Attachment A

Requests for Information by Members of the UT System Board of Regents to UT System Institutions
Made From 12/20/13 to 1/31/14 and Earlier Pending Requests

Req. #	Request	Requesting Regents/Date	Request Reviewed by Board Chairman and Chancellor	Executive Officer Who Placed the Request to Institution	Title/Contract Information	Date Request Sent to Institution	Deadline Set by the Original Requestor	Estimated Response Date Provided by the Institution	Explanation as to the Need or Benefit from the Information	Date Information Provided	Number of Pages Provided
10	Statement of work or contract used by UT Austin to hire the firm tasked with determining the organizational structure needed for recruiting a Vice President for Development	Hall, Wallace (1/28/14)	Yes	Safady, Randa	Vice Chancellor for External Relations (512) 499-4777	1/29/14	None	None	Not Provided by the Requesting Regent	Pending	
9	Proposal submitted by firm hired to determine the organizational structure needed for recruiting a Vice President for Development at UT Austin	Hall, Wallace (1/23/14)	Yes	Safady, Randa	Vice Chancellor for External Relations (512) 499-4777	1/24/14	None	None	Not Provided by the Requesting Regent	1/28/2014 (still open)	10
8	Statistics on applicants accepted and enrolled at the UT Law School requested as part of inquiry by Dan Sharphorn, Vice Chancellor and General Counsel, ad interim	Powell, Gene (1/13/14)	Yes	n/a	n/a	n/a	n/a	n/a	Not Provided by the Requesting Regent	Pending	
7	Answers to questions regarding proposed contract terms for Coach Strong and prior athletic statistics (request withdrawn)	Hall, Wallace (1/12/14)	Yes	Sharphorn, Dan	Vice Chancellor and General Counsel, ad interim (512) 499-4462	1/12/14	None	None	Not Provided by the Requesting Regent	Answers not provided by UT Austin; request was withdrawn by Regent Hall as moot	n/a

Compiled By: Office of the Board of Regents
Date Prepared: January 31, 2014

Requests for Information by Members of the UT System Board of Regents to UT System Institutions
Made From 12/20/13 to 1/31/14 and Earlier Pending Requests

Req. #	Request	Requesting Regents/Date	Request Reviewed by Board Chairman and Chancellor	Executive Officer Who Placed the Request to Institution	Title/Contract Information	Date Request Sent to Institution	Deadline Set by the Original Requestor	Estimated Response Date Provided by the Institution	Explanation as to the Need or Benefit from the Information	Date Information Provided	Number of Pages Provided
6	A copy of Coach Strong's contract with University of Louisville	Powell, Gene (1/11/14)	Yes	Sharphorn, Dan	Vice Chancellor and General Counsel, ad interim (512) 499-4462	1/12/14	None	None	Not Provided by the Requesting Regent	1/12/2014 (closed)	13
5	The most recent information on admission statistics for UT Austin undergraduates requested as part of inquiry by Dan Sharphorn, Vice Chancellor and General Counsel, ad interim	Hall, Wallace (1/10/14)	Yes	n/a	n/a	n/a	n/a	n/a	Not Provided by the Requesting Regent	Pending	n/a
4	Information about the procurement of services from Accenture by UT Austin for the Business Productivity Committee (Vice Chairman Gene Powell asked on 1/14/14 to be copied on the responses to this request)	Hall, Wallace (1/9/14)	Yes	Reyes, Pedro	Executive Vice Chancellor for Academic Affairs (512) 499-4237	1/17/14	None	None	Not Provided by the Requesting Regent	1/10/2014 (still open)	43

Requests for Information by Members of the UT System Board of Regents to UT System Institutions
Made From 12/20/13 to 1/31/14 and Earlier Pending Requests

Req. #	Request	Requesting Regents/Date	Request Reviewed by Board Chairman and Chancellor	Executive Officer Who Placed the Request to Institution	Title/Contract Information	Date Request Sent to Institution	Deadline Set by the Original Requestor	Estimated Response Date Provided by the Institution	Explanation as to the Need or Benefit from the Information	Date Information Provided	Number of Pages Provided
3	What services are outsourced at UT System institutions	Cranberg, Alex (10/18/13)	Yes	Kelley, Scott	Executive Vice Chancellor for Business Affairs. (512) 499-4560	1/10/14	None	None	Not Provided by the Requesting Regent	1/29/2014 (closed)	14
2	Information about the deliverables provided by Accenture to UT Austin's Business Productivity Committee (Vice Chairman Gene Powell asked on 1/14/14 to be copied on the responses and Regent Alex Cranberg asked for copies of the deliverables on 10/12/13)	Hall, Wallace (7/12/13)	Yes	Reyes, Pedro	Executive Vice Chancellor for Academic Affairs (512) 499-4237	7/12/13 10/30/13 12/16/13 12/18/13 1/8/14 1/17/14	None	None	Not Provided by the Requesting Regent	Pending	

Compiled By: Office of the Board of Regents
Date Prepared: January 31, 2014

Requests for Information by Members of the UT System Board of Regents to UT System Institutions
Made From 12/20/13 to 1/31/14 and Earlier Pending Requests

Req. #	Request	Requesting Regents/Date	Request Reviewed by Board Chairman and Chancellor	Executive Officer Who Placed the Request to Institution	Title/Contract Information	Date Request Sent to Institution	Deadline Set by the Original Requestor	Estimated Response Date Provided by the Institution	Explanation as to the Need or Benefit from the Information	Date Information Provided	Number of Pages Provided
1	Information related to gifts of transportation, lodging, or food associated with travel for business, personal, or outside board-related activities accepted by or on behalf of President Powers from any individual other than a family member since the start of his presidency	Hall, Wallace (7/11/13)	Yes	Pedro Reyes	Executive Vice Chancellor for Academic Affairs (512) 499-4237	7/26/13 8/30/13 9/13/13 10/18/13 11/13/13 1/8/14	None	None	Not Provided by the Requesting Regent	10/26/13 12/17/13 1/22/14 (Still Open)	61

Attachment B

6. **U. T. System Board of Regents: Discussion and appropriate action regarding amendment of Regents' *Rules and Regulations*, Rule 10101 (Authority) and Rule 10403 (to be retitled as Public Statements on Behalf of the Board); and adoption of proposed new Rule 10801 (Policy on Transparency, Accountability, and Access to Information)**

RECOMMENDATION

Chairman Foster recommends amendments to the Regents' *Rules and Regulations*, Rule 10101 (Authority) and Rule 10403 (Procedure), and adoption of new Rule 10801 (Policy on Transparency, Accountability, and Access to Information), concerning access to and requests for information, email addresses and accounts for U. T. System business, and official statements and coordination of press activities, as set forth in congressional style on the following pages.

BACKGROUND INFORMATION

Proposed revisions to Rule 10101 contains clarifications to current language on Board authority and duties including a new Section 5 related to records and information management. Section 5 covers compliance with System policies on records retention and information management and on encryption, retention, destruction, and release of documents. Section 5 also mandates related training and the establishment of a U. T. System email address for each Regent. It is recommended that the Board require any email messages sent by a U. T. employee to a Regent on a matter of public policy or U. T. business be sent only to the Regent's U. T. email address.

Proposed changes to Rule 10403 clarify who may speak on behalf of the Board and the System and set the expectation that Regents will coordinate media contacts with the Office of External Relations.

Chairman Foster also recommends the enactment of a new Rule 10801, intended to complement the numerous ongoing U. T. System transparency initiatives including enhanced data-gathering, data management, and access to data through the U. T. System's electronic Productivity Dashboard.

- The proposed new Rule acknowledges the need for a comprehensive plan and the capacity to make voluminous documents and a growing repository of data readily available for review, as appropriate, by all requestors – including the public, representatives of the media, members of the Legislature, and members of the Board of Regents.

- The recommended new Rule envisions a plan for significantly improving data management and access with the goals of increasing transparency and accountability while reducing administrative burdens through an orderly and efficient method of records management and production. For members of the Board seeking information, the proposed Rule formalizes a request process that facilitates discussion with the Chairman, the Chancellor, and the requesting Regent to assist in avoiding duplication of efforts and to work together to set the scope and deadlines for production in the context of System strategic priorities. The proposed Rule is not intended to prevent a member of the Board from access to information or data the Regent deems necessary to fulfill his or her official duties but to ultimately make more information and data readily available for all.

- Benefits expected include providing quicker access to data in a format more conducive to analytical review; making the best information available to decision-makers to fulfill their responsibilities; reducing workload on U. T. System and institutional staff members; providing better access to and use of the increasing amounts of data being collected by the U. T. System Administration and the U. T. System institutions; and allowing researchers to identify important challenges, patterns, and opportunities.

- U. T. System Administration and U. T. System institutions currently provide Web access to a listing of all requests made under the Texas Public Information Act from at least early 2013. The new Rule directs the U. T. System to look to identify improvement to the websites. As one facet of the enhanced access, the U. T. System will pilot a phased program to provide access to the actual documents responsive to each of the requests, to the extent feasible and legally permitted. The existing System Administration website may be accessed at http://www.utsystem.edu/.

The University of Texas System
Rules and Regulations of the Board of Regents **Rule: 10101**

1. Title

Board Authority and Duties

2. Rule and Regulation

Sec. 1 Authority of the Board. The Legislature, which is given the duty and authority to provide for the maintenance, support, and direction of The University of Texas by Article VII, Section 10 of the Texas Constitution, has delegated the power and authority to govern, operate, support, and maintain ~~administer~~ The University of Texas System to the Board of Regents. (See *Texas Education Code* Section 65.11 et seq. and Section 51.352) Texas court cases construing these statutes have held that the Board has wide discretion in exercising its power and authority and that the rules adopted by the Board have the same force as statutes. The System's lands and buildings are State of Texas property subject to the control of the Board as the State's agent.

Sec. 2 Amendment or Suspension of Rules. The Regents' *Rules and Regulations* may be added to, amended, waived, or suspended by a majority of all of the members of the Board of Regents present at any regular meeting or at any special meeting called for that purpose.

Sec. 3 ~~Communication with Staff and Faculty~~ Duties and Responsibilities of Each Regent.

3.1 In carrying out the duties and responsibilities referenced in Section 1 above, it ~~I~~t is the responsibility of each Regent to be knowledgeable in some detail regarding the operations, management, finances, and effectiveness of the academic, research, and public service programs of the U. T. System, and each member ~~members~~ of the Board of Regents has the right and authority to inform himself/herself ~~themselves~~ as to the ~~their~~ duties, responsibilities, and obligations of the member in such a manner as they each may deem proper. Members of the Board of Regents are to be provided access to such information as in their individual judgments will enable them to fulfill their duties and responsibilities as Regents of the U. T. System. (Moved from Regents' Rule 10403, Section 5)

3.2 Information requests for data or for the compilation of information by an individual member of the Board will be processed in compliance with Regents' Rule 10801 concerning Transparency, Accountability, and Access to Information.

The University of Texas System
Rules and Regulations of the Board of Regents **Rule: 10101**

Sec. 4 Communication with Faculty, ~~and~~ Staff, and Administration. Members of the Board of Regents are to be provided access to such personnel as in their individual judgments will enable them to fulfill their duties and responsibilities as Regents of the U. T. System. The regular channel of communication from members of the Board to the faculty, staff, and administration is through the Chancellor, the appropriate Executive Vice Chancellor, and the president of the institution involved, and a copy of any communication sent by a Regent directly to any member of the faculty, staff, or administration should be furnished to the Chancellor, the appropriate Executive Vice Chancellor, and the president of the institution involved; however, individual Board members are not precluded from direct participation and communication with the presidents, faculty, staff, and students of the U. T. System. (Moved from Regents' Rule 10403, Section 5)

Sec. 5 Records and Information Management. Members of the Board of Regents shall comply with the Systemwide policies regarding records retention and information management, including System Administration policies on encryption, retention, destruction, and release of documents.

5.1 In addition to required training under State law, each member of the Board will be provided training on records and document management, including compliance with U. T. System records and retention policies.

5.2 U. T. System Administration will provide a U. T. System email address and account to each Regent at the beginning of service as a member of the Board of Regents. Members of the Board are strongly encouraged to use U. T. System email addresses for all communications related to public business or public policy over which the Board of Regents has supervision or control.

5.3 Any email messages sent by a U. T. System employee to a member of the Board of Regents and related to public policy or U. T. business will be sent to the Regent's U. T. System email address.

The University of Texas System
Rules and Regulations of the Board of Regents **Rule: 10403**

1. Title

~~Procedure~~ Public Statements on Behalf of the Board

2. Rule and Regulation

. . .

Sec. 10 ~~Political or~~ Public Statements on Controversial Matters. The Board of Regents acts to determine the ~~reserves to itself the responsibility for passing upon matters of a political or obviously controversial nature, which represent an~~ official position of the U. T. System or the Board of Regents on matters of an obviously controversial nature ~~any institution or department thereof~~.

10.1 Statements on such matters shall be made by the Chairman of the Board or the Chancellor.

10.2 Except as allowed under Section 10.1 ~~Without the advance approval of the Board~~, no Regent, officer, or employee ~~faculty or staff member~~ shall make or issue any public statement on ~~any political or other subject of~~ an obviously controversial ~~nature~~ subject which might reasonably be construed as a statement of the official position of the U. T. System or the Board of Regents without the advance approval of the Board ~~any institution or department thereof~~. Each institution's Handbook of Operating Procedures may specify the institutional officers authorized to speak on behalf of the institution.

10.3 It is not the intent of this policy statement to stifle the right of freedom of speech of anyone speaking in a personal capacity where that person makes it clear that he or she is not speaking for the U. T. System or the Board of Regents ~~any of the institutions~~. ~~Statements on matters of an emergency nature shall be cleared by the Chancellor with the Chairman of the Board~~. To the extent possible, Regents are expected to coordinate media contacts with and to provide advance notice to the U. T. System Office of External Relations regarding any media contacts and press statements.

. . . .

The University of Texas System
Rules and Regulations of the Board of Regents **Rule: 10801**

1. Title

Policy on Transparency, Accountability, and Access to Information

2. Rule and Regulation

Sec. 1 The Board of Regents and U. T. System Administration are committed to enhancing transparency, accountability, and access and disclosure of information to the public, the media, elected and appointed state and federal officials, and executive policy makers.

Sec. 2 To assist in achieving these goals, the Board wishes to provide maximum transparency to the public and its representatives to the fullest extent allowed by law while ensuring compliance with best governance practices and appropriate protection of confidential information and personal privacy. The Board acknowledges significant U. T. System leadership and progress in expanding access and transparency, supports these ongoing efforts, and recognizes that the efforts will require continuing and long-term commitment.

Sec. 3 The Board requires all U. T. System Administration, U. T. System institutional employees, and members of the Board to respond thoroughly and appropriately to all legal requests for information and in accordance with state and federal laws to all lawful requests. The Board expects all employees to work to achieve and maintain an environment of transparency, cooperation, and compliance with applicable law and policy. The Board will support staffing levels and acquisition of resources necessary and reasonable to implement and achieve the intent of this Rule.

Sec. 4 Enhancement of Access to and Analysis of Data and Information.

4.1 Importance of Data Collection, Retention, and Analysis. The U. T. System recognizes and supports the importance of data collection, retention, and analysis for purposes such as reviewing System operations and policies, guiding decision-making, improving productivity and efficiency, and evaluating performance outcomes.

4.2 Increase in the Amount of Data Available. The U. T. System recognizes that the amount of significant data being accumulated by the U. T. System and U. T. System institutions is expanding exponentially each year. The System further recognizes that current data collection and management systems in use are not sufficient to effectively manage and utilize all data becoming available.

4.3 Opportunities for Additional Enhancements. The U. T. System is continually looking for ways to enhance the performance of its institutions, to support access and success for all students, to improve

educational outcomes, and to remain a national leader in providing access to data. As such, the U. T. System is committed to continue collecting additional data and finding and utilizing new, better and more expansive systems and software with which to manage and access these data. These improved systems and new software will greatly improve the ability to generate better informed decisions to enhance student success, to increase productivity and efficiency, and to facilitate access to and analysis of the data.

4.4 Framework for Advancing Excellence. The Framework, established in 2011, implemented a centralized data warehouse for the purposes of evaluating the progress of U. T. System institutions in achieving the goals set forth in the Framework. The data warehouse is a central source of information for the U. T. System Productivity Dashboard, which specifically supports the goals of transparency and efficiency as expressed in the Framework.

(Framework url: https://www.utsystem.edu/chancellor/speeches/a-framework-for-advancing-excellence-throughout-the-university-of-texas-system)

4.5 Information Accessible through Data Dashboard. The U. T. System Productivity Dashboard provides a rolling 10 years (where available) of data on the performance of all U. T. System institutions and is available free to the public. The Productivity Dashboard provides important data and metrics concerning students, faculty, research and technology transfer, health care, and productivity and efficiency.

(Productivity Dashboard url: http://data.utsystem.edu/)

Sec. 5 Processing Information Requests.

5.1 Requests by Members of the Public. To enhance transparency, U. T. System institutions and U. T. System Administration are expected to act in strict compliance with the Texas Public Information Act (TPIA) and applicable State and federal law in providing public access to governmental records.

5.2 Requests by Representatives of the Media. In addition to the public right of access to information through the TPIA, representatives of the media may utilize U. T. System Administration and institutional offices of external relations as an additional resource for questions.

5.3 Requests by Members of the Texas Legislature. The TPIA provides members of the Texas Legislature a special right of access to information needed for legislative purposes. U. T. System Administration and

institutional offices of governmental affairs serve as additional resources for questions from members of the Legislature.

5.4 Requests by Members of the Board of Regents and Chancellor.

5.4.1 This process is not intended nor will it be implemented to prevent a member of the Board of Regents or the Chancellor from access to information or data that the Board member or Chancellor deems is necessary to fulfill his or her official duties and responsibilities.

5.4.2 Requests by an individual Regent for information shall be submitted to the Chancellor with a copy to the Board Chairman and General Counsel to the Board.

