MEMORANDUM
September 4, 2013

TO: Academic Council*

COPY TO:  
David Daniel
Hobson Wildenthal
Andrew Blanchard
Calvin Jamison
Abby Kratz
John Wiorowski
Austin Cunningham

Denis Dean
George Fair
Dennis Kratz
Bert Moore
Bruce Novak
Hasan Pirkul
Mark Spong

FROM: Office of Academic Governance
Christina McGowan, Academic Governance Secretary

SUBJECT: Academic Council Meeting

The Academic Council will meet on WEDNESDAY, SEPTEMBER 4, 2013 at 2:00 p.m. in the Osborne Conference Room, ECSS 3.503. Please bring the agenda packet with you to the meeting. If you cannot attend, please notify me at cgm130130@utdallas.edu or x4791.

Attachments

2013-2014 ACADEMIC COUNCIL
Gail Breen
R. Chandrasekaran
David Cordell**
Murray Leaf*
Ravi Prakash
Tim Redman
Liz Salter
Richard Scotch
Tres Thompson

Liza Liberman, Student Government President

*Speaker
**Secretary

AN EQUAL OPPORTUNITY/AFFIRMATIVE ACTION UNIVERSITY
AGENDA

ACADEMIC COUNCIL MEETING
September 4, 2013
Osborne Conference Room, ECSS 3.503

1. CALL TO ORDER, ANNOUNCEMENTS & QUESTIONS  Dr. Daniel
2. APPROVAL OF THE AGENDA  Dr. Leaf
3. APPROVAL OF MINUTES  Dr. Leaf
   August 8, 2013 Meeting
4. SPEAKER’S REPORT  Dr. Leaf
5. FAC REPORT  Dr. Leaf
6. CEP Proposals  Dr. Radhakrishnan
7. MOOC Discussion  Dr. Leaf
8. Introduction of Randall Rikel, University Controller  Dr. Leaf
9. Consideration of policy for Graduate Committees in Schools  Dr. Leaf
10. School By Laws  Dr. Leaf
11. Faculty Personnel Review Committee  Dr. Leaf
12. Recommendations of the Committee on Committees  Dr. Leaf
   (S06) CEP Vice Chair Selection
   (S11) Committee on Qualifications of Academic Personnel
   (S14) Academic Program Review
   (U07) Information Resources Security Planning, and Policy Change
   (U08) Institutional Animal Care and Use Committee
13. The Development of a Committee Succession Policy  Dr. Leaf
14. Course Caps  Dr. Leaf
15. Annual Report for the University & Senate Committees  Dr. Leaf
16. ADJOURNMENT  Dr. Daniel
UNAPPROVED AND UNCORRECTED MINUTES

These minutes are disseminated to provide timely information to the Academic Council. They have not been approved by the body in question, and, therefore, they are not the official minutes.

ACADEMIC COUNCIL MEETING
AUGUST 7, 2013

PRESENT: Hobson Wildenthal, Gail Breen, R. Chandrasekaran, David Cordell, Murray Leaf, Liz Salter, Richard Scotch, Tim Redman, Tres Thompson

ABSENT: David Daniel, Ravi Prakash,

VISITORS: Andrew Blanchard, Abby Kratz, Calvin Jamison

1. Call to Order, Announcements & Questions
Provoz Wildenthal called the meeting to order. The main point of discussion was the resolution on encryption on high risk university desktops. The Provost noted that many faculty feel that UT Austin’s policy on encryption is much more reasonable and constructive. He felt that the council should be positive towards a policy that would be a good alternative. Andrew Blanchard encouraged the council to review the CISO site of UT: Austin from all perspectives. The site has very critical and precise language in how procedures are handled and implemented. The style of information transfer and language used in terms of collaboration is very well done. Speaker Leaf recommended that Dr. Blanchard, and Tres Thompson take the site’s recommendations to the Information Security Advisory Committee. Ravi Prakash has already begun using these recommendations to create the resolution.

R. Chandrasekaran noted that there are two committees currently working on the encryption issue: the Senate’s Information Security Advisory Committee and the Presidential Advisory Committee on Encryption. The Presidential Committee met on July 31. The Provost attended the committee on the President’s behalf. There were three faculty on this committee. The committee discussed the Regents edict that all desktops purchased after September 1 2013 must be encrypted. The main debate was over the definition of how rigid “all” was. Between August 7 2013 and May 2014 all current critically important and vulnerable desktops would be encrypted. A discussion on what constitutes “vulnerable” and “critical” followed. Examples of vulnerable and critical data would be data such as UTD ID numbers and Social Security numbers that could easily be obtained by passersby. From the discussion the provost found that the issues related to encryption were the same as for laptops. The problem with laptops is that laptops can easily be carried away, stolen or left behind somewhere. Anything that was on the laptop could easily fall into the wrong hands in such a manner. It is for this same reason that encryption needs to be done on desktops. It is possible for someone to carry off a desktop. Therefore if a desktop contains vulnerable data, and is in a vulnerable area it must be encrypted. The question is if 15% of the 6000 campus desktops or 85% of the 6000 desktops will need to encrypted. A new third judicial committee would be created to say where the line for encryption would be drawn.

Tim Redman raised the question that structurally the layout of committees does not make sense as there is already a Faculty Senate committee on encryption already created. What is the need for a Presidential committee and a judicial committee? The provost assured the council that the Presidential committee
would not be the sole committee. The new judicial committee may be part of the Faculty Encryption Committee’s responsibilities, but would they want to review between 100-300 applications for encryption exemption as the process is tedious. Due to the tediousness, it is recommended that a judicial committee whose sole purpose is to review these applications be formed. Dr. Blanchard noted that the Senate faculty committee does not have representatives from the user community, i.e. finance, or other subject matter experts; their input on if data is critical or not is important.

The Provost hypothesized that no faculty member’s desktops in their office would be considered a ‘critical’ computer. If a faculty member has critical data on the desktop it should be removed. Speaker Leaf noted that it will depend on the guidelines. The Provost recommended that the Council be proactive and submit possible guidelines for the university itself. Speaker Leaf confirmed that the Senate Information Security Advisory Committee would be drafting a version of the UT: Austin policies for our university. They will also bring to the Senate the wording of a resolution worded to that effect. Dr. Blanchard recommended that when the policy is written that the implementation not be written into the policy itself.

R. Chandrasekaran asked if there a technical way to make it impossible for faculty to download the sensitive data if they should not have it. Dr. Blanchard responded by comparing back to the UT: Austin policy. The procedure recommends that they use a particular drive, and the IT group will put a piece of software on it so that checks the flag that the faculty member is encrypted. If you don’t want to do that, follow this other procedure you encrypt and every time you want to save you have to input your encryption key, and it automatically encrypts it to that drive. The faculty member can choose how they wish to protect their data.

UT Austin’s policy is independent of technology. They make the statement that here are a list of suggestions that they feel are best practices from other universities and industries. They recommend this and here is a piece of software that if you do the third way we also recommend this piece of software because it gives you additional security. Security in this instance means that if a faculty member encrypts their drive and forgets their encryption key/passcode they how have a paperweight, unless they use an additional piece of software that allows the faculty member to store their encryption key with the IT department in a safe place where if it is forgotten, the faculty member can go to them and retrieve it. Speaker Leaf reminded the council that a year ago a committee was formed with Cy Cantrell and others to work with Leah Teutsch to create a safe place for faculty to store their encryption keys. This committee has been side tracked by the CISO’s insistence that they verify encryption via the program ‘Remote Manage,’ rather than trust the faculty.

Dr. Blanchard responded that UT: Austin also uses a program called ‘Secure Docs”. It is a piece of software that sits on the front end that checks the flag. This is an issue of trust. It is Dr. Blanchard’s view that the faculty believe in Cam Beasley, the ISO for UT: Austin, when he says ‘I am just checking to make sure the flag is flipped because I have to report it.’ It is the only thing he is checking for. They operate in a Federation environment. For example, everyone shares federated software that assesses vulnerability. If someone is managing a piece infrastructure you take a common software run it and the report that comes out is sent to you as the manager of that particular environment, and sent to the CISO as a report. The two get together and say everything is good, or you have vulnerability. There is a very collaborative interface between those two people. It is all an issue of trust. That does not mean they do not load on the front end, and they are very up front about it i.e. “We use this program and we assess what you have done because we have to report if you are encrypted or not. If you self-encrypt, which is allowable, you must use the capability that lets them know you have self-encrypted. If you decrypt, and
your machine is stolen, it is grounds for dismissal. It is a responsibility of the university employee to know the universities information security policies, and be responsible for their actions.”

Provost commented that the concern for the ISO is that someone could walk away with a machine and take sensitive data stored on its hard drive. If the information is stored on a university server behind logins and passwords, it is not a problem. It is the possibility of information on the physical machine that is the concern.

Dr. Blanchard summarized that if the best encryption is used it is blind to the user. It is unobtrusive and the trust is there, and it is like logging into one’s machine and there are no hardships for anyone. This is what is happening at UT Austin.

Dr. Blanchard requested clarification if the HOP committee had seen any of the information security policies come from the CISO’s office come through the committee. Abby Kratz, as chair of the HOP committee, responded that none have come through the committee. It is one of the problems of the integrity of the HOP that these policies are not included in the HOP. Dr. Blanchard expressed his concern that the HOP committee was put in place by a Regent’s rule that says that any policy change or development that the stakeholders must be participant in the creation/amendment of the policies. That does not exclude anyone, including the President’s policies.

The priorities regarding this topic are by September first there must be a communication to campus how computers are to be purchased. Anything purchased after the first must meet the Chancellor’s requirement of encryption. The second, not due until May 2014, is that important machines currently on campus should be encrypted. The concern that many have is that every machine on campus will be encrypted. Dr. Blanchard is fairly sure that there are 15% of the computers on campus that will require encryption. Unless Faculty are dealing with students information on a daily basis, for example undergraduate or graduate deans, the faculty will be storing information on the H drive, or it is their research work.

