information. Although it is information that has always been used in the course of business, we must be sensitive to the need to protect it with the same level of vigilance that we once protected its hardcopy predecessors. Many campus groups have been engaged in updating and creating policies relevant to information security, confidential information and password protection. You should see new policies by early summer.

With the increased attention on identity theft and its ramifications for individual victims, I am requiring specific attention to the following items:

- In anticipation of a new policy, you should perform an assessment, of confidential information being used in your unit. Each organizational unit should develop a written plan for safeguarding confidential information in your area, including:

  1. name of the office, department, or operation where confidential information is handled;

  2. justification for keeping confidential information (outside of secure administrative information systems);

  3. specific positions using confidential information and validation that the confidential information is necessary to perform job functions;

  4. administrative controls implemented to ensure appropriate individuals/positions have access to confidential

  5. description of methods for retaining and physically securing confidential records;

  6. description of methods for destruction of confidential records; and

  7. description of training provided to employees who handle confidential data including content, frequency, delivery method, etc.

- Employees under your supervision, including student assistants, should know what is considered "confidential data" and what is considered "personal data that can lead to identity theft." (See attached Confidential and Personal Data Elements.)

- Employees under your supervision, including student assistants, should complete the appropriate online security awareness training which will be offered in the fall of 2006. The curriculum is currently under development and will include separate courses for the basic user, MPPs and those who primarily work in technology positions.

- Take reasonable steps to secure all confidential and personal data used by employees under your supervision, including student assistants, !bat can lead to identity theft.

- Electronic files containing confidential data and personal data that can lead to identity theft are kept on University servers, not individual laptops or temporary storage devices. If it is necessary for the operational needs of your unit to keep these data on temporary devices, precautions should be taken to secure the devices, and remove the data as soon as possible.

- No such data should have your work area without your knowledge and approval.

Your written plan must be completed and submitted for review by the appropriate vice president no later than July 30. 2006.

Thanks for your prompt attention to this important topic.

JDW:pt

Attachment