5.4.3 Information requests from or on behalf of an individual member of the Board of Regents seeking the compilation of significant quantities of information or data from a U. T. System institution will be reviewed by the Chairman of the Board and the Chancellor and, if necessary, discussed with the requesting Regent to determine the appropriate scope of the request and timing of the response to avoid inefficiencies and duplication of effort but shall also ensure that requests are fulfilled in a timely manner consistent with applicable law and policy.

5.4.4 Smaller requests for existing information or data that do not appear to require significant time or effort may be processed through the Office of the Board of Regents and the Chancellor's Office.

Sec. 6 Access to Requests for Information.

6.1 The U. T. System Administration is directed to look for opportunities to expand the existing U. T. System websites, established in 2012 to provide public access to requests for information and which include all Texas Public Information Act requests.

(Open Records website: http://www.utsystem.edu/open-records?src=uts-homepage)

6.2 It is the intent of the Board that documents responsive to those requests be made available electronically to the extent legal and feasible, with the Chancellor to set timelines for implementation, in consultation with the Chairman.

Attachment C

1. Title

Records and Information Management

2. Policy

Sec. 1 *Handbook of Operating Procedures.* A Records and Information Management policy is to be included in institutional *Handbooks of Operating Procedures.*

Sec. 2 Records Retention Schedule. The University of Texas System recognizes the need for orderly management and retrieval of all official State records and a documented records retention schedule in compliance with all State and federal laws and related regulations. All official records (paper, microform, electronic, including all electronically stored information (ESI), or any other media) will be retained for the retention periods stated in the institutional Records Retention Schedule as approved by the Texas State Library and Archives Commission and the Texas State Auditor's Office in compliance with *Texas Government Code*, Chapter 441. After a specified period of time, official records must be disposed of in a manner that is consistent with, and systematically carried out in accordance with prescribed records and information management guidelines and procedures.

Sec. 3 Convenience Copies. Convenience copies, library materials, and stocks of obsolete forms or pamphlets originally intended for distribution are not considered to be official State records. Convenience copies should be destroyed when they cease to be useful and should never be kept longer than the official record copy.

Sec. 4 Responsibility for State Records. The Chancellor and each institutional president, as State agency heads, are responsible for the proper management of State records as outlined in *Texas Government Code*, Chapter 441.

Sec. 5 Agency's Representative. The Records Management Officer (RMO) acts as the agency's representative in all issues of records and information management policy, responsibility, and statutory compliance pursuant to *Texas Government Code* Section 441.184.

Sec. 6 Records Retention Schedule. The institutional Records Retention Schedule provides a list of official State records for each department on the campus and prescribes the periods of authorized retention. The schedule may be revised periodically to include a newly created records series, to change retention periods, or to delete a records

series no longer held. Appropriate approval procedures must be followed and completed before any revisions would become effective.

Minimum Holding Period. All records are to be kept for the minimum periods listed in the Records Retention Schedule. Notwithstanding such minimum retention periods, an official State record whose retention period has expired may not be destroyed if any litigation, claim, negotiation, audit, public information request, administrative review, or other action involving the record is initiated; its destruction shall not occur until the completion of the action and the resolution of all issues that arise from it.

6.1 An official State record whose retention period expires during any litigation, claim, negotiation, audit, public information request, administrative review, or other action involving the record may not be destroyed until the completion of the action and the resolution of all issues that arise from it.

6.2 Documents may be maintained for the prescribed retention periods in microform if the microform reproduction is accomplished pursuant to a procedure that complies with *Texas Government Code* Section 441.188 and 13 *Texas Administrative Code* Sections 6.21-6.35.

6.3 Official records kept only in electronic format must be identified and must comply with the administrative rules of the Texas State Library (13 *Texas Administrative Code* Sections 6.91-6.97).

6.4 Vital records should be identified and protected in accordance with *Texas Government Code* Section 441.183.

6.5 Archival documents should be identified in the Retention Schedule and maintained in accordance with *Texas Government Code* Section 441.181. Archival or historical records are to be preserved in the archives of the institution.

Sec. 7. Destruction of State Records. No official State records may be destroyed without permission from the Texas State Library as outlined in *Texas Government Code* Section 441.187 and 13 *Texas Administrative Code* Section 6.7. The Texas State Library has two established methods for obtaining legal authority to destroy State records. Procedures differ for records listed on an approved Records Retention Schedule and any records not listed.

7.1 Reasons for Not Destroying on Disposal Date. A State record may not be destroyed if any litigation, claim, negotiation, audit, open records request, administrative review, or other action involving the record is initiated before the expiration of the retention period for the record set in the approved institutional Records Retention Schedule. If no action as described above has been taken, records may be destroyed in accordance with the approved retention periods shown in the Records Retention Schedule. Prior to disposal of official records, all State and institutional records and information management regulations and policies must be followed.

7.2 Disposal of Records Not on Retention Schedule. State records not listed on the approved Records Retention Schedule may be destroyed after receiving approval by officials at the Texas State Library. The Form RMD 102, Request for Authority to Dispose of State Records, must be completed and submitted to the Records Management Division of the Texas State Library to obtain approval for the destruction of such official State records. Unlisted records must not be destroyed until the State Library Administrator approves and returns the form to the appropriate University officials.

Sec. 8 Release of Records (Texas Public Information Act). Under provisions of the Texas Public Information Act (*Texas Government Code*, Chapter 552), the Chancellor and the president of each U. T. System institution may delegate their authority as the custodians of records to Public Information Officers. The Chancellor has designated the Vice Chancellor and General Counsel as the Public Information Officer at U. T. System Administration. The Public Information Officer at each institution is the institution's chief business officer unless another individual is so designated in accordance with the procedures outlined in UTS139, *Texas Public Information Act*.

Requests for Records. Written requests for documents under the Texas Public Information Act should be directed to the Public Information Officer and handled immediately pursuant to the provisions of the Act and UTS139, *Texas Public Information Act*.

Sec. 9 Records Management Officer (RMO). State law requires each State agency to appoint a RMO to act as the agency's representative on all issues of records and information management policy, responsibility, and statutory compliance pursuant to *Texas Government Code* Section 441.184. The RMO from System Administration and from each institution will each submit their records retention schedules directly to the State Library for approval and recertification in accordance with

Texas Government Code 441.185 and 13 *Texas Administrative Code* Sections 6.1-6.10.

U. T. System Administration's RMO. The RMO at U. T. System Administration serves as coordinator of meetings of U. T. System and the institutions to collaborate on records and information management issues. In addition, the U. T. System RMO is available to assist institutional RMOs and any staff who are assigned records and information management responsibilities.

3. Definitions

Vital State Record - any State record necessary to the resumption or continuation of State agency operations in an emergency or disaster, the recreation of the legal and financial status of the agency, or the protection and fulfillment of obligations to the people of the state.

Archival State Record - any State record of enduring value that will be preserved on a continuing basis by the institutional archives until its archivist indicates that based on a reappraisal of the record it no longer merits further retention.

Confidential State Record - any State record to which public access is or may be restricted or denied under *Texas Government Code*, Chapter 552 or other State or federal law.

4. Relevant Federal and State Statutes

Texas Government Code, Chapter 441

Texas Administrative Code Sections 6.91-6.97

Texas Government Code, Chapter 552

5. Relevant System Policies, Procedures, and Forms

UTS139, *Texas Public Information Act*

Form RMD 102, Request for Authority to Dispose of State Records

SLR 104: Designation of State Agency Records Management Officer (RMO)

SLR 105: Records Retention Schedule

SLR 105C: Records Retention Schedule Certification

SLR 122: Records Retention Schedule Amendment

Records Retention Schedule for State Agencies, 4th Edition
Effective September 1, 2007

6. System Administration Office(s) Responsible for Policy

Office of Technology and Information Services

7. Dates Approved or Amended

August 8, 1998
September 30, 2009
March 10, 2011

8. Contact Information

Questions or comments about this policy should be directed to:

- bor@utsystem.edu

1. Title

Texas Public Information Act

2. Policy

Sec. 1 State Law. It is the policy of the State of Texas that each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees in accordance with the Texas Public Information Act ("the Act"), *Texas Government Code,* Chapter 552. This procedure shall be liberally construed in favor of granting a request for information.

Sec. 2 Applicability. A subpoena duces tecum or a request for discovery that is issued in compliance with a statute or a rule of civil or criminal procedures is not considered to be a request for information under the Act and is not subject to this procedure. A request for documents pursuant to an institutional hearing is considered to be a request for information under the Act.

Sec. 3 Procedures. The following sets forth procedures to be followed by The University of Texas System ("U. T. System") for complying with the Act. For purposes of this procedure, U. T. System includes U. T. System Administration ("System Administration") and the institutions. The term "institutions" refers to the general academic and health related institutions that comprise U. T. System. The generic term "institution" referenced throughout this procedure refers to System Administration and the institutions. It is the responsibility of System Administration and the institutions to properly instruct its employees regarding compliance with these procedures and the Act.

Sec. 4 Officers for Public Information and Designated Agents.

4.1 Delegation of Authority. The Texas Public Information Act designates the chief administrative officer of a governmental body as the officer for public information. The Chancellor of the U. T. System is the officer for public information for System Administration. The president of each institution is the officer for public information for his or her institution. The Chancellor and the president of each institution delegate their authority under the Act to the appropriate Public Information Officer as defined below.

4.2 Public Information Officer. The Public Information Officer of System Administration is the Vice Chancellor and General

Counsel or designee; the Public Information Officer of each institution is the institution's chief business officer or another institution officer designated in writing by the institution's president.

4.3 Notification. If an individual other than the chief business officer is designated by an institution, the president will notify the Vice Chancellor and General Counsel with a copy as appropriate to the Executive Vice Chancellor for Academic Affairs or the Executive Vice Chancellor for Health Affairs.

4.4 Designated Agent. The Public Information Officer ("officer") is the designated agent for coordinating responses to requests for public information appropriately submitted to his or her respective institution.

Sec. 5 General Duties of Public Information Officer.

5.1 Availability, Protection, and Maintenance of Information. The Public Information Officer shall make public information available for public inspection and copying; carefully protect public information from deterioration, alteration, mutilation, loss, or unlawful removal; and repair, renovate, or rebind public information as necessary to maintain it properly.

5.2 Limitations. The officer may not inquire into the purpose for which the information will be used or make other inquiry of a requestor except to establish proper identification or as follows:

(a) if information requested in unclear, the requestor may be asked to clarify the request; and

(b) if a large amount of information has been requested, the requestor may be asked how the scope of the request might be narrowed.

5.3 Requests for Clarification. All inquiries to the requestor for clarification or narrowing of a request shall be made in writing and may be sent via email or via facsimile transmission. If the requestor's request for information included the requestor's physical or mailing address, the communication shall be sent by certified mail to the requestor's physical or mailing address. The communication must state that all responses to the inquiry must also be made in writing and returned to the U. T. System by mail, email, or via facsimile transmission and that failure to respond in a timely manner may result in the request being

considered withdrawn. If the officer does not receive a written response from the requestor by the 61st day after the date the written request for clarification or narrowing is sent, the request for public information is considered to have been withdrawn by the requestor.

5.4 Uniform Treatment of Requests. The Public Information Officer shall treat all requests for information uniformly without regard to the position or occupation of the requestor, the person on whom behalf the request is made, or the status of the individual as a member of the media. The Act provides that U. T. System is not required to accept or comply with a request for information from an individual who is imprisoned or confined in a correctional facility.

5.5 Comfort and Facility. The Public Information Officer shall give to the requestor all reasonable comfort and facility for the full exercise of the rights granted by the Act.

Sec. 6 Sign. The Public Information Officer shall prominently display a sign in the form prescribed by the Attorney General that contains basic information about the rights of a requestor, the responsibilities of a governmental body, and the procedures for inspecting or obtaining a copy of public information. The officer shall display the sign at one or more places in administrative offices of the institution where it is plainly visible to:

6.1 members of the public who request public information in person; and

6.2 employees whose duties include receiving or responding to public information requests.

Sec. 7 Receiving and Referring Requests.

7.1 Written Requests. All requests for public information must be received in writing. For purposes of this Act, a written request includes a request made in writing that is sent by the requestor to the chief administrative officer, the Public Information Officer, or the person designated by the Public Information Officer, by regular mail, electronic mail, or facsimile transmission.

7.2 Forwarding of Requests. Any official or other employee receiving a written request for information via regular mail or hand-delivery must forward it immediately to the Public Information Officer.

7.3 Email and Facsimile Requests. Email and facsimile requests are not valid unless sent directly by the requestor to the Public Information Officer or his or her designee.

7.4 Submission to Public Information Officer. Individuals contacting System Administration with written or verbal inquiries regarding public information held by an institution should be advised to submit their requests in writing directly to the Public Information Officer of the appropriate institution.

Sec. 8 Routine Requests.

8.1 Compliance. When it is clear from the request that requested information is not excepted from required disclosure, the Public Information Officer should respond or coordinate responses to the request, notifying the chief administrative officer as appropriate. The Public Information Officer should promptly produce public information for inspection, duplication, or both, on application by any person. Public Information Officers comply with routine requests by:

(a) providing the public information for inspection or duplication in the offices of the institution; or

(b) sending copies of the public information by first class United States mail if the person requesting the information requests that copies be provided by mail and pays the postage and any other charges that the requestor has accrued.

8.2 Charges. Charges for providing a copy of public information are considered to accrue at the time the requestor is advised that the copy is available on payment of the applicable charges.

8.3 Information in Active Use or in Storage. If the requested information is unavailable at the time of the request to examine because it is in active use or in storage, the Public Information Officer shall certify this fact in writing to the requestor and set a date and hour within a reasonable time when the information will be available for inspection or duplication.

8.4 Request for Additional Time. If the requested information cannot be produced for inspection or duplication within 10 business days after the date the information is requested, the Public Information Officer shall certify that fact in writing to the requestor and set a date and hour within a reasonable time

when the information will be available for inspection or duplication.

8.5 Time Limitations. A requestor must complete the examination of the information not later than the 10th business day after the date the information is made available. If the requestor does not complete the examination of the information within 10 business days after the date the information is made available and does not file a request for additional time as follows, the requestor is considered to have withdrawn the request. The Public Information Officer shall extend the initial examination period by an additional 10 business days if, within the initial period, the requestor files a written request for additional time. The period must be extended by another 10 business days if, within the additional period, the requestor files a written request for more additional time.

8.6 Electronic or Magnetic Medium. If public information exists in an electronic or magnetic medium, the requestor may request a copy either on paper or in an electronic medium, such as on diskette or on magnetic tape. The Public Information Officer shall provide a copy in the requested medium if:

(a) the institution has the technological ability to produce a copy of the requested information in the requested medium;

(b) the institution is not required to purchase any software or hardware to accommodate the request; and

(c) provision of a copy of the information in the requested medium will not violate the terms of any copyright agreement between the institution and a third party.

8.7 Paper or Other Medium. If the institution is unable to comply with the request to produce a copy of information in a requested medium for any of the reasons described above, the institution must provide a paper copy of the requested information or a copy in another medium that is acceptable to the requestor. The institution is not required to copy information onto a diskette or other material provided by the requestor but may use its own supplies.

8.8 Written Statement. The Public Information Officer must provide the written statement to a requestor described below if the institution determines:

(a) that responding to a request for public information will require programming or manipulation of data; and

(b) that:

i. compliance with the request is not feasible or will result in substantial interference with its ongoing operations; or

ii. the information could be made available in the requested form only at a cost that covers the programming and manipulation of data.

8.9 Information for Written Statement. The written statement must include:

(a) a statement that the information is not available in the requested form;

(b) a description of the form in which the information is available;

(c) a description of any contract or services that would be required to provide the information in the requested form;

(d) a statement of the estimated cost of providing the information in the requested form, as determined in accordance with the guidelines for specifying charges for access to public information; and

(e) a statement of the anticipated time required to provide the information in the requested form.

8.10 Timing of Written Statement. The institution shall provide this written statement to the requestor within 20 days after the date of the institution's receipt of the request. The institution has an additional 10 days to provide the statement if written notice is given to the requestor, within 20 days after the date of receipt of the request, that the additional time is needed.

8.11 Requestor Response. After providing the written statement to the requestor as required above, the institution does not have any further obligation to provide the information in the requested form or in the form in which it is available unless within 30 days the requestor informs the institution in writing that the requestor:

(a) wants the governmental body to provide the information in the requested form according to the cost and time

parameters set out in the statement or according to other terms to which the requestor and the governmental body agree; or

(b) wants the information in the form in which it is available.

8.12 Withdrawal of Request. If a requestor does not make a timely written statement as specified above, the requestor is considered to have withdrawn the request for information.

8.13 Maintenance of Written Statements. The Public Information Officer must maintain a file containing all written statements issued pursuant to instructions above in a readily accessible location.

Sec. 9 Nonroutine Requests.

9.1 Consultation for Disclosure Exceptions. When it is not clear whether requested information is excepted from required disclosure by the Public Information Act, the Public Information Officer for the general academic and health related institutions shall consult with the Office of General Counsel within the time frames outlined below to determine whether the records in question should be withheld or released.

9.2 Attorney General Decisions. Subchapter C of the Public Information Act excepts a number of categories of information from required disclosure. On determination by the Office of General Counsel that requested information falls within one of these excepted categories, the Office of General Counsel shall forward a request for a decision to the Attorney General to confirm that such information shall be withheld from public disclosure. On determination by the Office of General Counsel that that requested information does not fall within one of the excepted categories, the request shall be processed following procedures specified above for a routine request.

Sec. 10 Requests for Personal Information.

10.1 Special Right of Access to Confidential Information. Information related to the person and that is held by the institution and protected from public disclosure by laws intended to protect that person's privacy interests will be disclosed to the person or the person's authorized representative in accordance with Sections 552.023, 552.229, and 552.307 of the Act. A person may also request to be informed about information that the

institution collects about the individual, as provided by Section 559.003(a)(1) of the *Texas Government Code*. Requests for information should be made in accordance with Section 7 of this policy. Nothing in this policy shall allow an individual access to information to which access is denied by the Act or by other law.