The issue is not that the machine has to be encrypted it is that software is being put on the machines that in real time may continually verify that the machine is encrypted. The university, as an institution, has to manage the fact that we have done appropriate encryption. That means that the university must certify that faculty, and staff are encrypting their data. What does our sister institutions do in regards to the frequency of certification? It seems that UT Austin certifies once a quarter. Some argue that that is too much; by comparison our University is checked twice a day.

David Cordell brought up an example of a professor has a grade book they keep their personal laptop. It has names, net ids, and assignment grades. This is classified, according to Dr. Blanchard, as category two, FERPA/HEPA related information. The net ids are freely available but the student grades are protected information. This would require that the laptop be encrypted. It is situations like this where a judicial committee for encryption should be created. It was agreed that it is a best practice to not have any university information on an unencrypted personal laptop as it is too much of a personal liability.

In the next couple months 65,000 square feet will be added to campus. The new ATEC building will be opening. The only ‘hiccup’ is that some of the high tech option in classroom may not all be running at start of classes. The University expects to have an additional 2000 students starting classes this fall. The University is challenged to make sure students are in the right classrooms. Enrollment caps were set in such that 80% of the cap numbers end in zero. The reason is that we have 10% more students on campus. 20% of the incoming students have not registered as of August 7. The University already has 500 closed classes. It is a concern that there are classes where the room can hold 145 students but the class cap is 90. Isn’t it possible to allow 5 more students in the class?
Speaker Leaf noted that gradebook information kept for personal use is excluded from the category of “educational records maintained by the institution” in FERPA.

Calvin Jamison updated the Council on the current projects on going on campus. For this fall there will be 1600 new beds in the new residence hall. Most campuses will house 25% of their students on the campus. By now having 5000+ student beds on campus the university has now reached approximately 25%.

There will be 750 new parking spaces available in the new parking garage. The university will be moving people into the new rental space north of Synergy, Synergy North Place. A request to the Regents for more space to be built onto the Student Services building is being submitted.

2. Approval of the Agenda
   Tim Redman moved to approve the Agenda as circulated. Richard Scotch seconded. The motion carried.

3. Approval of Minutes
   Richard Scotch moved to approve the minutes as circulated. Liz Salter seconded. The minutes were approved.

4. Speaker’s Report
   1. New guidelines for bylaws for schools. The committee has nearly concluded. I think we have reached a consensus but the committee has not yet agreed to it explicitly. One more round of emails should do it. I expect to have the draft for the Council meeting in September. The most important change from the current guidelines is that each school will have an executive committee from the faculty or an academic advisory committee that will work with the dean, and more processes will be spelled out in such a way as to assure administrative transparency and appropriate consultation.
   2. Encryption policy continues to be a problem. President Daniel has authorized our ISO, Leah Teusch, to appoint her own consulting committee, which she has done. This appears to indicate an intent not to work with the Senate Information Security Advisory Committee. Nevertheless, our committee is continuing to try to work with her, and in any case to develop its own policy recommendations. This includes item 13 on the agenda. UT System policy is that when policies are formed, before they get system approval they should have been reviewed by all stakeholders. Regents Rules, in addition, are clear that when the stakeholders are “faculty,” this means faculty organized through the governance system. The HOP committee has been established to assure that this happens before policies are sent forward for approval. Our HOP committee has acted accordingly, and will doubtless continue to do so.

3. Everything else that has been under discussion is reflected in the agenda.

5. Faculty Advisory Council Report
   The Executive Committee of the Faculty Advisory Council will meet on Friday, August 9. The main purpose is to set the agenda for the full FAC meeting at the end of September

6. Presentation by Serenity King on the Senate Legislature and 5th year
   Serenity King wished to present a 10-15 minute presentation of “Higher Education Legislative Summary” and another 5-7 minute presentation on “SACS Fifth Year Report”. Tim Redman moved to have the presentation put on the agenda. Richard Scotch seconded. The motion carried.

7. Introduction of Randall Rikel, University Controller
   The introduction was moved to the September meeting as it would be a better time.
8. **Updates to Chapter 49**
   The documents presented came to the Council from the HOP committee. The requirement for faculty notification of outcomes had been deleted. Speaker Leaf had suggested it be restored. Gene Fitch and Tim Shaw were rewording the document to do this. Tim Redman moved to have it placed on the agenda provided that the amendments be circulated the week before the Senate meeting. Richard Scotch seconded. The motion carried.

9. **Consideration of Policy for Graduate Committees in Schools**
   This was brought to the Council’s attention by Tim Redman. There was a concern that a committee in the Arts and Humanities are turning down Masters and Doctoral thesis, over-ruling the expert committee. Murray Leaf and Tim Redman would work together to prepare proper wording for the policy. Tim Redman moved to table the discussion until the next meeting. Richard Scotch seconded. The motion carried.

10. **School By Laws**
    Since the third 3+3 committee meeting additional changes have been made. Dean Mark Spong made two substantive changes. They would eliminate the requirement of a secret ballot. Speaker Leaf and the committee are working on their responses. The other issue was regarding the creation/ dissolving of programs. It is the committees opinion this should be addressed in a university policy not in the school by-law policy. There was one other minor change regarding Centers. Tim Redman moved to table the discussion until the next Council meeting. R. Chandrasekaran seconded. The motion carried.

11. **Faculty Personnel Review Committee**
    This discussion could not proceed until the School Bylaws have been passed. Tim Redman moved to table his item until the next Council meeting. R. Chandrasekaran seconded. The motion carried.

12. **Recommendations of the Committee on Committees**
    At the Council’s request the Council went through each page of recommendations. The Committee on Core Curriculum had one change; Tonya Wissinger was recommended instead of Liz Salter, as Dr. Wissinger works more with core curriculum as Associate Dean. Daniel Wickberg would be recommended as chair of the Library Committee. Dr. Redman also requested that Monica Evans be his replacement on the Advisory Committee to the University Budget. Andy Blanchard requested that he be added to the Information Security Advisory Committee as he is the CIO, and should be an Ex-Officio of the committee. David Cordell informed the Council that David Ford agreed to serve on the Committee for the Support of Diversity and Equity. Liz Salter agreed to serve on the Auxiliary Services Advisory Committee. The Committee on Qualification’s approval was tabled until a response from two possible appointees can be obtained. The Academic Program Review Committee was withdrawn in order to update the charge by expanding he membership in view of the increased workload. The Information Resources Security, Planning, and Policy Committee will also be delayed due in order to consider modifications to the charge.
    Tim Redman move to place the amended recommendations on the Senate agenda. Tres Thompson seconded. The motion carried.

13. **Policy regarding the installation of Invasive Software on University Computers**
    Richard Scotch moved to place the items on the Senate agenda. Tim Redman seconded. The motion carried.
14. The Development of a Committee Succession Policy
Richard Scotch moved to table this item until next Council Meeting. Tim Redman seconded. The motion carried.

15. Appointing a replacement for Cy Cantrell on the Academic Council
When the Council was elected more members than the minimum were appointed. The Council agreed that a replacement was not required.

16. Resolution on the passing of Cy Cantrell
Tim Redman moved to have this item placed on the Senate agenda. Richard Scotch seconded. The motion carried.

17. Senate Approval of April 17, 2013 Caucus Minutes
Tim Redman moved to have this item placed on the Senate agenda. Richard Scotch seconded. The motion carried.

18. Annual Report from Senate and University Committees
Tim Redman moved to have this item placed on the Senate agenda. Richard Scotch seconded. The motion carried.

19. Senate Agenda for August 21, 2013:
1. Approval of April 17, 2013 Caucus Minutes (From July Council Meeting)
2. Framework for Excellence in Doctoral Education (From July Council Meeting)
3. UTDPP 1052-Policy on Procedures for Completing a Graduate Degree (From July Council Meeting)
4. Presentation by Serenity King
5. Updates to Chapter 49
6. Committee on Committee Recommendations
7. Resolution on the installation of invasive software on University Computer
8. Resolution of the passing of Cy Cantrell
9. Annual Reports from University and Senate Committees

There being no further business, Richard Scotch moved to adjourn. Dr. Chandrasekaran seconded. The meeting adjourned.

APPROVED: ______________________________________ DATE: ____________________________
Murray J. Leaf
Speaker of the Senate
BYLAWS GUIDELINES FOR SCHOOLS

Contents

PREFACE ................................................................................................................................................... 1
PREAMBLE ............................................................................................................................................... 3
FACULTY ................................................................................................................................................... 3
   Voting Faculty ......................................................................................................................................... 3
   Meetings and Voting of the School Faculty. ........................................................................................... 4
      Regular meetings: ................................................................................................................................ 4
      Caucus Meetings: ............................................................................................................................... 5
   Conduct of business. ............................................................................................................................... 5
ADMINISTRATIVE OFFICES .................................................................................................................. 6
   Program head ......................................................................................................................................... 7
STANDING COMMITTEES ........................................................................................................................ 8
KEY ADMINISTRATIVE PROCESSES...................................................................................................... 10
   Appointments of tenure system faculty .............................................................................................. 11
   Appointments of non-tenure-system faculty. ....................................................................................... 11
Provisions for Amending the Bylaws. ....................................................................................................... 12

PREFACE

This document contains guidelines to assist individual Schools within UTD to draft or modify their respective bylaws. The purpose of such bylaws is to assure clear, transparent, and appropriate faculty and administrative processes for carrying out the major recurrent activities in each of the several schools of the university.

This is a template, not a rigid prescription. Uniformity is desirable because it can assure that the same general principles are being applied in the same way, but it should not come at the cost of recognizing real differences in the situations to which our several schools must respond.

Bylaws should be clear, concise, and constructive. They should be process oriented rather than legalistic, representing a joint effort on the part of administration and faculty to arrive at mutually satisfactory ways to discuss and resolve common problems.

