



OFFICE OF THE PRESIDENT

THE UNIVERSITY OF TEXAS AT AUSTIN

P.O. Box T • Austin, TX 78713-8920
(512) 471-1232 • (512) 471-8102

June 9, 2006

Chancellor Mark G. Yudof
The University of Texas System
OHH, 4th Floor (P4100)

Dear Mark:

I write to inform you of The University of Texas at Austin's plan for implementation of The University of Texas System's *Business Procedures Memorandum* (BPM) 75-04-06, *Protecting the Confidentiality and Integrity of Digital Research Data*, which was issued on April 11, 2006.

In accordance with Section 3.1 of BPM 75 (i.e., "to establish accountability for protecting the confidentiality and integrity of digital research data"), on June 19, Vice President Juan M. Sanchez and I will meet with the deans to apprise them of the University's plan to implement the new requirements. I will at that time also disseminate written notification to deans, department chairs, directors of organized research units, and members of the academic research community informing them of the institutional plans for addressing BPM 75. That notice, a draft of which is enclosed with this letter, reminds the University's lead researchers of "best practices" in protecting digital research data.

I have delegated to Dr. Juan M. Sanchez, Vice President for Research, the overall responsibility for assuring implementation of BPM 75 at The University of Texas at Austin. He has appointed a Steering Committee composed of representatives of the Offices of the Vice President for Research, Vice President for Information Technology, and Vice President for Institutional Relations and Legal Affairs. The Steering Committee has specific responsibility for developing implementation plans and guidance procedures related to the protection of digital research data.

The Steering Committee has already established an implementation timeline. Of particular importance will be the communication plan that defines key strategies for disseminating information to the research community regarding "best practices" and identifies available University resources pertinent to research data security. The Steering Committee has also modified the *Data Security Operations Manual*, originally developed in response to BPM 53, to incorporate research-specific elements related to BPM 75.

Chancellor Mark G. Yudof
June 9, 2006
Page 2

As required, by the first anniversary of the release of BPM 75 (viz., April 11, 2007), I will file with you a report that provides the status of implementation of the procedures set forth in Section 3. In the meantime, please let me know if you have any questions or need additional information.

Sincerely,



William Powers, Jr.
President

Enclosure

cc: Dr. Sheldon Ekland-Olson, Executive Vice President and Provost
Dr. Juan Sanchez, Vice President for Research
Dr. Dan Updegrove, Vice President for Information Technology
Dr. Sharon Brown, Associate Vice President for Research
Mr. Jeffrey Graves, Associate Vice President for Institutional Relations
and Legal Affairs
Dr. Brian Roberts, Associate Vice President for Information Technology
Services
Ms. Nancy McCowen, Assistant Vice President for Research
✓ Mr. Cameron Beasley, Information Security Officer
Ms. Anne Heitke, Audit Supervisor

DRAFT

MEMORANDUM

To: Deans
Department Chairs
Directors of Organized Research Units
Members of the Academic Research Community

From: William Powers, Jr., President

Date: June 19, 2006

Subject: UT System BPM 75-04-06: *Protecting the Confidentiality and Integrity of Digital Research Data*

Protecting the confidentiality and integrity of digital research data has become a top priority for The University of Texas at Austin and The University of Texas System, as well as federal funding agencies. It is imperative that we work together to safeguard such data, some of which are highly sensitive, from theft and fraudulent misuse.

On April 11, 2006, The University of Texas System issued *Business Procedures Memorandum (BPM) 75-04-06, Protecting the Confidentiality and Integrity of Digital Research Data*. I write to inform you of that memorandum and of our plans to assist researchers to protect their data.

Dr. Juan Sanchez, Vice President for Research, will direct our implementation of BPM 75. He has appointed a Steering Committee composed of representatives of the Offices of the Vice President for Research, Vice President for Institutional Relations and Legal Affairs, and Vice President for Information Technology. That committee has begun its work and will produce a series of recommendations. Through forums, a new website, and periodic communications, in the coming months we will apprise you of steps that need to be taken by researchers to implement data protection procedures. In the meantime, please remember the following "best practice requirements":

1. All researchers should review the provisions of BPM 75 (see <http://www.utsystem.edu/bpm/75.htm>).

DRAFT

June 19, 2006

Page 2

2. Each Lead Researcher at The University of Texas at Austin is responsible for implementing BPM 75 for all digital research data under that researcher's control.
3. The Information Security Office will provide to you and your departmental information technology (IT) staff the support and guidance needed to implement BPM 75. Please consult your departmental IT contact if you have questions or seek information about available services.
4. Research staff should report to the Lead Researcher any concerns they have regarding security of the digital research data with which they are involved. The Lead Researcher should take immediate action to ensure that the data are fully protected.
5. Digital research data should be backed up at regular intervals (daily or at least monthly, depending upon the nature of the data) on secured sites (e.g., secured servers or alternate internal drives).
6. The Minimum Security Standards found at <http://www.utexas.edu/its/policies/opsmanual/secstd.html> are mandatory and must be implemented for all servers, workstations, laptops, etc. They include, but are not limited to these three points:
 - Anti-virus software must be installed and enabled.
 - Operating system and application services security patches should be installed as they become available.
 - Access to digital research data should be password protected with strong passwords. Review the password guidelines available at: <http://www.utexas.edu/its/policies/opsmanual/index.html#sec16>.
7. Offices or labs that house digital research data must be secured and Lead Researchers should provide access only to authorized users.
8. For research involving human subjects, as well as any other data that involve confidential and sensitive information, the identifiers must be separated from the digital research data so that no one can link the data with specific individuals.
9. Records that contain digital research data (e.g., disks, hard drives) must be discarded in a way that protects the confidentiality of the data and in accordance with the University's records retention schedule.

DRAFT

June 19, 2006

Page 3

Ultimately, all Lead Researchers at the University have the responsibility to protect the confidentiality and integrity of the research data under their control. However, departmental IT staff are preparing to support your implementation of BPM 75. Your cooperation in helping the University set the highest standards of accountability is greatly appreciated.

cc: Dr. Sheldon Ekland-Olson, Executive Vice President and Provost
Dr. Juan Sanchez, Vice President for Research
Mr. Kevin Hegarty, Vice President and Chief Financial Officer
Ms. Patricia Ohlendorf, Vice President for Institutional Relations
and Legal Affairs
Mr. Dan Updegrove, Vice President for Information Technology
Mr. Jeff Graves, Associate Vice President for Institutional
Relations and Legal Affairs
Dr. Brian Roberts, Interim Associate Vice President for Information
Technology