10.2 Right to Request Correction of Incorrect Information.

(a) A person is entitled to have the institution correct information about the individual that is incorrect in accordance with the following procedures that are established in accordance with Section 559.004 of the *Texas Government Code*. This policy does not apply to an employee of the U. T. System who seeks to correct information in that employee's personnel file; such an employee should comply with the institution's grievance process.

(b) The person should request in writing that the institution correct information about the person that is held by the institution that is incorrect. The request should specifically identify (1) the information that the person believes to be incorrect, and (2) the document or other source in which the information is located. The request also should specify the correction that the person requests. Requests for corrections should be made in accordance with Section 7 of this policy.

(c) Not later than 10 days (excluding Saturdays, Sundays, and State and national legal holidays) after the date of the Public Information Officer's receipt of the request for correction, the Public Information Officer shall acknowledge in writing the receipt of the request. The Public Information Officer thereafter shall promptly either make the correction to the information as identified by the person or inform the person of the officer's refusal to amend the information in accordance with the person's request, the reason for the refusal, and the name and address of the official to whom the person may request a review of the refusal. The designated official will be the Chancellor or the president, as appropriate, or his or her designee.

(d) If the person disagrees with the refusal of the Public Information Officer to amend the information, the person may request in writing to the designated official a review of the refusal. Not later than 30 days (excluding Saturdays, Sundays, and State and national legal holidays) after the

date of the designated official's receipt of the request for review, the official shall complete a review of the matter and make a final determination unless, for good cause, the official extends the thirty-day period.

(e) The institution will make approved corrections in accordance with all applicable laws and regulations, including those pertaining to records retention. The institution may make approved corrections by adding a document that amends but does not replace the document containing the incorrect information.

Sec. 11 Responding to Repetitious or Redundant Requests.

11.1 Certifications. If the Public Information Officer determines that a requestor has made a request for information for which the institution has previously furnished copies to the requestor or made copies available to the requestor on payment of applicable charges, the Public Information Officer may respond to the request by certifying to the requestor that copies of all or part of the requested information, as applicable, were previously furnished to the requestor or made available. The certification must include:

(a) a description of the information for which copies have been previously furnished or made available to the requestor;

(b) the date that the institution received the requestor's original request for that information;

(c) the date that the institution previously furnished copies of or made available copies of the information to the requestor;

(d) a certification that no subsequent additions, deletions, or corrections have been made to that information; and

(e) the name, title, and signature of the Public Information Officer or the officer's agent making the certification.

11.2 Charges. A charge may not be imposed for making and furnishing the certification. Information not furnished in the previous request must be furnished for the new request.

Sec. 12 Requests Requiring More Than 36 Hours of Personnel Time (36 Hour Rule).

12.1 36 Hour Rule. Each requestor is limited to 36 hours of time per 12-month fiscal year that personnel of the institution are required to spend producing public information for inspection and duplication, or providing copies of public information to the requestor, without recovering its costs attributable to that personnel time.

12.2 Written Statements. Each time the institution complies with a request for public information, the institution shall provide the requestor with a written statement of the amount of personnel time spent complying with that request and the cumulative amount of time spent complying with requests for public information from that requestor during the applicable 12-month period. The requestor may not be charged for the amount of time spent preparing the written statement.

12.3 Written Cost Estimates. If, in connection with a request for public information, the cumulative amount of personnel time spent complying with requests for public information from the same requestor is expected to equal or exceed 36 hours, the institution shall provide the requestor with a written estimate of the total cost, including materials, personnel time, and overhead expenses necessary to comply with the request. The written estimate must be provided to the requestor on or before the 10th day after the date on which the public information was requested. If the institution determines that additional time is required to prepare the written estimate and provides the requestor with a written statement of that determination, the institution must provide the written statement as soon as practicable, but on or before the 10th day after the date the institution provided the notice that additional time was required.

12.4 Calculation of Costs. The costs charged for personnel time relating to the cost of locating, compiling, and producing the public information shall be calculated at the rates set by the Texas Attorney General's Office. A summary of the charges is available as Attachment 1. When calculating the amount of time spent complying with an individual's public information request(s), the institution may not include time spent on:

(a) determining the meaning and/or scope of the request(s);

(b) requesting a clarification from the requestor;

(c) comparing records gathered from different sources;

(d) determining which exceptions to disclosure, if any, may apply to information that is responsive to the request(s);

(e) preparing the information and/or correspondence required for an Attorney General decision;

(f) reordering, reorganizing, or in any other way bringing information into compliance with well established and generally accepted information management practices; or

(g) providing instruction to, or learning by, employees or agents of the institution of new practices, rules, and/or procedures, including the management of electronic records.

12.5 Payment by Requestor. If an institution provides a requestor with a written statement estimating the cost of personnel time to complete the requestor's request, the institution is not required to produce public information for inspection or duplication or to provide copies of public information in response to the requestor's request unless on or before the 10th day after the date the written statement was sent, the requestor submits a statement in writing to the governmental body in which the requestor commits to pay the lesser of:

(a) the actual costs incurred in complying with the requestor's request, including the cost of materials and personnel time and overhead; or

(b) the amount stated in the written statement.

12.6 Withdrawal of Request. If the requestor fails or refuses to submit a written commitment to pay statement, the requestor is considered to have withdrawn the requestor's pending request for public information.

12.7 Exceptions to 36 Hour Rule. This rule does not prohibit institutions from providing a copy of public information without charge or at a reduced rate when it is in the public interest or from waiving a charge for providing a copy of public information when the cost of processing the collection will exceed the amount of the charge. In addition, the 36 hour rule does not apply if the requestor is an individual who, for a substantial portion of the individual's livelihood or for substantial financial gain, gathers, compiles, prepares, collects, photographs, records, writes, edits, reports, investigates, processes, or

publishes news or information for and is seeking the information for:

(a) a radio or television broadcast station that holds a broadcast license for an assigned frequency issued by the Federal Communications Commission;

(b) a newspaper that is qualified under Section 2051.044, *Texas Government Code* to publish legal notices or is a free newspaper of general circulation and that is published at least once a week and available and of interest to the general public in connection with the dissemination of news;

(c) a newspaper of general circulation that is published on the Internet by a news medium engaged in the business of disseminating news or information to the general public; or

(d) a magazine that is published at least once a week or on the Internet by a news medium engaged in the business of disseminating news or information to the general public.

12.8 Additional Exceptions to 36 Hour Rule. Further, the 36 hour rule does not apply if the requestor is:

(a) an elected official of the United States, Texas, or a political subdivision of Texas; or

(b) a representative of a publicly funded legal services organization that is exempt from federal income taxation under Section 501(a), *Internal Revenue Code of 1986*, as amended, by being listed as an exempt entity under Section 501(c)(3) of that Code.

Sec. 13 Itemized Estimate of Charges.

13.1 Written Itemized Statement. If a request for a copy of public information will result in the imposition of a charge that exceeds $40, or a request to inspect a paper record will result in the imposition of a charge that exceeds $40, the institution shall provide the requestor with a written itemized statement that details all estimated charges that will be imposed, including any allowable charges for labor or personnel costs. If an alternative less costly method of viewing the records is available, the statement must include a notice that the requestor may contact the institution regarding the alternative method. The institution must inform the requestor of the responsibilities imposed on the

requestor and of the rights granted and give the requestor the information needed to respond, including:

(a) that the requestor must provide the institution with a mailing, facsimile transmission, or electronic mail address to receive the itemized statement and that it is the requestor's choice which type of address to provide;

(b) that the request is considered automatically withdrawn if the requestor does not respond in writing to the itemized statement and any updated itemized statement in the appropriate time and manner; and

(c) that the requestor may respond to the statement by delivering the written response to the institution by mail, in person, by facsimile transmission, or by electronic mail.

13.2 Withdrawal of Request. A request is considered to have been withdrawn by the requestor if the requestor does not respond in writing to the itemized statement by informing the institution within 10 business days after the date the statement is sent to the requestor that:

(a) the requestor will accept the estimated charges;

(b) the requestor is modifying the request in response to the itemized statement; or

(c) the requestor has sent to the Attorney General a complaint alleging that the requestor has been overcharged for being provided a copy of the public information.

13.3 Updated Itemized Statement. If the institution later determines, but before it makes the copy or the paper record available, that the estimated charges will exceed the charges detailed in the written itemized statement by 20% or more, the institution shall send to the requestor a written updated itemized statement that details all estimated charges that will be imposed, including any allowable charges for labor or personnel costs. If the requestor does not respond in writing to the updated estimate in the time and manner described above, the request is considered to have been withdrawn by the requestor.

If the actual charges that an institution imposes for a copy of public information, or for inspecting a paper record exceeds $40, the charges may not exceed:

(a) the amount estimated in the updated itemized statement; or

(b) if an updated itemized statement is not sent to the requestor, an amount that exceeds by 20% or more the amount estimated in the itemized statement.

13.4 Statement Date. An itemized statement or updated itemized statement is considered to have been sent by the institution to the requestor on the date that:

(a) the statement is delivered to the requestor in person;

(b) the institution deposits the properly addressed statement in the United States mail; or

(c) the institution transmits the properly addressed statement by electronic mail or facsimile transmission, if the requestor agrees to receive the statement by electronic mail or facsimile transmission, as applicable.

13.5 Response Date. A requestor is considered to have responded to the itemized statement or the updated itemized statement on the date that:

(a) the response is delivered to the institution in person;

(b) the requestor deposits the properly addressed response in the United States mail; or

(c) the requestor transmits the properly addressed response to the institution by electronic mail or facsimile transmission.

13.6 Timelines for Attorney General Decisions. These timelines do not affect the deadlines required for requesting an Attorney General's decision.

Sec. 14 Time of the Essence.

14.1 Requests to Attorney General. Institutions seeking to withhold requested information based upon a Subchapter C exception must notify the Office of General Counsel. The Public Information Act provides that a decision regarding applicability of the specified exception must be requested from the Attorney

General within 10 business days from the date that the request is received. Further, the requestor must be provided the following information within the same time frame:

(a) a written statement that the institution wishes to withhold the requested information and has asked for a decision from the Attorney General about whether the information is within an exception to public disclosure; and

(b) a copy of the institution's written communication to the Attorney General asking for the decision or, if the written communication discloses the requested information, a redacted copy of that written communication.

14.2 Requests Not Made to Attorney General Within Time Frame. If a decision of the Attorney General is not requested within 10 business days and the requestor is not provided with the information described in the paragraph above, the information is subject to required public disclosure and must be released unless there is a compelling reason to withhold the information. All related supplementary information required by the Attorney General must be provided not later than 15 business days after the date that the request is received.

14.3 Time Needed for Requests. These deadlines make it imperative that the Office of General Counsel be given as much time as possible to deal with requests to which the legal response is not immediately apparent. Unless the Public Information Officer determines that the requested information is unquestionably disclosable and routinely fills the request, the Office of General Counsel should have at least five business days of the 10-day decision deadline to review the request. In many cases, it may be necessary to compile the requested material, or representative material if filling the entire request is difficult and time consuming, and present it to the Office of General Counsel in order for counsel to make this determination. In all cases where an Attorney General's decision is deemed necessary by the Office of General Counsel, the requested information or representative material must be compiled and provided to the Office of General Counsel for forwarding to the Attorney General along with the request for decision. To facilitate the timely review by the Office of General Counsel, the Public Information Officer should begin compiling the requested information at the same time the Office of General Counsel is first contacted concerning the request.

14.4 Exceptions. All possible exceptions must be communicated to the Office of General Counsel. If an exception is not raised before the Attorney General, it is waived. The only exceptions to waiver are exceptions based on a requirement of federal law or exceptions involving third party property or privacy interests.

Sec. 15. Proprietary Information of a Third Party. If a request is made for information pertaining to a person's proprietary information that may be subject to exception under the Act and a request for Attorney General decision is made by the institution, the Public Information Officer shall make a good faith attempt to notify that person of the request for the Attorney General decision. Notice must:

15.1 be in writing and sent within a reasonable time not later than the 10th business day after the date the institution receives the request for the information; and

15.2 include

(a) a copy of the written request for the information received by the institution; and

(b) a statement, in the form prescribed by the Attorney General, that the person is entitled to submit in writing to the Attorney General within a reasonable time not later than the 10th business day after the date the person receives the notice

i. each reason the person has as to why the information should be withheld; and

ii. a letter, memorandum, or brief in support of that reason.

Sec. 16 News Media Requests.

16.1 Notification to Vice Chancellor for External Relations. An official or other employee of System Administration who receives a request for public information from a representative of the news media is strongly encouraged to inform the Vice Chancellor for External Relations.

16.2 Notification to Chief Administrative Officers. The Vice Chancellor for External Relations will inform the institution chief administrative officer about media requests affecting an institution.

16.3. Coordination of Responses. Public Information Officers are strongly encouraged to coordinate responses to news media

requests with the other Public Information Officers who have received the same or similar requests and, as appropriate, with the Vice Chancellor for External Relations.

Sec. 17 Requests from Legislators and Other Governmental Offices.

17.1 U. T. System Notification to Vice Chancellor for Governmental Relations. The Vice Chancellor and General Counsel shall notify the Vice Chancellor for Governmental Relations when U. T. System receives requests for public information from members of the Legislature or other governmental offices.

17.2 Institutional Notification to Vice Chancellor for Governmental Relations. At the direction of the president of an institution, the Public Information Officer of an institution shall notify the Vice Chancellor for Governmental Relations when the institution receives requests for public information from members of the Legislature or other governmental offices.

Sec. 18 Form and Approval of Responses.

18.1 Review of Requested Information. Except for routine responses, requested information should be reviewed and approved by the chief administrative officer or designee and the Public Information Officer or designee following appropriate consultation with the Office of General Counsel.

18.2 Cover Letters. As a general rule, cover letters responding to requests for public information should be signed by the Public Information Officer or designee.

Sec. 19 Resolution of Questions. Questions regarding the procedure for answering requests for public information should be directed to the Office of General Counsel.

Sec. 20 Recovery Costs and Guidelines.

20.1 Policy. In accordance with Subchapter F of the Act and Title 1 of the *Texas Administrative Code*, it is the policy of The University of Texas System to recover the full costs for retrieving and copying public records. Officers filling requests for public information should account for all costs in fulfilling these requests using the following guidelines.

20.2 Guidelines. The Public Information Officer shall make a preliminary estimate of the cost of retrieving and copying public

records under these guidelines and notify the requestor, giving the requestor the option to (1) agree to the cost and submit necessary prepayment (see Section (b)iii below), (2) alter, or (3) withdraw the request. If charges are in excess of $40, the Public Information Officer should follow the procedures outlined in Section 13. If personnel time will exceed 36 hours, the Public Information Officer should follow the procedures outlined in Section 12.

(a) Definitions: See Definitions section of policy.

(b) The U. T. System adopts the rules for establishing charges to be made for public records set out in the *Texas Administrative Code*, Title 1, and the Act as summarized below:

i. Inspection of Information. Where only inspection of paper documents is requested (i.e., no copies made), no charge may be assessed except when:

A. a requested page contains confidential information that must be edited from the document before the information can be released, the cost of making a copy of the edited page may be imposed;

B. the request puts the requestor over the 36 hour limit for institution personnel time for the current fiscal year; or

C. the public information specifically requested for inspection by the requestor:

1. is older than five years; or completely fills, or when assembled will completely fill, six or more archival boxes; and

2. the Public Information Officer or designee estimates that more than five hours will be required to make the public information available for inspection.

The Public Information Officer or designee may require the requestor to pay, make a deposit, or post a bond for the payment of anticipated personnel costs for making available for inspection such public information.

Where only inspection of information that exists in an electronic medium is requested, no charge may be assessed for access to the information, unless complying with the request will require programming or manipulation of data. In such a case, the requestor must be notified of estimated charges to be imposed before assembling the information.

ii. Waiver of Reduction. Costs shall be waived or reduced if it is determined that waiver or reduction is in the public interest.

iii. Prepayment.

A bond or deposit for payment of anticipated costs for the preparation of a copy of public records shall be required if the charges for providing the copy of the public information is estimated to exceed $100 and if the Public Information Officer or designee has provided the requestor with the required written itemized statement detailing the estimated charge for providing the copy.

The Public Information Officer or designee may require a deposit or bond for payment of unpaid amounts owing to the institution before preparing a copy of public information in response to a new request if those unpaid amounts exceed $100. A request for an Attorney General's opinion must still be made within 10 business days necessitating a review of the public information requested, even though the requestor's copy may not be prepared. The institution must fully document the existence and amount of those unpaid amounts or the amount of any anticipated costs, as applicable, before requiring a deposit or bond under this section. The documentation is subject to required public disclosure under this chapter.

A request for a copy of public information is considered to have been received by an institution on the date the institution receives the deposit or bond for payment of anticipated costs or unpaid amounts if the institution's Public Information Officer or the officer's agent requires a deposit or bond in accordance with this section.

A person requesting information who fails to make a deposit or post a bond before the 10th business day after the date the deposit or bond is required is considered to have withdrawn the request for the copy of the public information that precipitated the requirement of the deposit or bond.

iv. Charge Schedule.

A summary of the charges for copies of public information that have been adopted by the Attorney General is available as Attachment 1.

System Administration and institutions shall maintain a record of charges for public information requests (refer to Attachment 2 for the Public Information Charges Invoice form).

v. Examples of Charges for Copies of Public Information. A few examples of the calculation of charges for information are presented in Attachment 3.

(c) The entire amount of fees collected pursuant to policies outlined herein should be deposited back to the appropriate fund that incurred the costs involved.

(d) System Administration and institutions shall maintain a register that records receipt and processing of requests for public information.

3. Definitions

Chief Administrative Officer - the Chancellor of The University of Texas System and the president of each academic and health institution.