Academic tradition and Regents’ rules recognize a number of areas of policy that are primarily the responsibility of faculty. Rule 40101, section 3, articulates them this way:

3  General Authority
   Subject to the authority of the Board and subject further to the authority that the Board has vested in the various administrative officers and subdivisions of the System, the
faculties of the component institutions regularly offering instruction shall have a major role in the governance of their respective institutions in the following areas:

3.1 General academic policies and welfare.
3.2 Student life and activities.
3.3 Requirements of admission and graduation.
3.4 Honors and scholastic performance generally.
3.5 Approval of candidates for degrees.
3.6 Faculty rules of procedure. (Series: 40101)

The Board of Regents itself is responsible for other areas where the faculty has little voice, such as financial and fiscal security for the university as a whole, provision of physical facilities, and compliance with general law. The administration is in between, being delegated powers by the Regents but also responsible for carrying out academic policies established by the faculty. At the campus level, the division of responsibility between administration and faculty is represented by the rules and policies establishing the distinction between the faculty governance organization and the administration. Bylaws should establish how this division is implemented in schools and departments.

At the University of Texas at Dallas, the primary administrative unit is the school. The chief academic officer in a school is the dean. Deans are appointed by the President and report to the Provost; all the deans together make up the Council of Deans.

In Texas generally, by Coordinating Board convention, the degree-granting unit of the university is the program. Faculty must therefore be assigned to programs to carry out their teaching obligations. Every program must be assigned to at least one school for administrative purposes. Most programs are assigned to only one school. However, programs may utilize courses offered by other programs and other schools. UT Dallas has always sought to encourage interdisciplinary cooperation in program design, content, and implementation.

All of the faculty members assigned to the programs of a school make up the faculty of the school. The faculty of the school is responsible for academic policy in the school as a whole, and for exercising oversight over the individual programs. University policy requires schools to establish faculty committees for some of these purposes. Schools may develop additional committees or bodies on their own. The school bylaws are the primary document for describing what bodies will be responsible for such oversight and how it is to be carried out.

If a school has departments, the school bylaws should say what these departments are, and what their powers and responsibilities are compared to the powers and responsibilities of the faculty of the school as whole.

School bylaws must be drafted by a committee of faculty of the school, elected by the faculty of the school by secret ballot. Before adoption they must be available for consideration by all the faculty of the school. To be adopted, they must be approved by at least a majority of the faculty of the school in an open meeting with full notice and debate.
School bylaws may allow for departmental bylaws. Departmental bylaws should be consistent with school bylaws, which in turn should be consistent with UT rules and policies. If there are departmental bylaws, the departmental bylaws and the school bylaws together should be clear about which decisions are to be made at each level. It is generally understood at UT Dallas that meetings are conducted in accordance with Robert’s Rules of Order.

According to the amended Handbook of Operating Procedures, after the bylaws are approved by the school, they are to be approved by the Senate and the President. In reporting bylaw amendments to the Senate for approval, schools should describe the vote they received in the school.

Wherever these guidelines use the word “chair” for the head of a department or program, they should be understood as meaning “chair or head.”

The general elements that school bylaws should contain or should address are:

**PREAMBLE**

School bylaws should begin with a Preamble. The Preamble should name the school, the programs, the centers, and any other such features of the school organization that will be described in the bylaws. If there is an overall strategy that the school has agreed on in arriving at its policies and providing oversight to its operations, this could be usefully mentioned or described. For example, will the school rely heavily on meetings of the entire faculty, or will it delegate major functions to groupings of programs? If the latter, the groupings should be named here and included in the body of the description. For schools with departments, the departments should be named and the programs that each is responsible for. The preamble should also indicate whether there are features or aims in the school mission statement that should be referred to in its internal procedures.

The Preamble should also state that all meetings will be conducted according to Robert’s Rules of Order except as the bylaws may specify otherwise.

**FACULTY**

**VOTING FACULTY**

UT Dallas policy distinguishes Voting Faculty from the General Faculty. Voting faculty is only tenure-track. General faculty also includes non-tenure-track faculty, usually titled Senior Lecturer or Clinical Professor. The voting faculty of the university are described in The Handbook of Operating Procedures, Chapter 21, Section I B as follows:

Voting members of the General Faculty shall consist of the following:
(1) Faculty appointed half-time or more to The University of Texas at Dallas who hold the rank of Regental Professor, Professor, Associate Professor, or Assistant Professor.

(2) Faculty appointed to The University of Texas at Dallas who hold the rank of Instructor and who hold appointments of half-time or more.

The title “instructor” at UT Dallas has been used only for faculty newly hired to serve as Assistant Professors, but who failed to have their dissertations completed as promised. As such, the title is now substantially obsolete. Non-tenure-track faculty are not titled “instructor.”

The members of the voting faculty in the school may accord voting rights to members of the general faculty in the school on matters other than personnel actions for tenure-track faculty.

Since in principle all faculty meetings except those involving personnel decisions are open meetings, non-voting members of the general faculty must be able to attend meetings. Bylaws may say whether they have privilege of the floor. In the absence of a specification it should be assumed that they do have the privilege, since they would have it in a meeting of the Academic Senate.

The method of assigning faculty to programs should be described. This need not be overly formal. Self-selection and consensus are possible, as is assignment by the Dean. Catalogs list faculty associated with programs; this should describe how those associations are created. There is no numerical limit on the number of programs a faculty member can be assigned to for academic purposes, although for administrative purposes a school may assign one program or department as an administrative “home.”

If there are groupings of programs that faculty are assigned to apart from their associations with programs, this should be described.

If faculty are assigned to or associated with centers or institutes that are funded as part of the school activities, the method of making this assignment should be described.

A method for resolving disputes regarding the assignment of faculty to programs, program groupings, or centers, should be described.

**MEETINGS AND VOTING OF THE SCHOOL FACULTY.**

Bylaws should provide for two kinds of meetings: regular meetings and caucus meetings.

**Regular meetings:**
The bylaws should require at least two regular meetings per year on a fixed schedule. One meeting should be early in the fall term, the second near the end of the spring term.

If only two regular meetings are scheduled, provision must be made for calling additional meetings if faculty request them.

Regular meetings should be chaired by the Dean or the Dean’s Designee.

The quorum must be specified. In the absence of a different specification, a quorum is a majority of the voting faculty who are in residence that term.

Bylaws should specify the actions for which a vote of the full faculty is required.

Bylaws should specify where minutes will be kept and how they will be made available.

Bylaws should specify minimum notice for a meeting and for agenda items. They may also specify a requirement for accepting agenda items proposed during the meeting that were not on published agenda, such as by majority vote or two-thirds.

It should also be easy for faculty to call a regularly scheduled meeting, such as one of the annual meetings, if the dean fails to do so. The faculty might, for example, empower the chair of one of the faculty committees to call such a meeting.

Major decisions should be confined to meetings held in a period that corresponds to the nine month terms for which most faculty are appointed.

Caucus Meetings.
Bylaws should provide for caucus meetings of the faculty without the dean being present. Rules for the caucus may also exclude associate deans. Caucus meetings cannot make policies for the school that require assent of the dean.

Caucus meetings can formulate positions to be considered with the dean at regular meetings. There should be a simple procedure for a small number of faculty to call a caucus meeting of the faculty. Requirements for notice and for an agenda need not be the same as for a meeting called by the dean.

A caucus meeting may also be provided as a regular occurrence, as it is for the newly elected Senate.

CONDUCT OF BUSINESS.
There should be a statement that the school follows Roberts Rules of Order unless otherwise provided for in the bylaws. Examples of exceptions could include a procedure for the use of email ballots or alternative requirements for a quorum.
ADMINISTRATIVE OFFICERS

DEAN. The duties and responsibilities of the Dean with regard to academic policy should be indicated. In general, the Dean is responsible for the finances and physical resources of the school, representing the school to the Provost and President. The faculty, not the dean, has primary responsibility and the primary voice in setting academic policy in a strict sense, meaning setting intellectual standards and goals, setting the curriculum and standards for student evaluation, setting standards for and participating in peer review.

The section on the Dean should address, explicitly or implicitly, the way the balance between these two sets of responsibilities is maintained, respecting the integrity of each. The general duties of the Dean with regard to financial and other administrative policies should be indicated. Although it is understood at UTD that the Dean serves at the pleasure of the President and processes for selecting Deans are set by university and not school policy, there is no harm saying this. The common practice at UTD has been that the deans appoint the members of the school faculty committees. These appointive powers and the procedures for appointment should be indicated—who is appointed and by what process.

Schools may also have elected committees with elected chairs in addition to committees that must be elected under UT Dallas policies.

The role of the Dean in hiring should be described, distinguishing the positions that should be filled with faculty consultation and involvement from positions that the Dean can fill at his/her discretion.

ASSOCIATE DEAN FOR UNDERGRADUATE EDUCATION. These have clearly defined roles in university policy as members of the Council on Undergraduate Education, in preparing catalog copy, and usually in communicating with the scheduling office on course scheduling. These responsibilities should be delineated. In addition, the bylaws should specify how they are appointed (for example by the Dean or by the Dean with approval or confirmation of the faculty) qualifications, powers and duties. For example, must they be tenured? A persistent weak spot in the administration of our undergraduate programs has been supervision of contingent faculty, meaning faculty hired on a course-by-course or term-by-term basis. Is this part of their responsibilities? (If not, someone else should be responsible for them).

ASSOCIATE OR ASSISTANT DEAN FOR GRADUATE EDUCATION. This is an ex-officio member of the Graduate Council. They have established roles in coordinating the graduate programs, preparing catalog copy, and communicating with the scheduling office on course scheduling. Where these functions have devolved onto programs, as in NS&M, the relation of the Associate Dean for Graduate Studies for graduate studies to whoever does it in the programs should be indicated. Does the Associate Dean for Graduate Education have no responsibility at all (does copy go right from programs to the Dean?) or is there some limited responsibility?
The bylaws should specify how the Associate Dean for Graduate Education is appointed (for example by the Dean or by the Dean with approval or confirmation of the faculty), their qualifications (tenured only?), powers and duties. Is the Associate Dean for Graduate Education responsible for assigning TAs? Is the Associate Dean for Graduate Education responsible for hiring and supervising lecturers? (If not, the bylaws should say who is.) What is the role of the Associate Dean for Graduate Education in setting up *ad hoc* committees for dissertations?

**PROGRAM HEAD.**

Program heads are appointed by the school dean in consultation with the faculty.

**DEPARTMENT AND DEPARTMENT CHAIRS OR HEADS.** At present, only the School of Natural Sciences and Mathematics and the School of Engineering and Computer Science have departments. The chief administrative officer of a department is a “head” or “chair.” Departments are usually responsible for one or more academic programs. Department heads or chairs are appointed by the dean in consultation with the faculty.