Full Cost - the sum of all direct costs plus a proportional share of overhead or indirect costs.

Nonstandard-Size Copy - a copy of public information that is made available to a requestor in any format other than a standard-size paper copy. Microfiche, microfilm, diskettes, magnetic tapes, CD-ROM, and nonstandard-size paper copies are examples of nonstandard-size copies.

Public Information - information that is collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business by a governmental body or for a governmental body and the governmental body owns the information or has a right of access to it.

Readily Available Information - information that already exists in printed form, or information that is stored electronically and is ready to be printed or copied without requiring any programming, or information that already exists on microfiche or microfilm. Information that requires a substantial amount of time to locate or prepare for release is not readily available information.

Standard-Size Copy - a printed impression on one side of a piece of paper that measures up to 8 1/2 by 14 inches. Each side of a piece of paper on which an impression is made is counted as a single copy. A piece of paper that is printed on both sides is counted as two copies.

4. Relevant Federal and State Statutes

Texas Government Code, Chapter 552

Texas Government Code Section 559.004

Texas Government Code Section 559.003

Texas Administrative Code, Title 1

5. Relevant System Policies, Procedures, and Forms

Attachment 1 Summary of Charges for Copies

Attachment 2 Public Information Charges Billing Form

Attachment 3 Examples of Charges for Copies of Public Information

6. System Administration Office(s) Responsible for Policy

Office of General Counsel

7. Dates Approved or Amended

June 10, 2005
June 8, 2010
May 26, 2011
October 11, 2011
March 8, 2012

8. Contact Information

Questions or comments about this policy should be directed to:

- bor@utsystem.edu

1. Title

Information Resources Use and Security Policy

2. Policy

Sec. 1 Policy Statement. It is the policy of The University of Texas System to:

1.1 protect Information Resources based on risk against accidental or unauthorized access, disclosure, modification, or destruction and assure the availability, confidentiality, and integrity of Data;

1.2 appropriately reduce the collection, use, or disclosure of social security numbers contained in any medium, including paper records; and

1.3 apply appropriate physical and technical safeguards without creating unjustified obstacles to the conduct of the business and Research of the U. T. System and the provision of services to its many constituencies in compliance with applicable State and federal laws.

Sec. 2 Purpose.

2.1 Title 1 *Texas Administrative Code* 202.70(1) states that it is the policy of the State of Texas that Information Resources residing in the various institutions of higher education of state government are strategic and vital assets belonging to the people of Texas. Assets of U. T. System must be available and protected commensurate with their value and must be administered in conformance with federal and State law and the U. T. System Regents' *Rules and Regulations*. This Policy provides requirements and guidelines to establish accountability and prudent and acceptable practices regarding the use and safeguarding of the U. T. System Information Resources, to protect the privacy of personally identifiable information contained in the Data that constitutes part of its Information Resources, to ensure compliance with applicable policies and State and federal laws regarding the management and security of Information Resources, and to educate individual Users with respect to the responsibilities associated with use of U. T. System Information Resources.

2.2 This policy, which includes appended Information Security Practice Bulletins, is intended to serve as the foundation for each institution's, System Administration's, and The University

of Texas Investment Management Company's (UTIMCO's) (collectively known as the Entities) computer security program, providing these Entities the authority to implement policies, practice standards, and/or procedures necessary to implement a successful Information Security Program in compliance with this policy.

Sec. 3 Compliance with State Law. Information that is collected pursuant or that is related to an Entity's Information Security Program is subject to Section 552.139 of the *Texas Government Code* and is therefore confidential by law. Accordingly, an Entity may not withhold information or fail to include information required by this Policy and/or Security Practice Bulletins to be provided to or included in an Entity's Information Security Program.

Sec. 4 All of the requirements in this current Policy apply to all U. T. System Data, including social security numbers, that are maintained, transmitted, or made available in electronic media (Digital Data). However, the special requirements governing the use, disclosure, and maintenance of social security numbers, now set forth in Section 15 of this policy, apply to social security numbers contained in any media, including paper records, held by all Entities except UTIMCO. Therefore, special caution should be exercised when collecting, using, or disclosing any Data that includes a social security number.

Sec. 5. Information Resources Security Responsibility and Accountability.

5.1 Designation of Responsibility. All Entities must designate responsibility for the information security function by documenting key roles and responsibilities.

5.2 Chancellor. The Chancellor shall be responsible for the following:

(a) budget sufficient resources to fund ongoing and continuous information security remediation, implementation, and compliance activities that reduce compliance risk to an acceptably low level; and

(b) ensure that appropriate corrective and disciplinary action is taken in the event of noncompliance.

5.3 Chief Administrative Officers. The Chief Administrative Officers at each Entity shall be responsible for the following:

(a) the Entity's compliance with this Policy;

(b) budget sufficient resources to fund ongoing and continuous information security remediation, implementation, and compliance activities (e.g., staffing, training, tools, and monitoring activities) that reduce compliance risk to an acceptably low level;

(c) approve the Entity's Information Security Program, or designate someone to provide this approval in accordance with 1 *Texas Administrative Code* 202.71(a); and

(d) ensure that appropriate corrective and disciplinary action is taken in the event of noncompliance.

5.4 Chief Information Security Officer. The Chancellor shall designate an individual to serve as U. T. System Chief Information Security Officer (CISO). The responsibilities of the U. T. System CISO shall include the following:

(a) provide leadership, strategic direction, and coordination for the U. T. Systemwide Information Security Program including issuing Security Practice Bulletins relating to standards and best practices;

(b) establish the U. T. System CISO Council and hold meetings at least quarterly;

(c) develop and provide oversight for a U. T. Systemwide Information Security Compliance Program. This program shall include U. T. Systemwide and Entity action plans, training plans, and monitoring plans;

(d) provide guidance on the Entity's Information Security Program including organizational duties and responsibilities, covered activities, authority to act, terminology definitions, standard methodologies, and minimum standards;

(e) define the risk management process to be used for all information security risk management activities;

(f) explore and recommend the acquisition of tools and resources that can be utilized U. T. Systemwide and how expertise can be shared among Entities;

(g) establish reporting guidance, metrics, and timelines and monitor effectiveness of security strategies at each Entity; and

(h) apprise the Chancellor and the Board of Regents quarterly on the status and effectiveness of the Information Security Compliance Programs and activities at each Entity.

5.5 Information Resources Manager. The highest ranking administrator at each Entity charged with oversight of information technology (IT) at that Entity shall serve in the functional role of Information Resources Manager (IRM) as defined by 1 *Texas Administrative Code* 211.1 and will have authority for the entire Entity.

5.6 Information Security Officer. The Chief Administrative Officer at each Entity shall designate an individual other than the IRM to serve as the Information Security Officer (ISO) who shall serve in the capacity as required by 1 *Texas Administrative Code* 202.71(d) and with authority for that entire Entity. The responsibilities of the ISO shall include the following:

(a) provide information security for all Information Systems and computer equipment maintained in both central and decentralized areas;

(b) develop a full-scale Entity Information Security Program. This program shall include Entity action plans, training plans, and monitoring plans;

(c) document an information security risk assessment annually in accordance with 1 *Texas Administrative Code* 202.72 that identifies Mission Critical Information Resources in the central and all decentralized areas;

(d) ensure an annual information security risk assessment is performed (using the process defined above) by each Owner of Mission Critical Information Resources;

(e) require each Owner of Mission Critical Information Resources to designate an Information Security Administrator (ISA);

(f) establish an Entity Information Security Working Group composed of ISAs and hold meetings at least quarterly;

(g) document and maintain an up to date Entity Information Security Program. The program shall identify specific mitigation strategies to be used by each Owner of Mission Critical Information Resources to manage identified risks;

(h) establish reporting guidance, metrics, and timelines and monitor effectiveness of security strategies implemented in both central and decentralized areas;

(i) specify and require use of appropriate security software such as antivirus, firewall, configuration management, and other security related software on computing devices owned, leased, or under the custodianship of any department, operating unit, or an individual who is serving in the role as an employee of the Entity as deemed necessary to provide appropriate information security across the whole of the Entity;

(j) ensure that high-level information security awareness training is included in first-time compliance training and in every subsequent update for all employees;

(k) ensure that ISAs and Data Owners are properly trained on information security requirements;

(l) communicate instances of noncompliance to appropriate administrative officers for corrective, restorative, and/or disciplinary action;

(m) participate in the U. T. System CISO Council meetings;

(n) report quarterly to the U. T. System CISO the current status of the information security risk assessment and Information Security Program including any significant incidents, situations of noncompliance, barriers to program execution, and planned remedies for the whole Entity. The report is to include a certification that best efforts have been made to ensure appropriate strategies are in place to manage identified risks, that the strategies are being applied consistently over time, and that all Security Incidents have been reported; and

(o) report, at least annually, to the Chief Administrative Officer or his or her designated representative(s) and copy the Entity's Chief Information Officer and Compliance Officer, and the Systemwide CISO on the status and effectiveness of Information Resources security controls for the whole Entity.

5.7 Information Security Administrator. Owners of Mission Critical Information Resources at each Entity shall designate an individual to serve as an ISA to implement information security

policies and procedures and to report incidents to the ISO. The responsibilities of the ISA shall include the following:

(a) implement and comply with all IT policies and procedures relating to assigned systems;

(b) assist Owners in performing annual information security risk assessment for Mission Critical Resources;

(c) report general computing and Security Incidents to the Entity ISO;

(d) assist, as member of the ISA Work Group, the ISO in developing, implementing, and monitoring the Information Security Program;

(e) establish reporting guidance, metrics, and timelines for ISOs to monitor effectiveness of security strategies implemented in both the central and decentralized areas; and

(f) report at least annually to the ISO about the status and effectiveness of Information Resources security controls.

5.8 Department Heads and Lead Researchers. Department Heads and Lead Researchers at each Entity shall be responsible for compliance with this Policy as it relates to Non-Research and Research Data respectively under their control including when holding subcontracts for projects in which the prime award is at another institution or agency.

5.9 Institutional Compliance and Internal Audit. Institutional Compliance and Internal Audit at each Entity shall provide high-level monitoring of the Information Security Program through inspections and verifications of reported information and periodic audits respectively.

5.10 User Compliance. All Users must comply with this Policy. Users who fail to comply are subject to disciplinary action in accordance with Section 33.

Sec. 6 Information Resources Acceptable Use.

6.1 Acceptable Use Policy. All Entities shall have an acceptable use policy. All individuals accessing U. T. System Information Resources must formally acknowledge and abide by the acceptable use policy. Formal acknowledgment of the acceptable use policy by all individuals accessing U. T. System

Information Resources serves as a compliance and enforcement tool.

6.2 Reasonableness of Personal Use. Users are responsible for exercising good judgment regarding the reasonableness of personal use in accordance with all Policies associated with Information Resources acceptable use.

6.3 Incidental Personal Use. As a convenience to the U. T. System User community, limited incidental personal use of Information Resources is permitted.

6.4 Direct Cost or Risk. Incidental use of Information Resources must not result in direct cost to the U. T. System or expose U. T. System to unnecessary risks.

Sec. 7 Account Management. The U. T. System recognizes that proper management and use of computer accounts are basic requirements for protecting U. T. System Information Resources. All Entities shall adopt access management processes to ensure that access is administered properly. All offices that create access accounts for network and/or applications are required to manage the accounts in accordance with such access management processes and the requirements of the U. T. System Identity Management Federation Member Operating Practices (MOP). Access to a system may not be granted by another User without the permission of the Owner or the Owner's delegate of that system. An access management process must incorporate procedures for the following:

7.1 creating uniquely identifiable accounts for all Users. This includes accounts created for use by outside Vendors (see Section 31);

7.2 reviewing, removing, and/or disabling accounts at least annually, or more often if warranted by risk, to reflect current User needs or changes on User role or employment status; and

7.3 expiring or disabling passwords at least annually or more often if warranted by risk.

Sec. 8 Administrative/Special Access. All Entities shall adopt special procedures that ensure all administrative/special access accounts with elevated access privileges on computers, network devices, or other critical equipment (example: accounts used by system administrators and network managers) shall be used only for their intended administrative purpose and that all authorized Users must be made

aware of the responsibilities associated with the use of privileged special access accounts. These procedures must address:

8.1 acceptable use of administrative/special access accounts and intended administrative purposes;

8.2 authorizing use of administrative/special access accounts;

8.3 reviewing, removing, and/or disabling administrative/special access accounts at least annually, or more often if warranted by risk, to reflect current authorized User needs or changes on authorized User role or employment status; and

8.4 escrowing login passwords for each secured system for access during emergencies. Individual User login passwords shall not be escrowed.

Sec. 9 Backup Recovery of Network Servers and Data.

9.1 Backup Requirement. All U. T. System Data, including Data associated with research, must be backed up in accordance with risk management decisions implemented by the Data Owner (see Section 14).

9.2 Backup and Recovery Plan. All Data Owners with each Entity shall adopt a backup and recovery plan commensurate with the risk and value of the computer system and Data. The backup and recovery plan must incorporate procedures for the following:

(a) recovering Data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, human error, or system operations errors;

(b) assigning operational responsibility for backup of all servers connected to the applicable network;

(c) scheduling Data backups and establishing requirements for off-site storage;

(d) securing on-site/off-site storage and media in transit; and

(e) testing backup and recovery procedures.

Sec. 10 Change Management. All Entities shall adopt change management processes to ensure secure, reliable, and stable operations to which all

offices that support Information Resources are required to adhere. The change management process must incorporate procedures for:

10.1 formally identifying, classifying, prioritizing and requesting changes;

10.2 identifying and deploying emergency changes;

10.3 assessing potential impacts of changes;

10.4 authorizing changes and exceptions;

10.5 testing changes;

10.6 change implementation and back-out planning; and

10.7 documenting and tracking changes.

Sec. 11 Computer Virus Prevention. U. T. System's network infrastructure and other Information Resources must be continuously protected from threats posed by computer viruses, trojans, worms, and other types of hostile computer programs. All U. T. System owned and personal computers that connect to the U. T. System network must run all required protection software and adhere to any other protective measures as required by applicable policies and procedures.

Sec. 12 Classification of Digital Data.

12.1 Guidelines. All Entities shall develop Digital Data classification guidelines and a plan for identifying Digital Data maintained in both central and decentralized areas. Owners of Information Resources within the Entity shall classify Digital Data based on Data sensitivity and risk that is Sensitive. Sensitive Digital Data is defined in Section 14.4 of this Policy.

12.2 Classification Changes. An Entity may change its classification of Digital Data upon request by the Data Owner with review and approval by the Entity's executive officer and/or Office of Legal Affairs or U. T. System Office of General Counsel.

Sec. 13 Risk Management.

13.1 Annual Assessment. All Entities shall conduct and document an information security risk assessment annually that identifies Mission Critical Information Resources in the central and all decentralized areas.

13.2 Owners. Owners of Mission Critical Information Resources shall perform a security risk assessment on an annual basis. They shall identify, recommend, and document acceptable risk levels for Information Resources under their authority. Information Resources must be protected based on sensitivity and risk.

13.3 Custodians. Custodians of Mission Critical Information Resources shall implement approved mitigation strategies and adhere to information security policies and procedures to manage risk levels for Information Resources under their care.

13.4 Sensitive Digital Data. Sensitive Digital Data is defined as Digital Data maintained by an Entity that requires higher than normal security measures to protect it from unauthorized access, modification, or deletion. Sensitive Data may be either public or confidential and is defined by each Entity based on compliance with applicable federal or State law or on the demonstrated need to (a) document the integrity of that Digital Data (i.e., that the Data had not been altered by either intent or accident), (b) restrict and document individuals with access to that Digital Data, and (c) ensure appropriate backup and retention of that Digital Data. These would most frequently be required by:

- federal agencies (e.g., Food and Drug Administration);
- State agencies (e.g., data defined as High-Risk Information Resources by 1 Texas Administrative Code 202.72);
- employee benefit providers;
- Office of General Counsel or Entity Office of Legal Affairs (i.e., data subject to or involved in litigation or confidentiality agreements);
- intellectual property and/or technology transfer requirements; or
- federal regulations (e.g., FERPA, HIPAA, Gramm-Leach-Bliley, Biodefense, Homeland Security, Department of Defense, etc.)

The confidentiality and integrity of Sensitive Digital Data must be managed as required by this Policy.

13.5 Nonsensitive Digital Data. Digital Data that is not identified as Sensitive must be managed according to applicable standards

and policies and, in the case of Research Data, according to federal guidelines for the responsible conduct of Research.

Sec. 14 Reduction of Use and Collection of Social Security Numbers. U. T. System recognizes the special risks associated with the collection, use, and disclosure of social security numbers. Accordingly, the requirements of this section apply to social security numbers contained in any medium, including paper records that are collected, maintained, used or disclosed by any Entity except UTIMCO.

14.1 Reduction of Use and Collection. All Entities shall reduce the use and collection of social security numbers.

(a) All Entities shall discontinue the use of the social security number as an individual's primary identification number unless required or permitted by law. The social security number may be stored as a confidential attribute associated with an individual.

(b) If the collection and use of social security numbers is permitted but not required by applicable law, the Entity shall use and collect social security numbers only as reasonably necessary for the proper administration or accomplishment of the respective business, governmental, educational, and medical purposes, including, but not limited to:

i. as means of identifying an individual for whom a unique identification number is not known;

ii. for internal verification or administrative purposes; and

iii. use for verification or administrative purposes by a third party or agent conducting the Entity's business on behalf of the Entity where the third party or agent has contracted to comply with the safeguards described in Section 16 of this Policy.

(c) Except in those instances in which an Entity is legally required to collect a social security number, an individual shall not be required to disclose his or her social security number, nor shall the individual be denied access to the services at issue if the individual refuses to disclose his or her social security number. An individual, however, may volunteer his or her social security number. An Entity's request that an individual provide his or her social security number for verification of the individual's identity where the

social security number has already been disclosed does not constitute a disclosure for purposes of this Policy. Examples of federal and State laws that require the collection or use of social security numbers are included in Appendices 2 and 3. Questions about whether a particular use is required by law should be directed to the local ISO who will consult with the Office of General Counsel with respect to the interpretation of law.

(d) An Entity may, but is not required to, designate only selected offices and positions as authorized to request that an individual disclose his or her social security number.

(e) All Entities shall assign a unique identifier for each applicant, student, employee, insured dependent, research subject, patient, alumnus, donor, contractor, and other individuals, as applicable, at the earliest possible point of contact between the individual and the Entity.

(f) The unique identifier shall be used in all electronic and paper Information Systems to identify, track, and serve these individuals. The unique identifier shall:

i. be a component of a system that provides a mechanism for the public identification of individuals;

ii. be permanent and unique within the Entity as applicable and remain the property of, and subject to the rules of, that Entity; and

iii. not be derived from the social security number of the individual; or, in the alternative, if the unique identifier is derived from the social security number, it must be computationally infeasible to ascertain the social security number from the corresponding unique identifier.

(g) All services and Information Systems shall rely on the identification services provided by the unique identifier system.

14.2 Notification. All Entities shall inform individuals when they collect social security numbers.

(a) Each time an Entity requests that an individual initially disclose his or her social security number, it shall provide the notice required by Section 7 of the Federal Privacy Act

of 1974 (5 U.S.C. § 552a), which requires that the individual be informed whether the disclosure is mandatory or voluntary, by what statutory or other authority the number is solicited, and what uses will be made of it. A subsequent request for production of a social security number for verification purposes does not require the provision of another notice.

i. The notice shall use the applicable text from Appendix 4 of this Policy or such other text as may be approved by the ISO in consultation with the Office of General Counsel.

ii. It is preferable that the notice be given in writing, but if at times it will be given orally, procedures shall be implemented to assure and document that the notice is properly and consistently given.

iii. Existing stocks of forms need not be reprinted with the disclosure notice; the notice may be appended to the form. Future forms and reprints of existing stock shall include the notice printed on the form.

(b) In addition to the notice required by the Federal Privacy Act, when the social security number is collected by means of a form completed and filed by the individual, whether the form is printed or electronic, the notice as required by Section 559.003 of the *Texas Government Code* must also be provided. That section requires that the agency state on the paper form or prominently post on the Internet site in connection with the form that, with few exceptions, the individual is entitled on request to be informed about the information that is collected about the individual; under Sections 552.021 and 552.023 of the *Texas Government Code*, the individual is entitled to receive and review the information; and under Section 559.004 of the *Texas Government Code*, the individual is entitled to have the incorrect information about the individual corrected.

14.3 Prohibition of Personal Use. Employees may not seek out or use social security numbers relating to others for their own interest or advantage.

14.4 Public Display. All Entities shall reduce the public display of social security numbers.

(a) Grades may not be publicly posted or displayed in a manner in which all or any portion of either the social security number or the unique identifier identifies the individual associated with the information.

(b) The social security number may not be displayed on documents that can be widely seen by the general public (such as time cards, rosters, web pages, and bulletin board postings) unless required by law. This section does not prohibit the inclusion of the social security number on transcripts or on materials for federal or State Data reporting requirements.

(c) If an Entity sends materials containing social security numbers through the mail, it shall take reasonable steps to place the social security number on the document so as not to reveal the number in the envelope window.

(d) The Entity shall prohibit employees from sending social security numbers over the Internet or by email unless the connection is secure or the social security number is encrypted or otherwise secured. The Entity shall require employees sending social security numbers by fax to take appropriate measures to protect the confidentiality of the fax (such measures may include confirming with the recipient that the recipient is monitoring the fax machine).

(e) The Entity shall not print or cause an individual's social security number to be printed on a card or other device required to access a product or service provided by or through the Entity.

14.5 Compliance. All Information Systems acquired or developed must comply with the following:

(a) the Information System must use the social security number only as a Data element or alternate key to a database and not as a primary key to a database;

(b) the Information System must not display social security numbers visually (such as on monitors, printed forms, system outputs) unless required or permitted by law or permitted by this Policy;

(c) name and directory systems must be capable of being indexed or keyed on the unique identifier, once it is assigned, and not on the social security number; and

(d) for those databases that require social security numbers, the databases may automatically cross-reference between the social security number and other information through the use of conversion tables within the Information System or other technical mechanisms.

Sec. 15 Management of Sensitive Digital Data.

15.1 Protection. Each Entity's policies, standards, and/or procedures must describe and require appropriate steps to protect Sensitive Digital Data (e.g., social security numbers, Protected Health Information (PHI), Sensitive Research Data, digital Data associated with an individual and/or digital Data protected by law) stored on U. T. System's computing devices.

15.2 Access. All Entities shall control and monitor access to their Sensitive Digital Data based on Data sensitivity and risk (as determined in accordance with Section 14 of this Policy) and by the use of appropriate physical and technical safeguards.

(a) All Entities shall limit access to records containing Sensitive Digital Data to those employees who need access to the Data for the performance of the employees' job responsibilities.

Employees may not request disclosure of Sensitive Digital Data if it is not necessary and relevant to the purposes of U. T. System and the particular function for which the employee is responsible.

(b) All Entities shall monitor access to records containing Sensitive Digital Data by the use of appropriate measures as reasonably determined by the Entity.

(c) Employees may not disclose Sensitive Digital Data to unauthorized persons or entities except:

i. as required or permitted by law;

ii. with the consent of the individual;

iii. where the third party is the agent or contractor for the Entity and the safeguards described in Section 16.2(d) are in place to prevent unauthorized distribution; or

iv. as approved by the Office of General Counsel.

(d) If an Entity intends to provide Sensitive Digital Data to a third party acting as an agent of or otherwise on behalf of that Entity (e.g., an application service provider) and if it determines that its provision of Sensitive Digital Data to a third party will result in a significant risk to the confidentiality and integrity of such Data, a written agreement with the third party is required that must specify terms and conditions that protect the confidentiality and integrity of the Sensitive Digital Data as required by this Policy. The written agreement must require the third party to use appropriate administrative, physical, and technical safeguards to protect the confidentiality and integrity of all Sensitive Digital Data obtained and the Entity, as applicable, should monitor compliance with the provisions of the written agreement.

15.3 Security Safeguards. All Entities shall implement security safeguards to protect their Sensitive Digital Data. Such safeguards shall be appropriate to the sensitivity of the Digital Data to be protected based on risk and, in the case of Research, the research project requirements for that Sensitive Digital Data.

(a) Sensitive Digital Data shall be secured in accordance with each Entity's security plan and with this Policy.

(b) All Entities shall protect the security of records containing Sensitive Digital Data during storage using physical and technical safeguards (such safeguards may include encrypting electronic records, including backups, and locking physical files).

(c) Unless otherwise required by federal or State law or regulation, Sensitive Digital Data must not be stored on U. T. System or personal computers or other electronic devices (e.g., laptop, hand-held device, Flash drives, or other Portable Computing Devices) unless:

i. it is secured against unauthorized access in accordance with this Policy;

ii. it will not compromise business or Research efforts or privacy interests if lost or destroyed; and

iii. the Entity has specific procedures in place that address this section.

15.4 Discarding Electronic Media. All Entities shall discard electronic media (e.g., disks, tapes, hard drives, etc.) containing Sensitive Digital Data as follows:

(a) in a manner that adequately protects the confidentiality of the Sensitive Digital Data and renders it unrecoverable, such as overwriting or modifying the electronic media to make it unreadable or indecipherable or otherwise physically destroying the electronic media; and

(b) in accordance with the applicable Entity's records retention schedule.

15.5 Electronic Communications or Transmissions. All Entities shall, based on risk, implement all appropriate technical safeguards necessary to adequately protect the security of Sensitive Digital Data during electronic communications or transmissions.

Sec. 16 Electronic Communications. All Entities shall require each faculty member, staff, and student to exercise prudence in the use of Electronic Communications and use them in accordance with the Entity's policies, standards, and/or procedures related to Information Resources acceptable use and retention.

Sec. 17 Incident Management.

17.1 Reporting Requirements. Incidents involving computer security will be reported as required by State or federal law.

17.2 Incident Management Procedures. All Entities shall establish and follow Incident Management Procedures to ensure that each incident is reported, documented, and resolved in a manner that restores operation quickly while meeting the legal requirements for handling of evidence.

17.3 Employee Reporting. All Entities shall require employees to report promptly unauthorized or inappropriate disclosure of Sensitive Digital Data, including social security numbers, to their supervisors, ISO, and/or the Entity's compliance hotline.

17.4 Monitoring Techniques and Procedures. Custodians of Mission Critical Information Resources shall implement monitoring techniques and procedures for detecting, reporting, and investigating incidents.

17.5 Reporting Guidelines. All Entities shall report significant information security incidents, as defined by the U. T. System Security Incident Reporting Guidelines, to the U. T. System CISO. Incidents resulting in unauthorized disclosure of Confidential University Data must be reported immediately. Entities shall report incidents to the U. T. System CISO prior to reporting to non-U. T. System agencies or organizations except as required by State or federal law.

17.6 Disclosure. All Entities shall disclose in accordance with applicable federal and State law, incidents involving computer security that compromise the security, confidentiality, or integrity of Personal Identifying Information they maintain to any resident of Texas and Data Owners whose Personal Identifying Information was, or is reasonably believed to have been, acquired without authorization.

Disclosure shall be made as quickly as possible upon the discovery or receipt of notification of the incident taking into consideration (a) the time necessary to determine the scope of incident and restore the reasonable integrity of operations or (b) any request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that it will not compromise the investigation.

17.7 Incident Management Procedures Content. Entities' Incident Management Procedures must incorporate procedures for the following:

(a) formally identifying, reporting, and classifying incidents;

(b) responding to incidents;

(c) assessing potential damage of incidents;

(d) gathering and preserving physical and electronic evidence;

(e) assigning responsibility for gathering, maintaining, and reporting detailed information regarding incidents of local and U. T. Systemwide significance; actions taken to

remediate; and documentation of a management action plan to prevent a recurrence in accordance with Section 6 of this Policy;

(f) notifying appropriate System Administration officials, residents of Texas, Data Owners, and consumer reporting agencies as required by applicable State and federal law and U. T. System policy;

(g) determining the timing requirements for incident disclosure and notification; and

(h) determining the appropriate medium to provide notice based on incident significance and number of individuals adversely impacted.

Sec. 18 Internet Use.

18.1 Risks. The U. T. System recognizes that there are risks associated with the posting or consuming of information on the Internet. To mitigate these risks, U. T. System network Users must adhere to prudent and responsible Internet use practices as outlined in the Entity's policies associated with Information Resources acceptable use.

18.2 Policies, Standards, and Procedures. All Entities will develop and adhere to policies, standards, and/or procedures governing the secure transmission of Confidential University Data via public networks. These policies, standards, and/or procedures must incorporate procedures for encrypting all Confidential University Data or any specific Data identified as confidential by federal and State law transmitted over the Internet.

Sec. 19 Information Services (IS) Privacy. Users have no personal expectation of privacy pertaining to electronic files and Data created, sent, received, or stored on computers and other Information Resources owned, leased, administered, or otherwise under the custody and control of U. T. System. Files and Data may be accessed as needed for purposes of system administration and maintenance; for resolution of technical problems; for compliance with the Texas Public Information Act; for compliance with federal and State subpoenas, court orders, litigation holds, or other written authorizations; to perform audits; or to otherwise conduct the business of U. T. System.

Sec. 20 Network Access.

20.1 User Responsibilities. All network Users are required to acknowledge and abide by all policies relating to Information Resources acceptable use.

20.2 Approvals. The office or offices charged with maintaining the IT infrastructure at each Entity are required to approve all access methods, installation of all network hardware connected to the local-area network, and methods and requirements for attachment of any non-U. T. System owned computer systems or devices to the U. T. System network to ensure that access to the network does not compromise the operations and reliability of the network, or compromise the integrity or use of information contained within the network.

Sec. 21 Network Configuration. All Entities must designate responsibility for the Entity's network infrastructure and specify those responsible for configuration and management of the resource to ensure reliability of operations, proper accessibility to resources, and protection of Data confidentiality and integrity.

Sec. 22 Passwords.

22.1 Procedures. In order to preserve the security of Entity Information Resources and Data, strong passwords shall be used to control access to Information Resources. All passwords must be constructed, implemented, and maintained according to the requirements of the U. T. System Identity Management Federation and applicable policies, standards, and/or procedures governing password management. The Entity's policies, standards, and/or procedures must incorporate procedures for the following:

(a) vetting User identity when issuing or resetting a password;

(b) establishing password strength;

(c) changing passwords;

(d) managing security tokens when applicable; and

(e) securing unattended computing devices from unauthorized access.

22.2 Sharing. Users shall not share passwords or similar information or devices used for identification and authorization purposes.

Sec. 23 Physical Access.

23.1 Protection. All Information Resources must be physically protected, based on risk, as determined in accordance with Section 14 of this Policy, and associated risk management decisions as part of the overall security program for the U. T. System.

23.2 Safeguards. All Entities shall adopt physical access safeguards to ensure appropriate granting, controlling, and monitoring of physical access. All offices that own or maintain Information Resources are required to adhere to such physical access safeguards. The Entity's physical access safeguards must incorporate procedures for the following:

(a) protecting facilities in proportion to the criticality or importance of their function and the confidentiality of any impacted Information Resources affected;

(b) managing access cards, badges, and/or keys;

(c) changing and/or removing physical access to facilities to reflect changes on User role or employment status; and

(d) providing access to facilities to visitors and Vendors.

Sec. 24 Portable Computing and Remote Access.

24.1 User Responsibilities. To preserve the integrity, availability, and confidentiality of U. T. System information, Users accessing the Entity's infrastructure remotely must do so in accordance with Section 8 and all policies on Information Resource acceptable use.

24.2 Policies, Standards, and Procedures. All Entities must develop policies, standards, and/or procedures governing remote access and wireless connectivity.

Sec. 25 Security Monitoring. In accordance with Section 6 of this Policy, all Entities shall have an IT organization that is charged with providing security for all network resources, in both central and decentralized areas, and has the responsibility and Entity-wide authority to monitor network traffic and use of Information Resources to confirm that security practices and controls are adhered to and are effective. Any exceptions to required information security practices must include provisions that ensure compliance with this policy and must be approved and documented by the Entity's ISO.

Sec. 26 Security Training.

26.1 User Training. All Entities shall deliver security awareness general compliance training in accordance with the following schedule, or more frequently as determined by that Entity:

(a) training of all Users with access to the Entity's Information Resources shall take place at least yearly; and

(b) training of each new, temporary, contract, assigned, or engaged employee or worker shall take place within 30 days after the date that such a person is (a) hired by the Entity, or (b) otherwise engaged or assigned to perform such work.

26.2 Technical Support Training. All Entities shall provide appropriate technical training to employees providing IT help desk or technical support as determined by that Entity.

Sec. 27 Server and Network Device Hardening Standards. To protect against malicious attack, all Servers on U. T. System networks will be security hardened based on risk analysis and must be administered according to policies and standards procedures prescribed by the Entity, as applicable, and must incorporate procedures for the following:

27.1 managing the testing and installation of security patches; and

27.2 setting baseline security "hardened" configuration standards for all network device types (examples: routers, laptops, desktops, and personal digital assistants).

Sec. 28 Software Licensing. All software installed on U. T. System owned computers must be used in accordance with the applicable software license. Unauthorized or unlicensed use of software is regarded as a serious matter subject to disciplinary action and any such use is without the consent of U. T. System.

Sec. 29 System Development and Deployment.

29.1 Procedures. All Entities must ensure that the protection of Information Resources (including Data confidentiality, integrity, and accessibility) is considered during the development or purchase of new computer applications or services. The Entity's policies, standards, and/or procedures must, at a minimum, incorporate procedures for the following:

(a) providing methods for appropriately restricting privileges of authorized Users to all production systems and applications.

User access to applications is granted on a need-to-access basis; and

(b) maintaining separate production and development environments to ensure the security and reliability of the production system. Exceptions to this must be approved by the Entity's IRM.

29.2 Review. The Entity's ISO must review the data security requirements and specifications of any new computer applications or services that receive, maintain, and/or share Confidential Data.

29.3 Approval. The Entity's ISO must approve the security requirements of the purchase of required IT hardware, software, and systems development services for any new computer applications that receive, maintain, and/or share Confidential Data.

29.4 Contracts. IT contracts must address security, backup, and privacy requirements, and should include right-to-audit and other provisions to provide appropriate assurances that applications and Data will be adequately protected. Vendors must adhere to all State and federal laws and Regents' *Rules and Regulations* and U. T. System policies pertaining to the protection of Information Resources and privacy of Sensitive Data.

Sec. 30 Vendor Access. The U. T. System recognizes that Vendors serve an important function in the support of services, hardware, and software and, in some cases, the operation of computer networks, servers, and/or applications.

30.1 Contracts. Vendor contracts must require that Vendors comply with all applicable U. T. System rules associated with this policy, practice standards, and agreements, and address all federal and State laws to which U. T. System must adhere to ensure that U. T. System remains in compliance with such law.

30.2 Access Control Measures. All Entities shall control Vendor access to their Sensitive Data based on data sensitivity and risk (as determined in accordance with Section 14 of this Policy) and by the use of appropriate measures. Such measures must incorporate the following:

(a) Vendor shall represent, warrant, and certify it will:

i. hold all Sensitive Data in the strictest confidence;

ii. not release any Sensitive Data concerning an Entity student unless Vendor obtains Entity's prior written approval and performs such a release in full compliance with all applicable privacy laws, including the Family Educational Rights and Privacy Act (FERPA);

iii. not otherwise use or disclose Sensitive Data except as required or permitted by law;

iv. safeguard Sensitive Data according to all commercially reasonable administrative, physical, and technical standards (e.g., such standards established by the National Institute of Standards and Technology or the Center for Internet Security);

v. continually monitor its operations and take any action necessary to assure the Sensitive Data is safeguarded in accordance with the terms of this Policy; and

vi. comply with the Vendor access requirements that are set forth in this section.