The Chair position may also be a program head position for one or more programs, or the program head or heads may be separate.

Departments normally have an annual budget that includes faculty salaries. Chairs may have responsibilities in hiring. Chairs may also have responsibility for preparing annual review assessments and for preparing evaluations of faculty in the Period Performance Evaluations. They may also have responsibilities in setting course schedules, room assignments, and the like. A department should have an Executive Committee unless there are so few faculty that it is more efficient to have the entire faculty meet regularly with the Chair.

In schools with departments, bylaws should specify the term of appointment of the chair and whether it shall be renewable.

Each school should also specify the process by which the department chairs are appointed. Chairs appointed through an external search will be subject to the usual review process for faculty appointments and appointed by the President on recommendation of the Provost and Dean in the usual manner.

Departmental bylaws are probably better kept separate from school bylaws, but if schools have departments the school bylaws should indicate in general what part of school functions are delegated to departments and whether the departments should have further bylaws of their own.

**OTHER ADMINISTRATIVE ORGANIZATIONS WITHIN THE SCHOOL.** Some schools have groupings of programs that are not departments in the sense that they do not have budgetary autonomy and the main fiscal responsibilities of the school dean are not delegated to the faculty member who represents or heads these units. We have no established term for this kind of organization. Henceforth, bylaws should use either the term “program group” or “program area.” The faculty member designated to represent or coordinate them should be
designated “program group coordinator” or “area coordinator.” The choice between the two terms should be based on which provides the more accurate description. If they are in fact a grouping of programs, brought together because their courses or other activities are related or in order to share common resources, such as a secretary, they should be described as a program group. If they are rather a set of faculty brought together around a common interest that cross-cuts several programs, the idea of a “program area” and “area coordinator” is more appropriate. If they are significant in the teaching program of the school, the bylaws should describe such groups and the responsibility delegated to them.

CENTERS AND INSTITUTES. Our present Policy on University Research Units and Organized Research Units - UTDPP1010 assumes that centers or institutes are groupings of faculty concerned with common or interrelated research problems and are in principle independent of schools. Originally, they were conceived of as self-funding. As we have evolved, we have developed important centers with other kinds of functions and other kinds of funding. If a school has centers as an integral part of its functioning, and if faculty positions in the center are part of normal faculty assignments over which Deans, Associate Deans, or Department Heads have authority, their governance arrangements should also be included in the school bylaws. This should, again, indicate the arrangements for shared governance—are there faculty bodies to work with the directors and how are they constituted?

EVALUATION OF ADMINISTRATORS. Bylaws should note that Deans, Associate Deans, Department Chairs, and Program Heads are subject to upward evaluation under the UTD policy on Evaluation of Academic Administrators - UTDPP1047.

STANDING COMMITTEES

EXECUTIVE COMMITTEE OR ACADEMIC ADVISORY COMMITTEE. The previous Senate guidelines did not require school executive committees. School bylaws should now specify either an Executive Committee or an Academic Advisory Committee.

An Executive Committee is elected by the voting faculty of the school. The minimum size of such an Executive Committee should be seven. The bylaws may also provide for student representation on the Executive Committee. Election should be by secret ballot. The method should be specified in the bylaws. Schools may decide not to elect members at large; they could also be elected from specified subdivisions of the school faculty.

Faculty eligible for election to the Executive Committee shall not include the Dean, Associate Deans, Assistant Deans, or department Chairs or Heads.

Schools may choose to have an Academic Advisory Committee in place of Executive Committee. An Academic Advisory Committee will consist of the department heads or chairs of other such units together with at least three faculty who do not hold such appointments and who are elected by secret ballot from the school as whole. For an Academic Advisory Committee, it is important that the procedures for appointing chairs or program heads involves sufficient faculty
consultation that the chairs or program heads can properly be considered to represent faculty views and interests.

The Executive Committee or Academic Advisory Committee should meet with the dean regularly. Their scope of concern shall include academic policy and personnel matters that affect academic performance and faculty working conditions.

School bylaws may specify whether there should be formal faculty approval to authorize searches for new hires, and if so whether this approval should be by the school faculty, department faculty, program faculty, or Executive Committee. Non-tenure system faculty, if permitted under the school bylaws, shall not vote on personnel matters involving tenure system faculty. Student members shall not vote on personnel matters involving faculty.

While members of the Executive Committee may properly expect details of their views on delicate matters to be held confidential within the committee, the main actions of the committee recorded in minutes should be readily available to the faculty as a whole.

**FACULTY PERSONNEL REVIEW COMMITTEE.** This is a standing committee in each school mandated by three UT Dallas policies: the policy on annual reviews of faculty, on periodic performance evaluations, and on promotion and tenure. The Committee has a university charge that describes the general method of election. Bylaws may add further specifications. For example, in a school like ECS it might be advisable to specify representation by discipline.

**COMMITTEE ON EFFECTIVE TEACHING.** A school Committee on Effective Teaching is mandated by POLICY MEMORANDUM 96-III.21-70, which requires in part:

A. A teaching evaluation procedure developed and administered by an independent faculty committee.

B. Written objective standards for evaluating teaching performance. These standards must include student course evaluations, teaching load contributions, diversity of courses covered, course development and administration, and factors such as thesis and dissertation supervision.

C. Procedures for periodic collection of reliable and verifiable information related to teaching performance including periodic classroom visits by designated faculty to gather direct observation information that supplements information taken from sources such as course syllabi and student course evaluations.

D. Some mechanism for faculty to comment on their evaluations and provide information they feel is pertinent to the teaching evaluation process.
The bylaws should specify how the membership is constituted, the terms, how they report their results and to whom, and how their procedures are established, whether by the committee, the school, or both in some combined process.

**COMMITTEE FOR UNDERGRADUATE STUDIES.** In general, the bylaws should indicate who is responsible for planning, preparation of catalog copy, and scheduling courses in the undergraduate program. If this is done by an undergraduate program committee, then the bylaws should specify who the members are and how they are appointed or selected. If there is no school committee, then the bylaws should indicate who is responsible instead.

**COMMITTEE FOR GRADUATE STUDIES.** In general, the bylaws should indicate the process by which the graduate program is developed and implemented, specifically describing who is responsible for planning, preparation of catalog copy, and scheduling courses. If this is done by a graduate program committee, then the bylaws should describe it. If this is done by departments or programs, the bylaws should say how the information is aggregated and coordinated at the school level.

**PROGRAM COMMITTEES.** The bylaws may provide either for program committees associated with the various degree programs in the schools or combinations thereof, or they may provide a general pattern for all program committees. In either case, however, there should be clear provisions for who is to be on such committees, how disputes about who is to be on them are to be resolved, who chairs them, and what their relation is to the school committees. In schools with departments, program committees may be unnecessary; the decision should be up to the school or department.

**OTHER COMMITTEES.** Each school should specify their standing committees and when necessary should create temporary committees to meet their administrative and academic needs.

The bylaws should provide a way to form them, establish their operating rules, and dissolve them.

**KEY ADMINISTRATIVE PROCESSES.**

**STATE OF THE SCHOOL REPORT AND CONSULTATION.** The dean should present a “state of the school” report to the faculty at the beginning of each year at a meeting of the school faculty. This should include plans for searches and other program initiatives. The meeting should provide opportunity for discussion. Resolutions from the faculty in relation to the plan should be in order.

At the end of each spring term, the dean should report what was actually done and the faculty should again have the opportunity to offer advice and resolutions.
APPOINTMENTS OF TENURE SYSTEM FACULTY.

All appointments of tenure system faculty in the University of Texas at Dallas shall be made in accordance with the General Standards and Procedures: Initial Appointments to the Ranks of Instructor, Assistant Professor, Associate Professor, and Professor - UTDPP1057. Appointments to named chairs and appointments under the U T STARS program are not exceptions. A chaired professor is still a professor. They should go through the same approval process within the school as any other tenured appointment (assuming that it would be a tenured appointment).

University policy requires votes on all tenure and promotion reviews by “the faculty of the school or department in which the person under review has teaching and/or administrative responsibilities.” School bylaws should specify whether this vote is to be by department, school, or both. Bylaws may also specify the quorum requirements. The university policy specifies the procedure.

Ordinary searches. School bylaws may provide for faculty involvement in making up appropriate ad hoc committees for approved hires. Composition of such committees should require approval by either the Executive Committee or the full school faculty. If approval is to be by the full school faculty, bylaws should specify how the necessary meeting is to be called.

Opportunity searches. The bylaws may provide for faculty involvement in making up appropriate ad hoc committees. The default rule is that composition of ad hoc committees requires approval by the Executive Committee or Academic Advisory Committee. School bylaws may require approval by the full school faculty instead.

APPOINTMENTS OF NON-TENURE-SYSTEM FACULTY.

Bylaws should specify the approval process for hiring and reappointing non-tenure track faculty. This should include consultation with, or a recommendation from, the program faculty or program head.

Responsibility should be assigned for hiring part time faculty, adjunct or associate faculty, and for making non-tenure-track special appointments. There should also be provisions for the evaluation and reappointment of part time faculty, since these are not covered in the general University policies on promotion and tenure.

Criteria for promotion and tenure. University policy requires that faculty of the several schools develop their own supplementary guidelines to implement the general university criteria for promotion and tenure. The policy does not say what body represents “the faculty” for this purpose but it assumes that policies for the school will be made by the faculty of the school. This means that they should be approved by the faculty of the school as a whole, in assembly. School bylaws may delegate this to departments or other subordinate units.
CREATING NEW DEGREE PROGRAMS. School faculty should vote to approve new degree programs in the school. Bylaws should provide the procedure.

If there are departments, department faculty should vote to approve new degree programs in the department.

If the program involves faculty or disciplines from several departments, school bylaws should provide for votes in all the concerned departments.

Results of the votes should be reported to the Committee on Educational Policy and the Senate in requests for Senate approval of the new programs.