(b) To the extent that the Sensitive Data includes PHI as defined in 45 C.F.R. § 164.501, if required by an Entity, Vendor shall execute a Health Insurance Portability and Accountability Act (HIPAA) business associate agreement in the form required by U. T. System.

(c) Entities shall require the following from the Vendor:

i. If an unauthorized use or disclosure of any Sensitive Data occurs, the Vendor must provide:

A. written notice within one business day after Vendor's discovery of such use or disclosure; and

B. all information U. T. System requests concerning such unauthorized use or disclosure.

ii. Within 30 days after the termination or expiration of a purchase order, contract, or agreement for any reason, Vendor shall either:

A. return or destroy, as applicable, all Sensitive Data provided to the Vendor by the Entity, including all

Sensitive Data provided to Vendor's employees, subcontractors, agents, or other affiliated persons or entities; or

B. in the event that returning or destroying the Sensitive Data is not feasible, provide notification of the conditions that make return or destruction not feasible, in which case, the Vendor must continue to protect all Sensitive Data that it retains and agree to limit further uses and disclosures of such Data to those purposes that make the return or destruction not feasible as Vendor maintains such Data.

Sec. 31 Right to Monitor. Entities have the authority and responsibility to monitor Information Resources in accordance with *Texas Administrative Code* 202.75(7)(P):

31.1 to ensure compliance with this policy and State laws and regulations related to the use and security of Information Resources; and

31.2 to ensure that Information Resources security controls are in place, are effective, and are not being bypassed.

Sec. 32 Disciplinary Actions. Violation of this policy may result in disciplinary action for faculty, staff, and students in accordance with each Entity's rules and policies. For contractors and consultants this may include termination of the work engagement. For interns and volunteers, this may include dismissal. Any student who violates this policy will be referred to student judicial services at the student's home campus. Additionally, all individuals are subject to possible civil and criminal prosecution.

Sec. 33 Special Requirements for Initial Implementation of Policy.

Nothing in this Policy is intended to prohibit or restrict the collection, use, and maintenance of Sensitive Data as required or permitted by applicable law; to create unjustified obstacles to conduct the business of the U. T. System and the provision of services to its many constituencies; or to negatively affect U. T. System's commitment to engage in high-quality, innovative Research that entails the discovery, retention, dissemination, and application of knowledge in compliance with Regents' *Rules and Regulations*, U. T. System Policies, and State and federal laws and regulations.

3. Definitions

Backup - copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system failure.

Change - any addition, modification or update, or removal of an Information Resource that can potentially impact the operation, stability, or reliability of an Entity network or computing environment.

Change Management - process of controlling the communication, approval, implementation, and documentation of modifications to hardware and software to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

Confidential Data - data that is exempt from disclosure under the provisions of the Texas Public Information Act or other applicable State and federal laws.

Data - recorded data, regardless of form or media in which it may be recorded, which constitute the original data necessary to support the business of U. T. System or original observations and methods of a study and the analyses of such original data that are necessary to support Research activities and validate Research findings. Data may include, but is not limited to, printed records, observations, and notes; electronic data; video and audio records; photographs and negatives; etc.

Decentralized Areas - Entity business units, departments, or programs that manage or support their own information systems.

Digital Data - the subset of Data (as defined above) that is transmitted by, maintained, or made available in electronic media.

Information Resources - any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDAs), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, network environments, telephones, fax machines, printers, and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and Data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM) - the IRM is responsible for management of all of the Entity's Information Resources. The designation of an Entity Information Resources Manager is intended to establish clear accountability for setting policy for Information Resources management activities, provide for

greater coordination of the Entity's information activities, and ensure greater visibility of such activities within and between Entities. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards, and guidelines to protect the Information Resources of the Entity including both central and decentralized areas. If an Entity does not designate an IRM, the title defaults to the institution's president, and the president is responsible for adhering to the duties and requirements of an IRM.

Information Security Program - the policies, procedures, elements, structure, strategies, plans, metrics, reports, and resources that establish an Information Resources security function within an Entity.

Information System - an interconnected set of Information Resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, information, data, applications, communications, and people.

Local Area Network (LAN) - a data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

Mission Critical Information Resources - Information Resources defined by an Entity to be essential to the Entity's function and that, if made unavailable, will inflict substantial harm to the Entity and the Entity's ability to meet its instructional, research, patient care, or public service missions. Mission Critical Information Resources include Confidential Data.

Non-University Owned Computing Device - any device capable of receiving, transmitting, and/or storing electronic data and not owned or leased by or under the management of an Entity.

Owner - the manager or agent responsible for the business function that is supported by the Information Resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security and authorizing access to the Information Resource. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared.

Personal Identifying Information - information that alone or in conjunction with other information identifies an individual, including an individual's name, social security number, date of birth, or government-issued identification number; mother 's maiden name; unique biometric data, including the individual's

fingerprint, voice print, and retina or iris image; unique electronic identification number, address, or routing code; and telecommunication access device.

Portable Computing Devices - any easily portable device that is capable of receiving, transmitting, and/or storing data. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, cell phones, Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs and similar storage devices.

Security Incident - an event that results in unauthorized access, loss, disclosure, modification, disruption, or destruction of Information Resources whether accidental or deliberate.

Strong Passwords - a strong password is constructed so that another User or a "hacker" program cannot easily guess it. It is typically a minimum number of positions in length and contains a combination of alphabetic, numeric, or special characters.

User - an individual, automated application, or process that is authorized by the Owner to access the resource, in accordance with the Owner's procedures and rules. This individual has the responsibility to (1) use the resource only for the purpose specified by the Owner, (2) comply with controls established by the Owner, and (3) prevent disclosure of Confidential or Sensitive Data. The User is any person who has been authorized by the Owner of the information to read, enter, or update that information. The User is the single most effective control for providing adequate security.

UTIMCO - The University of Texas Investment Management Company that manages U. T. System's investment assets.

U. T. System Administration - the central administrative offices that lead and serve the Entities by undertaking certain central responsibilities that result in greater efficiency or higher quality than could be achieved by individual Entities or that fulfill legal requirements.

Vendor - someone outside of U. T. System who exchanges goods or services for money or other consideration.

4. Relevant Federal and State Statutes

Title 1 *Texas Administrative Code* 202.2

Texas Education Code § 65.31

Federal Privacy Act of 1974 (Section 7 of Pub. L. 93-579 in Historical Note), 5th U.S.C. § 552a

Social Security Act, 42 U.S.C. §§ 408(a)(8) and 405(c)(2)(C)(viii)(I)

Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g

Texas Business and Commerce Code §35.58

Texas Government Code § 559.003

5. Relevant System Policies, Procedures, and Forms

Template for an Acceptable Use Policy is available at the following address: http://www.utsystem.edu/ciso/documents/SystemWideAcceptableUseTemplate_1208.doc

Appendix 1: Chronological Implementation Plan for Protection of the Confidentiality of Social Security Numbers

Appendix 2: Examples of Federal Laws Requiring the Use or Collection of Social Security Numbers

Appendix 3: Examples of State Laws Requiring the Use or Collection of Social Security Numbers

Appendix 4: Preapproved Text for Notice Required by the Federal Privacy Act of 1974

Information Security Practice Bulletin #1: Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices

Information Security Practice Bulletin #2: Baseline Standard for Information Security Programs

Bulletin #2 Corresponding Documents

- U. T. System Information Security Program Elements
- U. T. System Information Security Program Metrics Reported to U. T. System
- Institutional Information Security Program Quarterly Status Report Template

6. System Administration Office(s) Responsible for Policy

Office of Technology and Information Services

7. Dates Approved or Amended

April 12, 2007

June 15, 2010
August 15, 2012

9. Contact Information

Questions or comments about this policy should be directed to:

- bor@utsystem.edu

Attachment D

Creating an e-History of the Board

Gathering and displaying governance documents and photos online can help educate the public, promote transparency, and preserve historical artifacts.

THOMAS JEFFERSON WROTE that "it is the duty of every good citizen to use all the opportunities which occur to him for preserving documents relating to the history of our country."

To suggest the same sentiment holds true for the preservation of college and university histories is not a stretch. And no department has more primary documents and access to more firsthand knowledge of major institutional decisions than the office that supports the governing board.

The problem is, higher education boards face so many complicated, critical, and timely issues that the supporting office often has time and energy to meet only the most pressing needs, such as producing conventional minutes of meetings. Most consider the history of the board to be of only passing interest, which is why staff time and expertise are seldom devoted to systematically organizing board history.

Except in Texas. Under the leadership of a board chair with lifelong interest in history

• BY FRANCIE A. FREDERICK AND RHONDA HANKINS •

and great respect for the historical record, the Office of the Board of Regents of the University of Texas System has discovered that understanding the history of the board and making historical documents widely available serves both practical and scholarly purposes. Such documents might be considered a road map to landmark decisions in the development of the University of Texas System. They clearly document the architectural history of the campuses and offer insights into recurring issues system leaders faced.

What's more, providing greater access to unpublished and unofficial materials, following careful review, contributes to the transparency of the board and complements the spirit of the sunshine laws that apply to most public universities. What follows is a description of how the Texas system board archives has blossomed in recent years.

In-House Display. In 2004, when James R. Huffines was elected chair of the University of Texas System Board of Regents, he brought with him an enthusiasm for history, especially Texas history and the history of the University of Texas.

With his encouragement, the board office staff began culling files to make photographs and original documents more accessible; organizing historical presentations to be delivered at board meetings; and arranging celebrations of significant board events. The files offered a virtual gold mine of photographs, primary documents, clippings, telegrams, and handwritten notes dating to the board's founding in 1881.

One of the first historical projects involved framing the group photos of regents. More than 50 photos of different boards now hang in the office suite, in the chair's office, and in the office reserved for regents when they work in Austin. Easels allow these photos to be displayed on tabletops during board meetings or special events.

Additional photographs of regents attending various events over the years were retrieved from the files and preserved in archival-quality photograph albums kept on a coffee table in the office lobby. These photographs show some prominent Texans attending building dedications, giving speeches at commencement ceremonies, and attending special events honoring university leaders. Some of the photos are little more than snapshots, but they serve as vivid reminders of the continuum of public service and decision making over the years.

The board office staff also displayed sepia portraits of each former board chair, which had been warehoused years ago during a building renovation, to transform an ordinary conference room at the UT system into a mini-museum. Collectively, these distinguished portraits create a dramatic representation of the long tradition of Texas higher education administration and its role in creating one of the nation's largest and most notable public university systems.

Going Online. Looking through board office files, we saw a treasure trove of one-of-a-kind documentation of the university's history languishing in file cabinets; we knew it needed to be made more widely available. Beginning in 2006, the staff quickly made more than 100 years of board minutes available online in a searchable format to facilitate research and access—not to mention to preserve the aging documents.

The board office created hundreds of Web pages devoted exclusively to former regents. These pages (available at *www.utsystem.edu/bor/FormerRegents.htm*) highlight the most significant, interesting, or unusual issues concerning a particular regent. The site also now provides the public and board office staff with an easy way to research the contri-

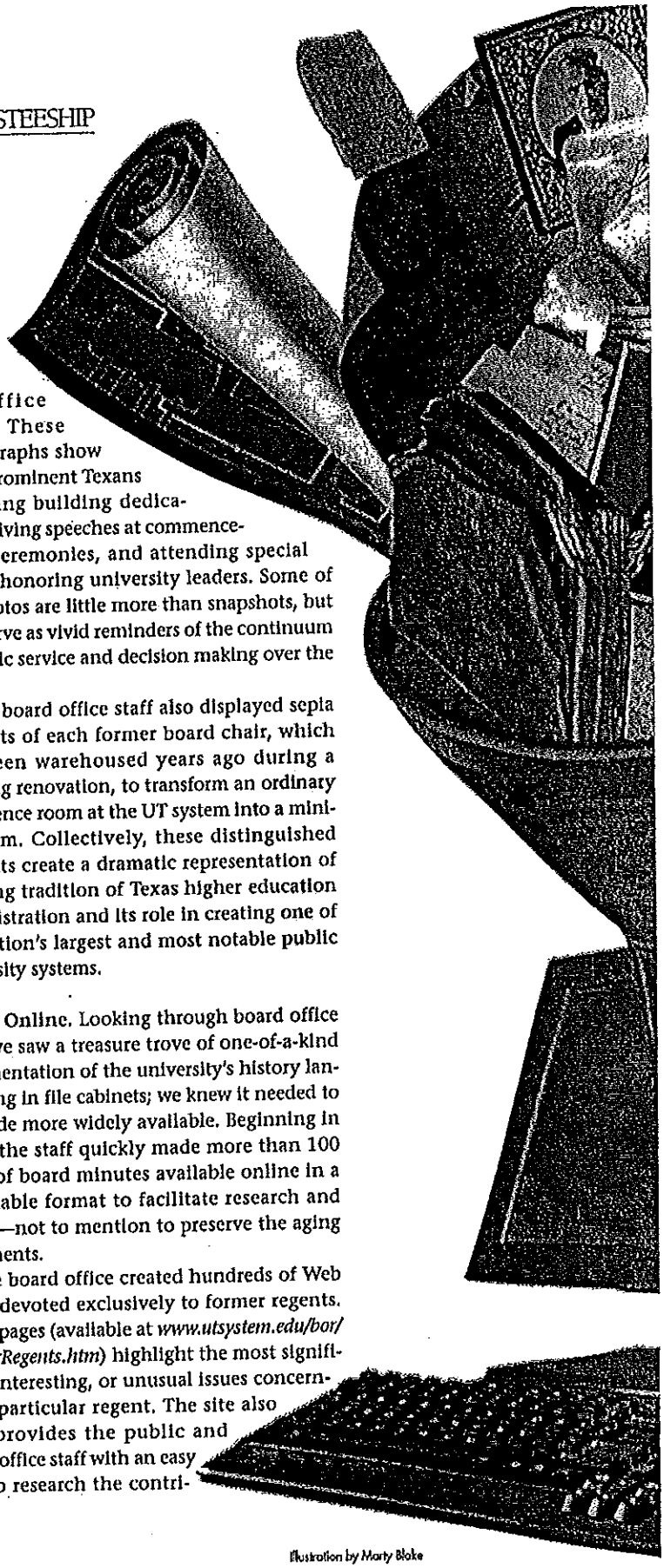
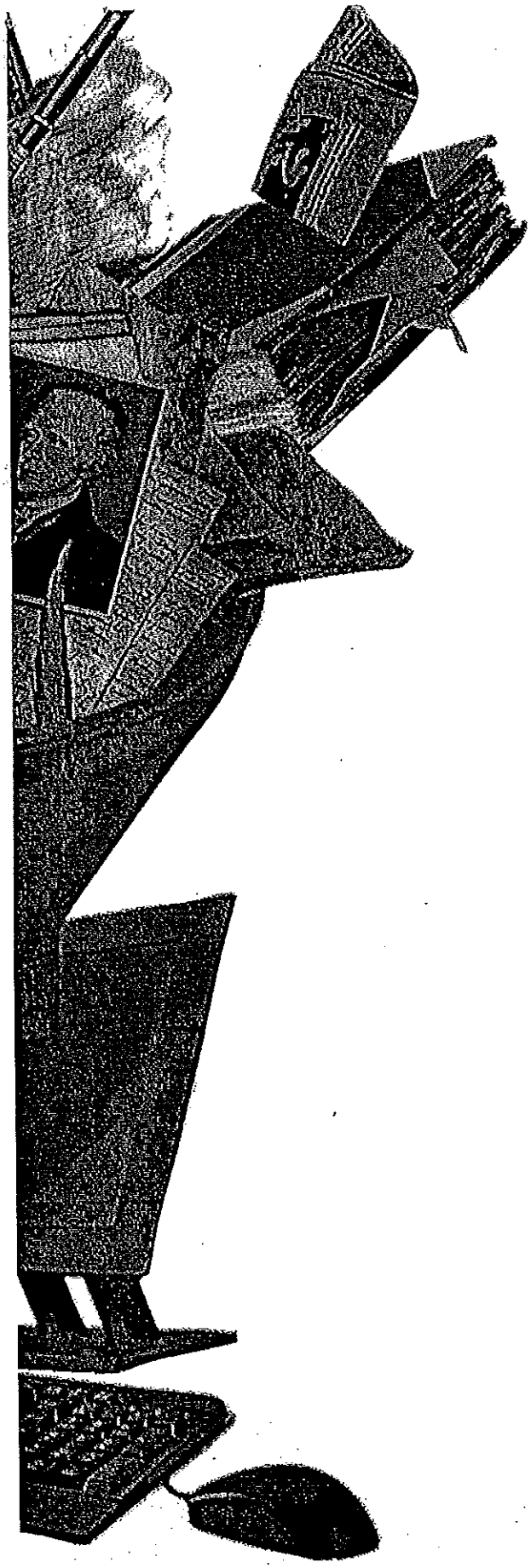


Illustration by Marty Blake



butions and accomplishments of past regents. Some highlights:

- The reproduction of a handwritten letter from regent Thomas Dudley Wooten, M.D., to fellow regent Thomas Harwood, dated October 20, 1893, is believed to be the earliest known document referring to the establishment of a law library at the University of Texas at Austin.
- A transcript of remarks by former regent Lady Bird Johnson, the former first lady, reveals her passionate support for the National Endowment for the Arts and her belief that speaking up was an important catalyst for change.
- A link to the postcard collection donated to the UT Arlington library by former regent Jenkins Garrett and the link to the Americana Collection at UT San Antonio donated by former regent John Peace reflect some of the personal connections of former regents to particular institutions.

The Web site provides the public and board office staff with an easy way to research the contributions and accomplishments of past regents.