CLOSING EXISTING DEGREE PROGRAMS. Combining or eliminating degree programs and transferring their faculty to other programs in the school should require votes by the program faculty and school faculty. Voting procedures should be specified. Votes in programs should be taken before votes in departments (if any) or schools. Votes in programs should be made available to department faculty (if any) before they vote; results of the vote in programs and departments should be made available to school faculty before they vote.

Elimination of programs that would result in termination of tenured faculty requires conformance to Regents Rule 31003, Section 2, Elimination of Academic Positions of Programs: Elimination for Academic Reasons as implemented in the UTD Academic Program Abandonment Policy - UTDPP1000.

PROVISIONS FOR AMENDING THE BYLAWS

All bylaws should include a provision for amending the bylaws. Requirements now vary. Amendment should require at least a majority of the faculty present.
PREFACE

This document contains guidelines to assist individual Schools within UTD to draft or modify their respective bylaws. The purpose of such bylaws is to assure clear, transparent, and appropriate faculty and administrative processes for carrying out the major recurrent activities in each of the several schools of the university.

This is a template, not a rigid prescription. Uniformity is desirable because it can assure that the same general principles are being applied in the same way, but it should not come at the cost of recognizing real differences in the situations to which our several schools must respond.

Bylaws should be clear, concise, and constructive. They should be process oriented rather than legalistic, representing a joint effort on the part of administration and faculty to arrive at mutually satisfactory ways to discuss and resolve common problems.

Academic tradition and Regents’ rules recognize a number of areas of policy that are primarily the responsibility of faculty. Rule 40101, section 3, articulates them this way:
3 General Authority
Subject to the authority of the Board

[of Regents]

and subject further to the authority that the Board has vested in the various administrative officers and subdivisions of the System, the faculties of the component institutions regularly offering instruction shall have a major role in the governance of their respective institutions in the following areas:
3.1 General academic policies and welfare.
3.2 Student life and activities.
3.3 Requirements of admission and graduation.
3.4 Honors and scholastic performance generally.
3.5 Approval of candidates for degrees.
3.6 Faculty rules of procedure. (Series: 40101)

The Board of Regents itself is responsible for other areas where the faculty has little voice, such as financial and fiscal security for the university as a whole, provision of physical facilities, and compliance with general law. The administration is in between, being delegated powers by the Regents but also responsible for carrying out academic policies established by the faculty. At the campus level, the division of responsibility between administration and faculty is represented by the rules and policies establishing the distinction between the faculty governance organization and the administration. Bylaws should establish how this division is implemented in schools and departments.

At the University of Texas at Dallas, the primary administrative unit is the school. The chief academic officer in a school is the dean. Deans are appointed by the President and report to the Provost; all the deans together make up the Council of Deans.

In Texas generally, by Coordinating Board convention, the degree-granting unit of the university is the program. Faculty must therefore be assigned to programs to carry out their teaching obligations. Every program must be assigned to at least one school for administrative purposes. Most programs are assigned to only one school. However, programs may utilize courses offered by other programs and other schools. UT Dallas has always sought to encourage interdisciplinary cooperation in program design, content, and implementation.

All of the faculty members assigned to the programs of a school make up the faculty of the school. The faculty of the school is responsible for academic policy in the school as a whole, and for exercising oversight over the individual programs. University policy requires schools to establish faculty committees for some of these purposes. Schools may develop additional committees or bodies on their own.
The school bylaws are the primary document for describing what bodies will be responsible for such oversight and how it is to be carried out.

If a school has departments, the school bylaws should say what these departments are, and what their powers and responsibilities are compared to the powers and responsibilities of the faculty of the school as whole.

School bylaws must be drafted by a committee of faculty of the school, elected by the faculty of the school by secret ballot. Before adoption they must be available for consideration by all the faculty of the school. To be adopted, they must be approved by at least a majority of the faculty of the school in an open meeting with full notice and debate.

School bylaws may allow for departmental bylaws. Departmental bylaws should be consistent with school bylaws, which in turn should be consistent with UT rules and policies. If there are departmental bylaws, the departmental bylaws and the school bylaws together should be clear about which decisions are to be made at each level.

At UT Dallas, meetings are conducted in accordance with Robert’s Rules of Order.

It is generally understood at UT Dallas that meetings are conducted in accordance with Robert’s Rules of Order.

According to the amended Handbook of Operating Procedures, after the bylaws are approved by the school, they are to be approved by the Senate and the President. In reporting bylaw amendments to the Senate for approval, schools should describe the vote they received in the school.

Wherever these guidelines use the word “chair” for the head of a department or program, they should be understood as meaning “chair or head.”

The general elements that school bylaws should contain or should address are:

**PREAMBLE**
School bylaws should begin with a Preamble. The Preamble should name the school, the programs, the centers, and any other such features of the school organization that will be described in the bylaws. If there is an overall strategy that the school has agreed on in arriving at its policies and providing oversight to its operations, this could be usefully mentioned or described. For example, will the school rely heavily on meetings of the entire faculty, or will it delegate major functions to groupings of programs? If the latter, the groupings should be named here and included in the body of the description. For schools with departments, the departments should be named and the programs

[for which each is responsible.]

that each is responsible for. The preamble should also indicate whether there are features or aims in the school mission statement that should be referred to in its internal procedures.

The Preamble should also state that all meetings will be conducted according to Robert’s Rules of Order

[end here and delete “except as the bylaws may specify otherwise”]

except as the bylaws may specify otherwise.

**FACULTY**

**VOTING FACULTY**

UT Dallas policy distinguishes Voting Faculty from the General Faculty.

[The voting faculty consists only of tenured or tenure-track faculty.]

Voting faculty is only tenure-track. General faculty also includes non-tenure-track faculty, usually titled Senior Lecturer or Clinical Professor. The voting faculty of the university are described in The Handbook of Operating Procedures, Chapter 21, Section I B as follows:

Voting members of the General Faculty shall consist of the following:

1. Faculty appointed half-time or more to The University of Texas at Dallas who hold the rank of Regental Professor, Professor, Associate Professor, or Assistant Professor.
2. Faculty appointed to The University of Texas at Dallas who hold the rank of Instructor and who hold appointments of half-time or more.

The title “instructor” at UT Dallas has been used only for faculty newly hired to serve as Assistant Professors, but who failed to have their dissertations completed as promised. As such, the title is now substantially obsolete. Non-tenure-track faculty are not titled “instructor.”
The members of the voting faculty in the school may accord voting rights to

[some]

members of the general faculty in the school

[(usually ten percent)]

on matters other than

[policies that might affect]

personnel actions for tenure-track faculty.

Since in principle all faculty meetings except those involving personnel decisions are open meetings, non-voting members of the general faculty must be able to attend meetings. Bylaws may say whether they have privilege of the floor. In the absence of a specification it should be assumed that they do have the privilege, since they would have it in a meeting of the Academic Senate.

The method of assigning faculty to programs should be described. This need not be overly formal. Self-selection and consensus are possible, as is assignment by the Dean. Catalogs list faculty associated with programs; this should describe how those associations are created. There is no numerical limit on the number of programs a faculty member can be assigned to for academic purposes, although for administrative purposes a school may assign one program or department as an administrative “home.”

If there are groupings of programs that faculty are assigned to apart from their associations with programs, this should be described.

If faculty are assigned to or associated with centers or institutes that are funded as part of the school activities, the method of making this assignment should be described.

A method for resolving disputes regarding the assignment of faculty to programs, program groupings, or centers, should be described.

MEETINGS AND VOTING OF THE SCHOOL FACULTY.

Bylaws should provide for two kinds of meetings: regular meetings and caucus meetings.

Regular meetings:

The bylaws should require at least two regular meetings per year on a fixed schedule. One meeting should be early in the fall term, the second near the end of the spring term.
If only two regular meetings are scheduled, provision must be made for calling additional meetings if faculty request them.

Regular meetings should be chaired by the Dean or the Dean’s Designee.

The quorum must be specified. In the absence of a different specification, a quorum is a majority of the voting faculty who are in residence that term.

Bylaws should specify the actions for which a vote of a quorum of the full faculty is required.

Bylaws should specify where minutes will be kept and how they will be made available.

Bylaws should specify minimum notice for a meeting and for agenda items. They may also specify a requirement for accepting agenda items proposed during the meeting that were not on published agenda, such as by majority vote or two-thirds.

It should also be easy for faculty to call a regularly scheduled meeting, such as one of the annual meetings, if the dean fails to do so. The faculty might, for example, empower the chair of one of the faculty committees to call such a meeting.

Major decisions should be confined to meetings held in a period that corresponds to the nine month terms for which most faculty are appointed.

Caucus Meetings.
Bylaws should provide for caucus meetings of the faculty without the dean being present. Rules for the caucus may also exclude associate deans. Caucus meetings cannot make policies for the school that require assent of the dean.

Caucus meetings can formulate positions to be considered with the dean at regular meetings. There should be a simple procedure for a small number of faculty to call a caucus meeting of the faculty. Requirements for notice and for an agenda need not be the same as for a meeting called by the dean.
A caucus meeting may also be provided as a regular occurrence, as it is for the newly elected Senate.

CONDUCT OF BUSINESS.
There should be a statement that the school follows Roberts Rules of Order

[Robert’s Rules of Order.]

unless otherwise provided for in the bylaws.

[delete “unless otherwise provided for in the bylaws”]

Examples of
[Delete. Add “However, an exception could be made in the bylaws for”

exceptions could include

[delete]

a procedure for the use of email ballots or alternative requirements for a quorum.

ADMINISTRATIVE OFFICERS

DEAN. The duties and responsibilities of the Dean with regard to academic policy should be indicated. In general, the Dean is responsible for the finances and physical resources of the school, representing the school to the Provost and President. The faculty, not the dean, has primary responsibility and the primary voice in setting academic policy in a strict sense, meaning setting intellectual standards and goals, setting the curriculum and standards for student evaluation.

[and]

setting standards for and participating in peer review.

The section on the Dean should address, explicitly or implicitly, the way the balance between these two sets of responsibilities is maintained, respecting the integrity of each. The general duties of the Dean with regard to financial and other administrative policies should be indicated. Although it is understood at UTD that the Dean serves at the pleasure of the President and processes for selecting Deans are set by university and not school policy, there is no harm saying
The common practice at UTD has been that the deans appoint the members of the school faculty committees in consultation with the Executive Committee or the Academic Advisory Committee. These appointive powers and the procedures for appointment should be indicated—who is appointed and by what process.