The Web pages are liberally sprinkled with scanned photographs of regents at work during board meetings, on campus tours, or attending student events, giving viewers a sense of the regents' various responsibilities. The Web pages also link to bibliographies of works by and about regents.

Another part of the effort has involved scanning significant historical documents into a sophisticated yet user-friendly electronic content management system. This secure, searchable environment makes documents instantly accessible and easily managed. An automated content management system saves the original documents from excessive handling, and thus aids in preservation, while allowing extensive cross-referencing without requiring additional physical space.

These digitization efforts will continue so that our online archive will emerge as a valuable research tool for scholars, students, or interested members of the public. It also ensures compliance with state laws related to the retention period for documents and gives staff an opportunity to review paperwork to screen out confidential information, such as Social Security numbers.

Historical Highlights. The centerpiece of the UT system's board office exhibit is an authentic reproduction of the original handwritten 1881 board minutes, which were reproduced by UT Austin Printing. The expertise of various staff members of the conservation program at that institution's Harry Ransom Humanities Research Center made it possible to authentically recreate these seminal minutes. A DigiBook—acquired specifically to scan UT Austin's rare books and manuscripts without damaging the materials—allowed safe digitization.

A pristine electronic copy of the 1881 minutes was then passed on to UT's printing facility, where experts selected appropriate paper and binder covers to make four copies almost identical to the original. While the reproductions look exactly like the original, the experts used a sturdier paper so the pages can be handled without the risk of accidental tears or spills destroying the paper.

The result is a beautiful bound volume that can be perused by visitors who might enjoy seeing a list of the salaries of the first faculty members in 1883, a summary of the classes first offered at UT Austin, and a description of agenda items considered by the original regents in the late 19th century. As an added bonus, a high-quality scan of the 1881 minutes is available on CD.

A historical display case custom-made by a UT Austin Physical Plant team showcases the reproduction of the original minutes and allows exhibition of meaningful physical objects, such as original volumes of *The University Record,* that detail the system's policies and rules. A sample bronze medallion given to regents at the start of their terms reflects the weight of their responsibilities.

Also on display is a limited-edition book given to special honorees and various gavels regents have used over the years—one of which is made from the wood of UT Austin's Old Main Building, which was razed in 1934, and another gavel from the rig timber of the original oil well that in 1923 produced the first gusher for our Permanent University Fund.

Past and Future. At the strategic level, the history of the governing body of a higher education institution builds a sense of shared culture among board members and professionals, even as it helps them make sense of the current university structure and policies.

The history of the board builds a sense of shared culture among board members and professionals, even as it helps them make sense of the current university structure and policies.

But as Lewis Carroll noted, "It's a poor sort of memory that only works backward." A better appreciation of the record and decisions of boards can teach many lessons on how to move forward most strategically. The deeper understanding of the university that results is sure to contribute to a greater appreciation for all that has been accomplished and a better future for individual campuses and for the university system as a whole. ◆

AUTHORS: Francie A. Frederick is general counsel to the board of regents, and Rhonda Hankins is a board professional staff member, in the Office of the Board of Regents of the University of Texas System; other board office staff members contributed to the development of this article.
E-MAIL: ffrederick@utsystem.edu, rhankins@utsystem.edu
T'SHIP LINKS: Neal C. Johnson and Edward J. Finkel, "E-Boards Emerging," November/December 2005. James C. Hearn, Michael K. McLendon, and Leigh Z. Gilchrist, "The Mixed Blessings of Sunshine Laws," May/June 2004.

Attachment E

THE UNIVERSITY *of* TEXAS SYSTEM

MAJOR ACCOMPLISHMENTS

of

THE UNIVERSITY *of* TEXAS SYSTEM

for

2011, 2012, 2013*

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

1. UT Permian Basin

a. New petroleum engineering program.

b. New nursing program ($3 million for the building renovation to house the program and the thermal plant).

c. Established a new $10,000 degree in STEM fields.

d. Established a new $5,000 online degree program (Bachelor of Applied Arts and Science) that allows high school students with 60 semester credit hours to complete their degree in two years.

e. New blended and online course program with a goal of increasing enrollment from 4,000 to 5,500 in three to four years.

f. $67 million for new student housing over a four-year period.

g. First in Texas virtual/online high school/college collaboration with Presidio ISD, funded in part by Meadows Foundation grant. This unique Early College High School offers almost all courses online. (Note: Presidio ISD is 250 miles from UT Permian Basin.)

2. UT Tyler

a. New blended and online course program with a goal of doubling enrollment from 4,000 to 8,000 in five years. Funding of $4 million provided for technology infrastructure required for program.

b. New Doctor of Nursing Practice program.

c. Online graduate nursing programs rated 11th out of nearly 860 programs surveyed by the *U.S. News & World Report*.

d. Approved the creation of the College of Pharmacy after Texas Legislature passed UT Tyler Pharmacy Bill. Approved the proposed business model and tuition plan for the new school.

e. Approved the construction of a $22.5 million building to house the College of Pharmacy.

f. Board is negotiating to purchase a $16 million new student housing project.

g. Approval to establish a university charter school.

3. UT Arlington

a. Online nursing program with 9,000 students enrolled.

b. 20,755 students taking courses both online and on campus.

c. Increased enrollment from 25,000 in 2007 to 33,000 in 2012.

d. Tuition held flat in 2012 and 2013 because of online programs.

e. Best civil engineering school in North Texas.

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

f. $82 million College Park Center funded in 2009. (A majority of the Board that voted for funding in 2009 are current members of the Board.)

g. Shimadzu Institute for Research Technologies established with $7.5 million allocation of PUF, matched by Shimadzu Scientific Instruments. The Institute houses the Shimadzu Center for Advanced Analytical Chemistry, the Center for Imaging and the Center for Environmental, Forensic, and Materials Analysis.

h. Established a $10,000 degree plan.

i. $49 million for new student housing over a four-year period.

j. One of six universities in the nation named a "Next Generation University" in a report by the New America Foundation. The report recognizes "models of national reform" that are "continuing their commitment to world class research while increasing enrollment and graduation rates, even as the investments from their states have declined." The report is based on analyses of federal education data, site visits and interviews with university leaders.

k. In 2013, appointed Dr. Vistasp M. Karbhari as President of UT Arlington.

4. UT Dallas

a. Nationally top-ranked engineering school.

b. Flat tuition program for entire institution.

c. A commitment of $77 million approved in 2012 for the $108 million Bioengineering and Sciences Building.

d. Approved to move from the Capital Improvement Program to Design and Development the $81 million Edith O'Donnell Arts and Technology Building. (Commitment for funding approved in 2008.)

e. A commitment of $5 million approved in 2011 for the $25 million School of Management Phase II.

f. Ranked one of nation's best values among public colleges.

g. $168 million for new student housing over a four-year period.

h. Ranked second in Texas Research Incentive Program (TRIP) funds among all eight universities in Texas vying for funding in quest for Tier One research status.

5. UT San Antonio

a. $44 million for new student housing over a four-year period.

b. Commitment of $22 million approved for the $52 million academic and administrative office building.

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

c. New campus master plan.

d. Raised admission standards.

e. New highly successful football team and success of program (attendance/wins) catapulted institution to a new, highly competitive athletic conference ahead of schedule.

f. Ongoing joint education and research program with UTHSC San Antonio.

g. Approval to establish a Doctor of Translation Science degree program offered jointly with UTHSC San Antonio, UT Austin and UTHSC Houston.

h. $25 million renovation in an administrative and classroom building.

I. $22 million for new Park West Athletics Complex.

j. $6.5 million for an Engineering Design and Innovation Center.

k. College of Business named among the "Best of the Best" Top MBA Schools for Hispanics by DiversityComm, Inc. and its four diversity magazines.

l. Approval to establish a Ph.D. degree in Mechanical Engineering.

m. UTSA, along with UT Arlington and UT El Paso, now eligible for $159 million Texas Competitive Knowledge Fund.

6. UT Pan American and UT Brownsville and the RAHC in Harlingen

a. Approved a new university for South Texas eligible for Permanent University Funds.

1. A university of the 21st Century.
2. A university initially serving 28,000 students and estimated to grow over ten years to more than twice that size.
3. The second largest Hispanic-serving university in America in terms of enrollment.

b. Time from the first Vista Summit in October 2011 until consideration of the legislative bill for the new university was only 17 months!

c. Approval for a new medical school and a commitment of $100 million by the Regents and $10 million for each year of the biennium from the Legislature. Current plans are for the first class of medical students to be admitted into a South Texas track through or at UTHSC-SA in 2014, consistent with Liaison Committee on Medical Education (LCME) guidelines. Students will receive first two years of education in San Antonio and last two years in the Rio Grande Valley.

d. On July 16, 2013, Governor Perry joined key Texas legislators and more than a thousand students, parents, educators, and community leaders from across South Texas to celebrate landmark legislation authorizing the creation of a new UT university, which will include a medical school in the Rio Grande Valley. The Governor ceremonially signed copies of Senate Bill 24, the legislation that authorizes the creation of the new university, in both Edinburg and Brownsville.

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

e. $30 million commitment to develop UTeach, a simulated hospital, and faculty funding using STARS equivalent funds for the best researchers in bio-medicine, energy/environment science and manufacturing engineering.

f. UT Brownsville established a new $10,000 degree plan.

g. Approval of a $42.7 million Fine Arts Academic and Performance Complex approved at UT Pan American to be funded primarily with tuition revenue bonds.

h. In 2013, UT Pan American received a $1.7 million National Science Foundation grant to help boost graduation rates in engineering and science.

i. Approval to issue a Request for Qualifications for development of a Campus Master Plan for the new university in South Texas.

j. In 2010, appointed Dr. Robert S. Nelsen as President of UT Pan American.

7. UT El Paso

a. Approved to move from the Capital Improvement Program to Design and Development the $59 million health science and nursing building. (Commitment for funding approved in 2008.)

b. Produces the most Hispanic graduate engineers in America.

c. College of Business Administration named among the "Best of the Best" Top MBA Schools for Hispanics by Diversity.Comm, Inc. and its four diversity magazines.

d. Approval to establish a Ph.D. degree in Ecology and Evolutionary Biology.

e. Approval to establish a Ph.D. degree in Biomedical Engineering.

f. Approval to establish a Doctor of Nursing Practice degree.

g. Approval to establish a Doctor of Physical Therapy degree.

h. $10 million Campus Transformation Project approved as part of the institution's centennial celebration.

i. $23 million for new student housing over a four-year period.

j. A team of student entrepreneurs who founded American Water Recycling, awarded $100,000 in seed funding for winning the UT System Horizon Fund Student Investment Competition.

8. UT Austin

a. Master plan for a $334 million medical school approved. With this plan as a guide, UT Austin is in a position to accommodate growth and enhance the existing campus, as well as extend, if needed, the infrastructure to new academic and research venues.

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

b. The Board agreed in 2012 to commit additional Available University Fund (AUF) monies toward the creation of a medical school, equal to the greater of $25 million annually or a 3% increase in annual AUF distribution. There is no limit established on how long the additional funds will be provided, and it is currently estimated that $25 million will exceed the additional 3% increase for at least the next eight years for a total of $200 million over that period of time.

c. In 2013, the Board allowed UT Austin to fund $150 million of the $310 million cost for the construction of the Engineering and Education Research Center for the Cockrell School of Engineering through the UT System's Revenue Financing System. The Regents had previously approved spending $105 million in Permanent University Funds to finance a third of the building's cost and UT Austin's plan to raise $105 million in gifts to be directed toward either construction of the building or broad-based initiatives for the School, including scholarships. Once the facility is complete, UT Austin has agreed to increase the number of undergraduate engineering students by 1,000 – the first significant increase in capacity for the School.

d. Nine Massive Open Online Courses (MOOCs) approved by edX. edX is a ground-breaking, non-profit blended and online learning initiative founded by Harvard University and the Massachusetts Institute of Technology. $1.5 million was loaned to develop these courses as part of a sustainable online program. Close to 100,000 students registered for the first four courses, which began September 1, 2013.

e. $6.6 million per year for two years ($13.2 million) to cover holding tuition flat, with encouragement to UT Austin leadership to find cost savings to cover this increase.

f. The Committee on Business Productivity identified potential savings of $490 million over 10 years. The Committee found these savings after reviewing only 25% of the UT Austin operations.

g. $20 million in Science and Technology Acquisition and Retention (STARS) funding to recruit outstanding faculty.

h. A commitment in 2011 of $28 million toward the $56 million to expand the High Performance Computing Facility.

i. Ranked 26th best university in the world by the *Center for World University Rankings*.

j. Ranked as one of the "Best Buys in Higher Education" by *Fiske Guide to Colleges*.

k. McCombs School of Business named among the "Best of the Best" Top MBA Schools for Hispanics by Diversity.Comm, Inc. and its four diversity magazines.

l. $20 million for four years to match external contributions targeted towards recruitment of faculty.

m. $10 million since 2010 to address significant fire and life safety projects.

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

n. $8 million to construct a permanent freestanding repository for the Blanton Museum.

o. Approval to establish a Ph.D. degree in African and African Diaspora Studies.

p. Approval to establish a Ph.D. degree in Statistics.

q. Total commitment by Regents is almost $1 billion since 2009.

9. UT MD Anderson

a. In 2011, appointed Ronald A. DePinho, M.D. as President of UT MD Anderson. President DePinho came out to UT MD Anderson from Harvard.

b. Hired almost the entire Belfer Institute research team (37 key researchers) from Harvard with a financial commitment from the Board to provide a financial backstop to UT MD Anderson.

c. Embarked on the "Moon Shots" program to cure eight kinds of cancer.

d. Board of Regents authorized comprehensive philanthropic, cause marketing and corporate alliance program - creating a new model of advancement - the first innovative plan of its kind in the UT System, to generate alternative private revenue streams.

e. Ranked by *U.S. News & World Report* as the nation's top hospital for cancer care for the seventh straight year. In the last 12 years, MD Anderson has ranked number one ten times.

10. UTHSC San Antonio

a. Commitment of $74 million approved for the $95 million Center for Oral Health Care and Research building.

b. $45 million for the Academic Learning and Teaching Center was approved.

c. $15 million since 2010 to address significant fire and life safety projects.

d. $13 million was allocated by the Board from Permanent University Bond proceeds to reduce the debt for the Cancer Therapy Research Center (CTRC). CTRC is using the $800,000 it saves annually in debt service payments to fund the compensation for researchers.

e. In 2009, appointed William L. Henrich, M.D., as President of the UTHSC San Antonio.

11. UTMB Galveston

a. Billion-dollar rebuilding program after Hurricane Ike. Significant "hardening" of buildings and infrastructure occurred to better protect buildings, labs, and other assets from future storms.

b. New network of clinics off the island to service patients in the Gulf Coast region.

c. Negotiated a new agreement with the state for health care of the prison population with substantial assistance from the UT System and the Board.

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

12. UT Southwestern Medical Center

a. *Academic Rankings of World Universities* published by Shanghai Jiao Tong University named UT Southwestern the sixth best world university in clinical medicine and pharmacy. The top five schools were Harvard University; University of California, San Francisco; University of Washington; Johns Hopkins University; and Columbia University. Twelve of the world's top 15 institutions in this category are in the United States.

b. Approved moving the $800 million Clements University Hospital from the Capital Improvement Program to Design and Development in 2010. Hospital was originally put on the Capital Improvement Program in 2003 and will be completed in 2014.

c. Approved $187 million for construction of an 11-story, 275,000 gross square feet academic/ clinical building.

13. UTHSC Tyler

a. Successful new Internal Medicine Program for 54 residents at Good Shepherd Medical Center in Longview, Texas, which will bring more physicians to East Texas.

b. In its first year, the new Cancer Center facility is reaching out to serve the health needs of East Texas at a rate which originally was thought to require several years.

c. Received the first National Institutes of Health (NIH) grant for commercialization of a new drug as part of a new NIH initiative in this area.

14. UTHSC Houston

a. UTHSC Houston started a unique program with BlueCross BlueShield of Texas to use de-identified patient data to study cost and treatments in Texas. This is one of the first efforts for academic analysis of this kind of data.

b. The institution also recently received one of the largest grants for a multi-disciplinary, multi-institutional study of trauma care led by Retired Colonel John Holcombe, M.D., who revolutionized treatment in Desert Storm.

c. $25 million in new student housing over a four-year period.

d. In 2012, appointed Giuseppe N. Colasurdo, M.D., as President of UTHSC Houston.

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

System-wide Initiatives and Recognition

1. The Chancellor's Framework for Advancing Excellence approved by the Board in August 2011. The Framework has facilitated the accomplishments achieved. The Chancellor has been invited to the White House twice to explain to the President, Vice President and Secretary of Education how the transformations in Texas are being accomplished. This Framework has become a national model on how to change higher education to meet the student needs of the 21st Century. The Board unanimously and enthusiastically approved the Framework. Ninety-five percent of the Framework has been implemented two years after it was approved.
2. The Transformation in Medical Education (TIME) initiative to produce better doctors faster has become a national model for transforming medical education. Combining undergraduate education with medical school education cuts one to two years from the traditional eight years for a medical degree. Regents committed $4 million to this initiative in 2010 and approved an additional $4 million to expand the program in 2013.
3. UT System has realized more than $2 billion in savings since 2007 by using and targeting innovative methods to save money, such as collective buying and outsourcing. In 2012, the System saved $383 million and expects to save another $2 billion by 2016. Regent Brenda Pejovich was asked last year by the Board Chairman to assist Executive Vice Chancellor for Business Affairs Dr. Scott Kelley and to represent the Board in helping expand and accelerate this effort.
4. UT System institutions had a record-breaking year for philanthropy in 2012. Overall giving (cash, pledges, and new testamentary gifts) reached $1.2 billion and actual cash received was $801 million. Nearly 220,000 individual donors joined with numerous corporations and foundations to achieve these exceptional results. Overall giving was $1.1 and $1.0 billion in 2010 and 2011 respectively, and cash received was $683 million and $744 million in 2010 and 2011 respectively.
5. In 2011, the UT System invested $10 million in the myEdu personal counseling software and has now provided it to every academic institution in the System. The software has been expanded to assist students in finding internships, good jobs, and will eventually be used to track students' success post-graduation. Please see the myEdu update attached to this list. (Note: The statistics attached are provided by myEdu and not by the UT System.)
6. The Milestone Agreement Form for Ph.D. students seeking degrees at UT institutions provides a System-wide template to be negotiated and signed by a Ph.D. student and their professor. It specifies for the student milestones he/she is to reach in moving toward graduation. This initiative will better inform graduate students about the post-Ph.D. world they will encounter and also help the candidates reduce time to degree.
7. Allocation of $90 million in Science and Technology Acquisition and Retention (STARS) funding to the academic and health institutions to recruit and retain high-quality faculty. (Note: This was a continued commitment from previous Boards and is continued today by the current Board.)