Schools may also have elected committees with elected chairs in addition to committees that must be elected under UT Dallas policies.

The role of the Dean in hiring should be described, distinguishing the positions that should be filled with faculty consultation and involvement from positions that the Dean can fill at his/her discretion.

ASSOCIATE DEAN FOR UNDERGRADUATE EDUCATION. These have clearly defined roles in university policy as members of the Council on Undergraduate Education, in preparing catalog copy, and usually in communicating with the scheduling office on course scheduling. These responsibilities should be delineated. In addition, the bylaws should specify how they are appointed (for example by the Dean or by the Dean with approval or confirmation of the faculty) and their qualifications, powers and duties. For example, must they be tenured? A persistent weak spot in the administration of our undergraduate programs has been supervision of contingent faculty, meaning faculty hired on a course-by-course or term-by-term basis. Is this part of their responsibilities? (If not, someone else should be responsible for them).

ASSOCIATE OR ASSISTANT DEAN FOR GRADUATE EDUCATION. This is an ex-officio member of the Graduate Council. They have established roles in coordinating the graduate programs, preparing catalog copy, and communicating with the scheduling office on course scheduling. Where these functions have devolved onto programs, as in NS&M, the relation of the Associate Dean for Graduate Studies for graduate studies to whoever does it in the programs should be indicated. Does the Associate Dean for Graduate Education have no responsibility at all (does copy go right from programs to the Dean?) or is there some limited responsibility?

The bylaws should specify how the Associate Dean for Graduate Education is appointed (for example by the Dean or by the Dean with approval or confirmation of the faculty), their
qualifications (tenured only?), powers and duties. Is the Associate Dean for Graduate Education responsible for assigning TAs? Is the Associate Dean for Graduate Education responsible for hiring and supervising lecturers? (If not, the bylaws should say who is.) What is the role of the Associate Dean for Graduate Education in setting up ad hoc committees for dissertations?

PROGRAM HEAD.

Program heads are appointed by the school dean in consultation with the faculty.

DEPARTMENT AND DEPARTMENT CHAIRS OR HEADS. At present, only the School of Natural Sciences and Mathematics and the School of Engineering and Computer Science have departments. The chief administrative officer of a department is a “head” or “chair.” Departments are usually responsible for one or more academic programs. Department heads or chairs are appointed by the dean in consultation with the faculty.

The Chair position may also be a program head position for one or more programs, or the program head or chairs may be separate.

Departments normally have an annual budget that includes faculty salaries. Chairs may have responsibilities in hiring. Chairs may also have responsibility for preparing annual review assessments and for preparing evaluations of faculty in the Period Performance Evaluations. They may also have responsibilities in setting course schedules, room assignments, and the like. A department should have an Executive Committee unless there are so few faculty that it is more efficient to have the entire faculty meet regularly with the Chair.

In schools with departments, bylaws should specify the term of appointment of the chair and whether it shall be renewable.

Each school should also specify the process by which the department chairs are appointed. Chairs appointed through an external search will be subject to the usual review process for faculty appointments and appointed by the President on recommendation of the Provost and Dean in the usual manner.

Departmental bylaws are probably better kept separate from school bylaws, but if schools have departments the school bylaws should indicate in general what part of school functions are delegated to departments and whether the departments should have further bylaws of their own.

OTHER ADMINISTRATIVE ORGANIZATIONS WITHIN THE SCHOOL. Some schools have groupings of programs that are not departments in the sense that they do not have budgetary autonomy and the main fiscal responsibilities of the school dean are not delegated to the faculty member who represents or heads these units. We have no established term for this kind of organization. Henceforth, bylaws should use either the term “program group” or “program area.” The faculty member designated to represent or coordinate them should be designated “program group coordinator” or “area coordinator.” The choice between the two terms should be based on which provides the more accurate description. If they are in fact a
grouping of programs, brought together because their courses or other activities are related or in order to share common resources, such as a secretary, they should be described as a program group. If they are rather a set of faculty brought together around a common interest that cross-cuts several programs, the idea of a “program area” and “area coordinator” is more appropriate. If they are significant in the teaching program of the school, the bylaws should describe such groups and the responsibility delegated to them.

CENTERS AND INSTITUTES. Our present Policy on University Research Units and Organized Research Units - UTDPP1010 assumes that centers or institutes are groupings of faculty concerned with common or interrelated research problems and are in principle independent of schools. Originally, they were conceived of as self-funding. As we have evolved, we have developed important centers with other kinds of functions and other kinds of funding. If a school has centers as an integral part of its functioning, and if faculty positions in the center are part of normal faculty assignments over which Deans, Associate Deans, or Department Heads have authority, their governance arrangements should also be included in the school bylaws. This should, again, indicate the arrangements for shared governance—are there faculty bodies to work with the directors and how are they constituted?

EVALUATION OF ADMINISTRATORS. Bylaws should note that Deans, Associate Deans, Department Chairs, and Program Heads are subject to upward evaluation under the UTD policy on Evaluation of Academic Administrators - UTDPP1047.

STANDING COMMITTEES

EXECUTIVE COMMITTEE OR ACADEMIC ADVISORY COMMITTEE. The previous Senate guidelines did not require school executive committees. School bylaws should now specify either an Executive Committee or an Academic Advisory Committee.

An Executive Committee is elected by the voting faculty of the school. The minimum size of such an Executive Committee should be seven. The bylaws may also provide for student representation on the Executive Committee.

[The election will be conducted with an open nominating procedure and a secret ballot.]

If the method is the same as that used to elect the UTD Academic Council, the result should be as in the Council—generally well balanced representation from the major constituencies as the faculty sees them. Election should be by secret ballot. The method should be specified in the bylaws. Schools may decide not to elect members at large; they could also be elected from specified subdivisions of the school faculty.

Faculty eligible for election to the Executive Committee shall not include the Dean, Associate Deans, Assistant Deans, or department Chairs or Heads.

Schools may choose to have an Academic Advisory Committee in place of Executive Committee. An Academic Advisory Committee will consist of the department heads or chairs of
other such units together with at least three faculty who do not hold such appointments and who are elected by secret ballot from the school as whole. **For an Academic Advisory Committee, it is important that the procedures for appointing chairs or program heads involves sufficient faculty consultation that the chairs or program heads can properly be considered to represent faculty views and interests.**

The Executive Committee or Academic Advisory Committee should meet with the dean regularly. Their scope of concern shall include academic policy and personnel matters that affect academic performance and faculty working conditions.

School bylaws may specify whether there should be formal faculty approval to authorize searches for new hires, and if so whether this approval should be by the school faculty, department faculty, program faculty, or Executive

[or Academic Advisory]

Committee. Non-tenure system faculty, if permitted under the school bylaws, shall not vote on personnel matters involving

[tenure-system]

tenure system faculty. Student members shall not vote on personnel matters involving faculty.

While members of the Executive Committee may properly expect details of their views on delicate matters to be held confidential within the committee, the main actions

[the votes]

of the committee recorded in minutes should be readily available to the faculty as a whole.

**FACULTY PERSONNEL REVIEW COMMITTEE.** This is a standing committee in each school mandated by three UT Dallas policies: the policy on annual reviews of faculty, on periodic performance evaluations, and on promotion and tenure. The Committee has a university charge that describes the general method of election. Bylaws may add further specifications. For example, in a school like ECS it might be advisable to specify representation by discipline.

[Since only equal or above-rank faculty can participate in these reviews, it is recommended that this committee should consist of tenured full professors.]

**COMMITTEE ON EFFECTIVE TEACHING.** A school Committee on Effective Teaching is mandated by POLICY MEMORANDUM 96-III.21-70, which requires in part:

A. A teaching evaluation procedure developed and administered by an independent faculty committee.
B. Written objective standards for evaluating teaching performance. These standards must include student course evaluations, teaching load contributions, diversity of courses covered, course development and administration, and factors such as thesis and dissertation supervision.

C. Procedures for periodic collection of reliable and verifiable information related to teaching performance including periodic classroom visits by designated faculty to gather direct observational information that supplements information taken from sources such as course syllabi and student course evaluations.

D. Some mechanism for faculty to comment on their evaluations and provide information they feel is pertinent to the teaching evaluation process.

The bylaws should specify how the membership is constituted, the terms for which they serve, how they report their results and to whom, and how their procedures are established, whether by the committee, the school, or both in some combined process.

COMMITTEE FOR UNDERGRADUATE STUDIES. In general, the bylaws should indicate who is responsible for planning, preparation of catalog copy, and scheduling courses in the undergraduate program. If this is done by an undergraduate program committee, then the bylaws should specify who the members are and how they are appointed or selected. If there is no school committee, then the bylaws should indicate who is responsible instead.

COMMITTEE FOR GRADUATE STUDIES. In general, the bylaws should indicate the process by which the graduate program is developed and implemented, specifically describing who is responsible for planning, preparation of catalog copy, and scheduling courses. If this is done by a graduate program committee, then the bylaws should describe it. If this is done by departments or programs, the bylaws should say how the information is aggregated and coordinated at the school level.
PROGRAM COMMITTEES. The bylaws may provide either for program committees associated with the various degree programs in the schools or combinations thereof, or they may provide a general pattern for all program committees. In either case, however, there should be clear provisions for who is to be on such committees, how disputes about who is to be on them are to be resolved, who chairs them, and what their relation is to the school committees. In schools with departments, program committees may be unnecessary; the decision should be up to the school or department.

OTHER COMMITTEES. Each school should specify their standing committees and when necessary should create temporary committees to meet their administrative and academic needs.

The bylaws should provide a way to form them, establish their operating rules, and dissolve them.

KEY ADMINISTRATIVE PROCESSES.

STATE OF THE SCHOOL REPORT AND CONSULTATION. The dean should present a “state of the school” report to the faculty at the beginning of each year at a meeting of the school faculty. This should include plans for searches and other program initiatives. The meeting should provide opportunity for discussion. Resolutions from the faculty in relation to the plan should be in order.

At the end of each spring term, the dean should report what was actually done and the faculty should again have the opportunity to offer advice and resolutions.

APPOINTMENTS OF TENURE SYSTEM FACULTY.

All appointments of tenure system faculty in the University of Texas at Dallas shall be made in accordance with the General Standards and Procedures: Initial Appointments to the Ranks of Instructor, Assistant Professor, Associate Professor, and Professor - UTDPP1057. Appointments to named chairs and appointments under the UT STARS program are not exceptions. A chaired professor is still a professor. They should go
[Appointments must] through the same approval process within the school as any other tenured appointment (assuming that it would be a tenured appointment).

University policy requires votes on all tenure and promotion reviews by “the faculty of the school or department in which the person under review has teaching and/or administrative responsibilities.” School bylaws should specify whether this vote is to be by department, school, or both. Bylaws may [must] also specify the quorum requirements. The university policy specifies the procedure.

**Ordinary searches.** School bylaws may provide for faculty involvement in making up appropriate ad hoc [ad hoc] committees for approved hires.

[The composition] Composition of such committees should require approval by either the Executive Committee or the full school faculty. If approval is to be by the full school faculty, bylaws should specify how the necessary meeting is to be called.

**Opportunity Searches.** The bylaws may provide for faculty involvement in making up appropriate ad hoc [ad hoc] committees. The default rule is that composition of ad hoc [ad hoc] committees requires approval by the Executive Committee or Academic Advisory Committee. School bylaws may require approval by the full school faculty instead.

**APPOINTMENTS OF NON-TENURE-SYSTEM FACULTY.**

Bylaws should specify the approval process for hiring and reappointing non-tenure track faculty. This should include consultation with, or a recommendation from, the program faculty or program head.
Responsibility should be assigned for hiring part-time faculty, adjunct or associate faculty, and for making non-tenure-track special appointments. There should also be provisions for the evaluation and reappointment of part-time faculty, since these are not covered in the general University policies on promotion and tenure.

**Criteria for promotion and tenure.** University policy requires that faculty of the several schools develop their own supplementary guidelines to implement the general university criteria for promotion and tenure. The policy does not say what body represents “the faculty” for this purpose but it assumes that policies for the school will be made by the faculty of the school. This means that they should be approved by the faculty of the school as a whole, in assembly. School bylaws may delegate this to departments or other subordinate units.

**CREATING NEW DEGREE PROGRAMS.** School faculty should vote to approve new degree programs in the school. Bylaws should provide the procedure.

If there are departments, department faculty should vote to approve new degree programs in the department.

If the program involves faculty or disciplines from several departments, school bylaws should provide for votes in all the concerned departments.

Results of the votes should be reported to the Committee on Educational Policy and the Senate in requests for Senate approval of the new programs.

**CLOSING EXISTING DEGREE PROGRAMS.** Combining or eliminating degree programs and transferring their faculty to other programs in the school should require votes by the program faculty and school faculty. Voting procedures should be specified. Votes in programs should be taken before votes in departments (if any) or schools. Votes in programs should be made available to department faculty (if any) before they vote; results of the vote in programs and departments should be made available to school faculty before they vote.

Elimination of programs that would result in termination of tenured faculty requires conformance to Regents Rule 31003, Section 2, Elimination of Academic Positions of Programs: Elimination for Academic Reasons as implemented in the UTD Academic Program Abandonment Policy - UTDPP1000.
AUTHORITY

No provisions in the various bylaws may override or contravene established university or Regents’ policies.

PROVISIONS FOR AMENDING THE BYLAWS

All bylaws should include a provision for amending the bylaws. Requirements now vary. Amendment should require at least a majority of the faculty present.
Proposed policy

Faculty Personnel Review Committee

Each School in the University of Texas at Dallas with more than four tenure-track faculty shall establish a Faculty Personnel Review Committee. The Committee has a general responsibility, on behalf of the faculty in the school, to assure that the university and school personnel review policies are applied fairly and equitably. The Committee has specific duties in relation to annual reviews, the promotion and tenure process, and periodic performance evaluations.

Membership

Faculty Personnel Review Committees are chaired by the dean of the school and must include at least five tenured faculty members from the School elected by the school faculty. Election will be by secret ballot, with plurality voting. The bylaws of the school may allow one additional member to be appointed by the Dean to assure balance. Service on the Personnel Review Committee should rotate among the tenured faculty on a staggered annual cycle with no member’s term to exceed two years. Only tenured faculty may serve on this committee, and recommendations regarding tenured Associate Professors and Professors may be made only by tenured Professors. A majority of the members should be of the rank of full professor.

Responsibilities

University review define three main processes for faculty review: 1. Annual reviews for all faculty, including non-tenure track faculty, 2. Peer review processes for tenure-track faculty for retention, promotion, and tenure, and 3. Periodic Performance Evaluation for tenured faculty. The specific responsibilities of the committee and the relevant policies in each case are:

1. Annual reviews.

The Committee does not conduct annual reviews of faculty and has no required duties in the process, but it since it must use the annual reviews in its two other required tasks, it should concern itself with the quality and evident fairness of the reports. If it finds problems, these should be reported to the school Dean and faculty. Faculty who consider their annual reviews to be inconsistent with university and school policy may address a request for corrections to the Personnel Review Committee. The Committee response should be provided to the Dean with a copy to the faculty member.
2. Retention, tenure, and promotion.

Each year in the fall term, the committee shall recommend to the Dean of the School those faculty members for whom ad hoc committees should be appointed for consideration for retention, tenure, and promotion. In order to formulate this advice, the Committee may review the faculty of the entire school by itself, or it may call for recommendations from departments or other subordinate units. School bylaws should describe the process. For this purpose, the Committee and any subordinate units involved in the process will have access to the faculty annual reviews for the current year and previous years. They may also request additional information. This annual review process will lead to one of three recommendations:

1. In the case of faculty in their first or second year of service, to not reappoint the faculty member.

2. To recommend that an ad hoc committee be composed for renewal of a non-tenured appointment (normally in the third year of service as an Assistant Professor) or for consideration for tenure or promotion as required under the General Standards and Procedures: Faculty Promotion, Reappointment, and Tenure (UTDPP1077).

3. To make no recommendation, thereby retaining the faculty member at their current rank.

These recommendations will be communicated by the Dean to the Provost according to the schedule.

A faculty member may request an ad hoc committee review for retention, tenure, or promotion even if the School’s initial decision is not to initiate such a review. Such requests will be submitted to the Dean of the School. The Dean will seek the advice of the Faculty Personnel Review Committee.


The committee also serves as the School Peer Review Committee as required by the Procedures Governing Periodic Performance Evaluation of Tenured Faculty (UTDPP1064), and the General Standards and Procedures for Review of Nontenure-System Faculty - UTDPP1062. Generally, the Committee is to review the preliminary evaluation prepared by the dean and provide its own written recommendation in response, which the dean is to take into account in preparing his final evaluation. Both the dean’s recommendation and that of the Committee will be forwarded to the Provost.
Recommendations regarding tenured Associate Professors may be made only by tenured Professors.

**Additional Responsibilities**

A Faculty Personnel Review Committee may be charged with additional responsibilities under other university policies or by school bylaws. The Dean may seek the Committee’s advice on additional personnel actions, including new hires.

*NOTE: If this approved, the current section on the Faculty Personnel Review Committee in General Standards and Procedures: Faculty Promotion, Reappointment, and Tenure should be replaced by the following:*

Recommendations for establishing *ad hoc* committees to consider faculty for retention, promotion, or tenure, will normally originate with dean of the school and the Faculty Personnel Review Committee, as described in the policy establishing Faculty Personnel Review Committees and as implemented in school bylaws.
Academic Program Review - UTDPP1013

Policy Charge

Academic Program Review PRC

Policy Statement

Academic units and programs are reviewed regularly to evaluate their quality and their effectiveness in supporting the university's mission. As described by this policy, the Program Review Committee, a standing committee composed of members of The University of Texas at Dallas faculty and academic administration, oversees the review process. The Committee functions in cooperation with the Executive Vice President and Provost (Provost), under whose auspices Academic Program Reviews are conducted.

Program Review Committee (PRC)

This university committee maintains general oversight of the review process to assure its efficacy and uniformity. During each program review, one member of the Program Review Committee, designated the Program Review Committee Monitor, participates directly in the process. The entire Program Review Committee evaluates the operation of the review process on a continuing basis and makes an annual report to the Provost and Academic Senate. In this report, it recommends any modifications of policies or procedures regarding reviews it considers advisable. In addition, it consults with and advises the Provost on other aspects of reviews as requested.

The membership of the Program Review Committee is comprised of six faculty members and four deans who are appointed by the President to two-year renewable terms. Members from the faculty are recommended by the Academic Senate after consultation with the Committee on Committees; deans are recommended by the Provost. Faculty should be drawn from the schools in which reviews will be conducted during the year of their service, or from the library if the library is to be reviewed.

The Responsible University Official is the Executive Vice President and Provost.

The term "Academic Program" or "unit" as used in this document may refer either to a degree-granting program, department, School, or to any academically coherent, distinctively functioning subdivision thereof.

Frequency of Review and Criteria for Selection
In accord with Texas Administrative Code, Title 19, Part 1, Chapter 5, Subchapter C, Section 5.52, Academic Programs ("units") shall be reviewed in intervals not to exceed seven years. Reviews may occur more frequently if the Provost, in consultation with the appropriate dean, finds that the circumstances of a particular program warrant an earlier date. However, a program may not need to be reviewed under the procedures of this policy if mandated external accreditation reviews occur regularly and substantially meet the criteria outlined under The Review Procedure below. According to Texas Administrative Code, Title 19, Part 1, Chapter 5, Subchapter C, Section 5.52 (c)(11) and (d)(11), institutions may submit reviews performed for programmatic licensure or accreditation in satisfaction of the state’s review and reporting requirements.

Master's programs classified with the same 6-digit Classification of Instructional Programs (CIP) as doctoral programs are reviewed simultaneously with their related doctoral programs. UT Dallas reviews bachelors programs in the same discipline as masters and doctoral programs simultaneously with those programs.