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

8. The Institute for Transformational Learning (ITL) was set up as part of the Chancellor's Framework. The Regents funded $50 million to build a System-wide program of blended and online learning. The ITL was responsible for negotiating the agreement with edX in just three months and funding the first round of massive open online courses (MOOCs) with edX.

9. The following prestigious honors and awards were presented to UT System faculty since 2011: Nobel Prize (one) and memberships in the National Academy of Science (five), Institute of Medicine (one), and National Academy of Engineering (three). Since 2011, the UT System has also recruited three faculty who have had these honors bestowed on them before coming to the UT System.

10. Degrees awarded for the institutions of the UT System have grown by 6% from 2011 to 2012.

11. Founded in 2011, the UT Horizon Fund is the strategic venture fund of The University of Texas System. Based on cutting-edge research at UT System institutions, the UT Horizon Fund works with entrepreneurs and the investment community to help translate innovations out of UT to practical use. The UT Horizon Fund is evergreen and returns are re-invested for future growth and development. $10 million was provided in 2011 for the first phase of the UT Horizon Fund, and another $12.5 million was added to the Fund in 2013.

    - Since its creation by UT System, the UT Horizon Fund has made nine investments in companies commercializing a diverse range of UT technologies including therapeutics for pain and aging, medical devices to treat cardiovascular and gastrointestinal disease, expanding mobile access and nanotechnology. UT Horizon funding has resulted in matching funding and the ratio of co-investment to UT Horizon funds is currently 20-to-1 on a portfolio basis.

    - In 2013, the UT Horizon Fund student investment competition included winners from five current UT System institution competitions (UT Austin, UT Dallas, UT San Antonio, UT El Paso and UT Pan American) and at-large applicants (UT Arlington, UT MD Anderson, UT Health Science Center at Houston, UT Health Science Center at San Antonio and UT Southwestern). On May 2, 2013, UT El Paso Ph. D. student Eva Deemer, MBA student Diego Capeletti, and undergraduate student Alex Pastor were awarded $100,000 in seed funding for their company, American Water Recycling. The company is commercializing graphene technology out of UT El Paso for separating waste from water.

    - In 2012, the UT Horizon Fund student investment competition awarded UT San Antonio student-faculty startup, Cardiovate, which offers a new and much-needed cardiovascular stent-graft to prevent aneurysm leakage following cardiovascular surgeries. The $50,000 award helped launch Cardiovate, and the startup has since moved to an incubator space and expects to close on an additional $100,000 seed funding soon.

12. Transparency and accountability in higher education in the UT System. The following measures have been implemented by the UT System during 2011 and 2012:

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

- **The UT System Productivity Dashboard:** This public website provides instant access to a huge range of data about our 15 institutions. This "dashboard" has been lauded as one of the best in the nation. With the click of a button, the public can have access to data on UT institution graduation rates, enrollment, cost of degrees, post-graduation success of our students and more, by visiting http://www.data.utsystem.edu. The UT System recently launched an iPad app to make this information even easier to access.
- **Public Information Requests:** All UT System academic institutions now have online databases of public information requests that are up-to-date and accessible by the public. Simply go to http://www.utsystem.edu/open-records/institutional-open-records-information for links to make and view any open records requests that have been made to UT institutions. Plans are in the works to make this database even more informative and user-friendly.
- **Conflicts of Interest Database:** Regents' *Rule* 30301 has strengthened conflict of interest and conflict of commitment policies for all employees of the System and UT institutions. The UT System is now a national leader in this area. Campuses will be finalizing their institutional policies and the collection of data will be occurring in the coming months.
- **Reducing Student Debt:** It is critical that students and parents fully understand the true cost of college, the cost of different degrees and the cost of taking on various forms of debt. The UT System and UT institutions are providing this information in a variety of ways, including through this website: http://www.utsystem.edu/affordability/.
- **Research Data Repository:** Through a secure database, faculty from all 15 UT System institutions can now review research being done on other UT campuses. This allows professors and researchers to find colleagues performing similar research so that they can collaborate and even pursue grants together. This kind of access and sharing ultimately could lead to new discoveries and cures.

13. On June 4, 2013, Chancellor Cigarroa hosted more than 100 key Texas education and business leaders to discuss how to revitalize partnerships among higher education, government, philanthropy and business. The meeting was the third of five that will be held across the United States. Discussion centered on a recent report created by *The National Academy of Sciences* and a group of top government, university, and business leaders, including Chancellor Cigarroa.
14. On June 21, 2013, Chancellor Cigarroa and Executive Vice Chancellor for Business Affairs Kelley spoke with the White House Domestic Policy Council as part of an ongoing partnership to promote college affordability and completion.
15. On June 27, 2013, Chancellor Cigarroa was announced as the recipient of the Chair's Award, one of the highest honors given by the Congressional Hispanic Caucus Institute.

UT SYSTEM MAJOR ACCOMPLISHMENTS
2011, 2012, 2013*

16. Dr. Stephanie Hule, Vice Chancellor for UT System Strategic Initiatives, is leading a national effort to increase student success, reduce administrative costs, and improve system and campus capacity to use data. Dr. Hule was selected to serve as chair of an advisory committee with the National Association of System Heads, which is funding the initiative with a grant from the Bill and Melinda Gates Foundation.

17. The Southwest District of the Council for Advancement and Support of Education (CASE) has recognized the fundraising and advancement services of the UT System with the Gold Award for Building Philanthropic Capacity Among UT Institutions and the Silver Award for Endowment, Stewardship and Compliance. The Southwest District encompasses a five-state region and more than 200 universities.

18. Finish@UT is an online program that was created for students who have earned their core college credits but need a flexible and affordable path to complete an undergraduate degree. Students can take accelerated courses entirely online in a broad range of degree programs offered through UT Arlington, UT Brownsville, UT El Paso and UT Permian Basin. It is estimated that there are 34,000 individuals in Texas who could utilize this program to finish their degrees.

19. Chairman Powell established five task forces to ensure best practices across the UT System:

    - **Task Force on Blended and Online Learning:** charged with reviewing current online course instruction at the UT System and its academic institutions. In addition, the task force identified successful approaches and best practices in online instruction across the nation at other higher education institutions. Work done by the Task Force form the basis and foundation of the Framework for Advancing Excellence. This Task Force was chaired by Regent Wallace Hall.
    - **Task Forced on University Excellence and Productivity:** charged with reviewing the efficiency and productivity of the UT System academic institutions, while at the same time, increasing the quality of education and maintaining excellence across the UT System. Work done by the Task Force form the basis and foundation of the Framework for Advancing Excellence. This Task Force was chaired by Regent Brenda Pejovich.
    - **Task Force on Employee/Student Relationships:** charged with reviewing and making recommendations on issues surrounding inappropriate relationships between employees and students at all UT System institutions and reviewing all existing programs directed at preventing sexual abuse, sexual harassment and sexual misconduct to ensure a safe, healthy environment for students. The goal is to write and establish a national model for relationships that occur in higher education. Report is expected in November 2013. This Task Force is chaired by current Chairman Paul L. Foster.

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

- **Advisory Task Force on Best Practices Regarding University-Affiliated Foundation Relationships:**
  established to identify best practices for relationships between UT System institutions and the UT System and affiliated foundations and serve as a national model for public universities for the best management, compliance and oversight practices. A draft report containing five recommendations was sent in August 2013 to all UT presidents and the heads of each affiliated foundation for comment. This Task Force was chaired by Regent Brenda Pejovich.
- **Task Force on Engineering Education for the 21st Century: charged with** reviewing and identifying key issues related to demand, capacity, efficiency, supply and research related to engineering programs in the state of Texas; how these issues impact Texas and the nation; and what the UT System can do to be most responsive to the state's needs. The Task Force is expected to finalize its recommendations this fall. This Task Force is chaired by Regent Alex Cranberg and UT Dallas President David Daniel.

20. Inducted twelve outstanding educators into the inaugural class of the UT System Academy of Distinguished Teachers. The Academy was created to recognize outstanding educators at UT's nine academic institutions. The Academy will serve as a System-level advocacy group dedicated to enhancing teaching, fostering innovation in the classroom and promoting interdisciplinary perspectives on education.

21. Established a University Lands Advisory Committee to increase the level of expertise and suggest value-added recommendations that could be employed in the management of the Permanent University Fund Lands. The Committee is composed of five members with expertise in oil and gas, real estate or finance:
    - Mr. I. Jon Brumley, Bounty Investments, LP, Ft. Worth, Texas
    - Secretary Donald L. Evans, The Don Evans Group, Ltd., Midland, Texas
    - Mr. Printice L. Gary, Carleton Residential Properties, Dallas, Texas
    - Mr. Robert B. Rowling, TRT Holdings, Inc., Irving, Texas
    - Mr. R. H. "Steve" Stevens, Jr., Stevens & Matthews LLP, Houston, Texas

22. Texas Fresh Academia Industry Roundtable (FreshAIR) initiative developed to create successful partnerships between UT System health institutions and the life sciences industry. These partnerships between academia and industry offer advantages to both entities by addressing the challenges of developing innovative drugs for their mutual benefit and the wellbeing of society and ensuring that Texas remains competitive as a strong player in science and technology.

23. Funding of up to $1 million for campus security enhancements related to the deployment of security personnel and devices. Proposed campus security enhancements are intended to better prepare the UT System Police to respond to threats throughout the State of Texas at any of the 15 UT System institutions and where UT System affiliates and assets are located.

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

24. $1 million funding for Collegiate Recovery Programs at UT System academic institutions. These programs will offer resources to help students who are committed to living clean and sober lives.
25. New communication program developed to provide updates every three to four weeks with details of major activity around the System. This helps the Regents to be better informed on a regular basis.
26. New and improved detailed orientation and training program for new Regents.
27. New and improved detailed orientation and training program for new UT System institution presidents.
28. Highly successful 2013, 83rd Session, of the Texas Legislature, which resulted in:
    - Funding for higher education was up cumulatively by 7.53% for all UT academic institutions and 8.65% for all UT health institutions.
    - Authorization for the creation of a new University of Texas institution in South Texas, which will have an integrated medical school and will be eligible for support from the Permanent University Fund and additional state funding.
    - Funding for the Texas Competitive Knowledge Fund that has benefited UT Austin and UT Dallas and will now benefit UT Arlington, UT El Paso and UT San Antonio.
    - Funding for the Texas Research Incentive Program, which matches private philanthropy with state funds at the UT System's four emerging research institutions.
    - Funding the graduate medical education (GME) formula and new programs that will expand GME to address the state's health care workforce needs.
    - Allowing UT institutions to benefit from the federal funds generated through the Texas Healthcare Transformation and Quality Improvement Program (the Section 115 waiver).
    - Fund correctional care provided to the Texas Department of Criminal Justice by The University of Texas Medical Branch at Galveston.
    - State funding for the first time to offset the cost of the Hazelwood tuition benefit for veterans and their families.
    - A reshaped strategic relationship between the UT System and Board of Regents and the Texas Higher Education Coordinating Board.

***Selected activities initiated in other years and supported during 2011-13 identified by date.**

MyEdu Update

New products built and launched to meet UT System students demand:

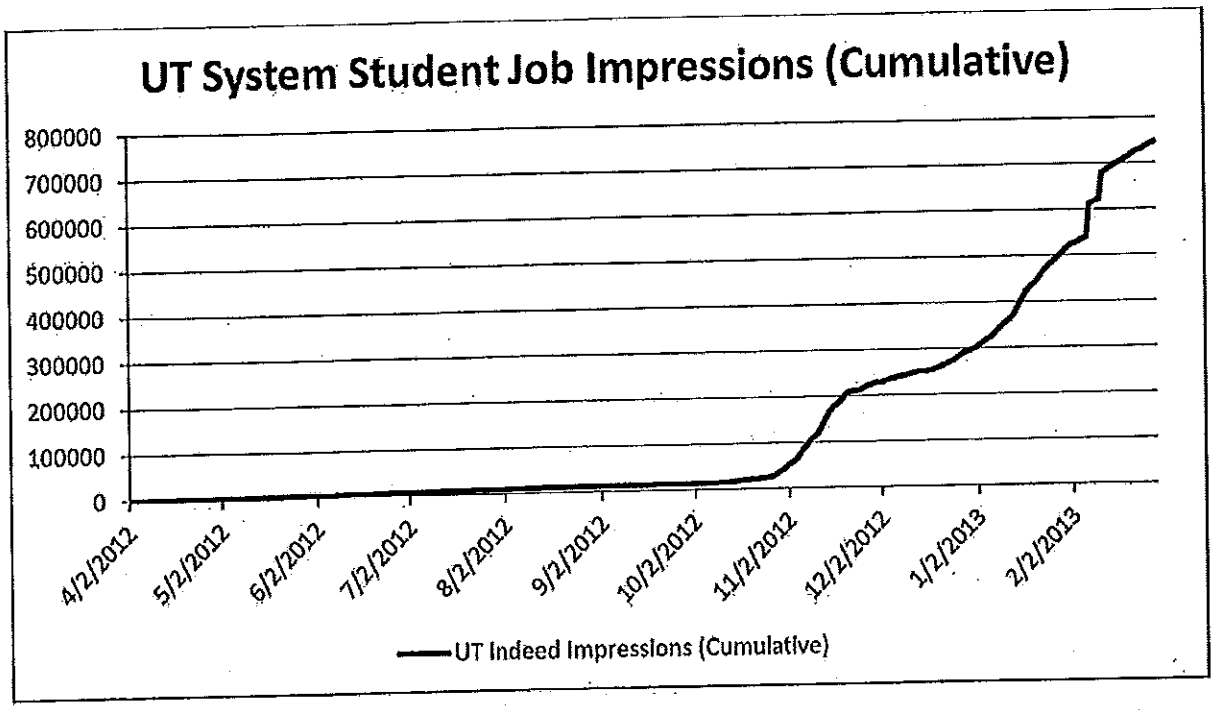
1) **Course Planning Tools** – significant improvements in course review, selection and planning. Integrated faculty input and ideas for greater participation / control.

2) **Student Profile** – an innovative product that improves the student's ability to tell their story to potential employers regarding skills, credentials and competencies. Replaces the resume.

3) **Student Job Platform** – a new platform that enables UT System students at all campuses to source, research and apply to internships and part / full-time jobs that match their skill sets.

4) **Employers Platform** – employers can connect with and target students about employment opportunities. Over 200,000 jobs in Texas have been captured and made available to students and alumni.

If there is any question regarding the importance of a Jobs platform, over 750k job views were initiated by UT System students in 4 months.



Major Products in under development:

1) **Personal Education Planner** – 1st product to enable students to plan / manage their education process regardless of where courses are taken, how many schools they attend and varying credits.
   a. Delivered a major research study on the Academic Journey for Students that was the foundation for the Education Planner design and functionality

Highlights of some of our UT System partnering activities:

1) The McCombs School of Business on integrating MyEdu to help schedule, promote and provide information into their on-line initiatives for their Foundation Courses
2) Partnering with Texas Exes for enabling students to interact, seek mentoring and increase potential job outcomes with alumni. Our joint development will be made available to all alumni organizations.
3) Partnering with President Bill Powers and Provost Steve Leslie on what more MyEdu can be doing for students to increase success rates
4) Partnering with UTSA and their CIO Ken Pierce on innovative initiatives for sharing information, content and leveraging secure sign-on technologies all to help students improve outcomes.
5) Partnering with Brownsville and their Career Services Office to increase jobs and career outcomes.
6) Meetings with Tyler, Arlington, Dallas, El Paso, Austin on working with and supporting their efforts to increase job outcomes for their students
7) Numerous discussions with campuses on how we integrate MyEdu into their online course initiatives

Some recent marketplace activities:

1) Gates Foundation – now providing grants to schools to deploy the MyEdu platform
2) Michael & Susan Dell Foundation – beginning to work with them on some key academic initiatives
3) SXSW – MyEdu heavily involved in the Education section and Ed Tech Incubator program

Key statistics:

1) 87,320 members – up 80% over the last 12 month
2) Member spend on average 54 minutes per month on the site
3) Averaging over 1,100 new members per week of UT System Students
4) 188,838 skills have been added in the last 90 days to their student profiles / resumes
5) 1,386,336 courses have been added to the schedule planner
6) 97% customer satisfaction rating
7) 750,000 job profiles / connections by UT System students in the prior 4 months

UT SYSTEM MAJOR ACCOMPLISHMENTS 2011, 2012, 2013*

The University of Texas System Board of Regents

2011, 2012 and 2013

Gene Powell, Chairman

Paul Foster, Vice Chairman*

Steve Hicks, Vice Chairman

Jim Dannenbaum, Vice Chairman**

Printice Gary, Regent**

Brenda Pejovich, Regent

Wallace Hall, Regent

Alex Cranberg, Regent

Robert Stillwell, Regent

Jeff Hildebrand, Regent ***

Ernest Aliseda, Regent***

*Became Chairman August, 2013

**Term expired February, 2013

***Term began February, 2013

Student Regents

Kyle Kalkwarf

John David Rutkauskos

Ashley Purgason

Nash Horne