Selection of units to be reviewed in a given year will be made by the Provost after consultation with the Program Review Committee and the appropriate dean(s). The review schedule will be submitted to the Texas Higher Education Coordinating Board (THECB) staff. The factors (not in priority order) to be considered when creating the review schedule include:

1. Planned program changes;
2. Elapsed time since last major review of budget, staff and academic programs;
3. University or program accreditation cycles;
4. Significant changes in student demand; and
5. Overlap or shared responsibilities with other programs being reviewed.

The Review Team

The Program Review Committee oversees the evaluation conducted by a Review Team that is appointed and charged by the Provost. The Provost consults with the unit undergoing review and/or the Program Review Committee, as appropriate, regarding selection of Review Team members. The Review Team's composition may vary from program to program, but will incorporate both internal and external members. Typically, it will include:

1. At least two members from the UT Dallas faculty and academic administration who are not affiliated with the program to be reviewed, appointed by the Provost after soliciting recommendations from consultation with the Program Review Committee.
2. One member of the Program Review Committee, appointed by the Provost after consultation with the Program Review Committee, to act as the Program Review Committee Monitor. In addition to responsibilities as a regular member of the Review Team, the Program Review Committee Monitor will have the duty of conferring with and reporting to the Program Review Committee and, on the basis of knowledge acquired as a member of the Program Review Committee, of helping each Review Team ensure
The Provost may add additional members as appropriate. One member of the Review Team, usually a member not affiliated with UT Dallas, will be designated Chair of the Review Team by the Provost at the time the Team is constituted. The Review Team will evaluate the unit as requested by a written charge prepared by the Provost after consultation with the Program Review Committee.

The Review Procedure

Reviews will be conducted as follows:

The unit undergoing review will consult with the Provost regarding suitable dates for the Review Team's campus visit, and the detailed schedule of events during the visit. It will prepare a comprehensive self-study document (an internal planning document, not intended for general distribution) in accordance with guidelines and instructions issued by the Provost. These guidelines include criteria outlined in Texas Administrative Code, Title 19, Part 1, Chapter 5, Subchapter C, Section 5.52, Review of Existing Degree Programs. The Review Team also will collaborate with the Provost in ensuring that the Review Team's on-campus needs are met. The Provost will designate a Review Coordinator (the Dean, Head, Director, or suitable substitute) from the unit under review to ensure that the duties assigned to the unit in connection with the Review Team are carried out.

The Provost will provide the Review Team a detailed charge, along with the unit's self-study document. The Office of the Provost will issue the visit schedule, oversee the visit arrangements for the Review Team (transportation, housing, meals, reimbursement, etc.) and serve as liaison between the Review Team and the unit being reviewed.

Before the campus visit, the Review Team will familiarize itself with the unit's self-study, and with the Provost's charge. During the visit, it will consult with members of the unit's faculty, students, and staff and inspect facilities. It may request additional information beyond that provided in the self-study. Adequate time will be allowed in the latter part of the visit for the Review Team to deliberate in private and reach its conclusions.
At the beginning of the visit, the Review Team will have an introductory interview with the Provost. Before leaving the campus, the Review Team will hold two exit interviews. In the first, held with the Program Review Committee and the unit's faculty and administration, the Review Team will provide its preliminary assessment of the goals, plans, staffing, resources, existing and potential strengths, etc., of the unit, and those areas needing improvement. In the second, held with the Provost, the President and other appropriate senior administrators, the Review Team will summarize its immediate impressions and provide a forecast of its eventual written report. Then, within one month of the campus visit, the Chair of the Review Team will provide a complete written report on the Review Team's conclusions to the Provost.

Along with addressing any unique aspects of its charge, the Review Team's report will assess the unit's overall performance and its specific strengths and weaknesses and make recommendations for any changes the Review Team thinks are advisable. The evaluation should refer to the program's self-study and note items of agreement and disagreement between the Review Team's assessments and those of the self-study. The Review Team will share its final report with the faculty and administration of the unit. The unit's chief administrative office, in cooperation with faculty and staff, will provide a written response to the report to the Provost, giving specific actions planned in the light of the Review Team's recommendations. Where the unit disagrees with findings and/or recommendations of the Review Team, it will state its reasons for such disagreements. The unit's faculty will have access to this document as well as to the Review Team's report. The Provost will discuss the Review Team's report and unit's response with the unit's administration and faculty. Finally, the Provost will prepare recommendations to the President. The university administration will submit a report of the outcomes of each review, including the evaluation of the Review Team and actions the institution has taken or will take to improve the program, to the THECB no later than 90 days after the Review Team has submitted its findings to the institution.

In the years between reviews of the unit, this record of the Program Review will be pertinent to decisions on budget, staffing, curricular and degree changes, and allocation of special resources.

Policy History

- Editorial Amendments: February 2, 1998
- Editorial Amendments: September 1, 2000
- Revised: July 11, 2005
- Editorial Amendments: August 3, 2006
- Editorial Amendments: March 26, 2007
- Revised: June 1, 2012

Policy Links

- Permalink for this policy: http://policy.utdallas.edu/utdpp1013
- Link to PDF version: http://policy.utdallas.edu/pdf/utdpp1013
- Link to printable version: http://policy.utdallas.edu/print/utdpp1013
UT System Information Resources Use and Security Policy

Responsible Officer: Chief Information Security Officer
Sponsoring Office: Office of the Chief Information Security Officer
Effective Date: April 12, 2007
Last Reviewed: June 15, 2010
Errors or changes to: policyoffice@utsystem.edu

CONTENTS

Policy Statement

Rationale

Scope

Website Address For This Policy

Related Statutes, Policies, Requirements Or Standards

Contacts

Definitions

Responsibilities

Procedures

Special Requirements for Initial Implementation of Policy

Forms Tools/Online Processes

Appendix
POLICY STATEMENT

It is the policy of The University of Texas System (UT System) to:

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;

2. Appropriately reduce the collection, use or disclosure of social security numbers contained in any medium, including paper records;

3. Apply appropriate physical and technical safeguards without creating unjustified obstacles to the conduct of the business and Research of the UT System and the provision of services to its many constituencies in compliance with applicable state and federal laws.

RATIONALE

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 UT System must be available and protected commensurate with their value and must be administered in conformance with federal and state law and The University of Texas 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 UT System Information Resources; protect the privacy of personally identifiable information contained in the Data that constitutes part of its Information Resources; ensure compliance with applicable policies and state and federal laws regarding the management and security of Information Resources; and, educate individual Users with respect to the responsibilities associated with use of UT System Information Resources.

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

This Policy consolidates the following policies:

- UTS 165 Information Resources Use and Security Policy;
- UTS 166 Protecting the Confidentiality of Social Security Numbers; and
- UTS 167 Protecting the Confidentiality and Integrity of Digital Research Data

Most of the requirements in this policy were consolidated from three previous policies: UTS 165 (previously BPM 53) "Information Resources Use and Security Policy", UTS 167 (previously BPM 75) "Protecting the Confidentiality and Integrity of Digital Research Data", and UTS 166 (previously BPM 66)" Protecting the Confidentiality of Social Security Numbers. All of the requirements in this current policy apply to all UT 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 10 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.

SCOPE

All Entities

WEBSITE ADDRESS FOR THIS POLICY

http://www.utsystem.edu/policy/policies/uts165.html

RELATED STATUTES, POLICIES, REQUIREMENTS OR STANDARDS
## UT System Administration Policies & Standards

<table>
<thead>
<tr>
<th>Other Statutes, Policies &amp; Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Title 1 <em>Texas Administrative Code 202.2</em></td>
</tr>
<tr>
<td>• Texas Education Code § 65.31</td>
</tr>
<tr>
<td>• Federal Privacy Act of 1974 (Section 7 of Pub. L. 93-579 in Historical Note), 5th U.S. C. § 552a</td>
</tr>
<tr>
<td>• Social Security Act, 42 U. S. C. §§ 408(a)(8) and 405(c)(2)(C)(viii)(I)</td>
</tr>
<tr>
<td>• Family Educational Rights and Privacy Act, 20 U. S. C. § 1232g</td>
</tr>
<tr>
<td>• Texas Business and Commerce Code §35.58</td>
</tr>
<tr>
<td>• Texas Government Code § 559.003</td>
</tr>
</tbody>
</table>

## CONTACTS

If you have any questions about UT System Administration Policy UTS165 Information Resources Use and Security Policy, contact the following offices:

<table>
<thead>
<tr>
<th>Subject</th>
<th>Office Name</th>
<th>Telephone Number</th>
<th>Email/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Office of the Chief Information Security Officer</td>
<td>(512) 499-4249</td>
<td><a href="mailto:ciso@utsystem.edu">ciso@utsystem.edu</a></td>
</tr>
</tbody>
</table>
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.

Chief Administrative Officer: The highest ranking executive officer at each Entity. For most Entities, this is the President.

Computer Virus: A computer program that attaches itself to a file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive without the knowledge or permission of the User. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows Users to generate macros.

Confidential Data: Data that is exempt from disclosure under the provisions of the Public Records Act or other applicable state and federal laws.

Confidential University Data: Confidential Data maintained by an Entity of The University of Texas System.

Custodian: An individual or entity responsible for implementing Owner-defined controls and access to an Information Resource. Custodians include Information Security Administrators, Entity information technology/systems departments, vendors, and any third party acting as an agent of or otherwise on behalf of an Entity.

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 UT 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 or maintained made available in, electronic media.

**Electronic Communication**: Method used to convey a message or exchange information via Electronic Media instead of paper media. It includes the use of Electronic Mail, instant messaging, Short Message Service (SMS), facsimile transmission, and other paperless means of communication.

**Electronic Mail**: Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

**Electronic Media**: Any of the following: a) Electronic storage media including storage devices in computers (hard drives, memory) and any removable/transportable digital storage medium, such as magnetic tape or disk, optical disk, or digital memory card; or b) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, intranet, and the physical movement of removable/transportable electronic storage media.

**Email**: Abbreviation for Electronic Mail.

**Entity or Entities**: The nine academic teaching institutions and the six health science centers in The University of Texas System, UT System Administration, and UTIMCO.

**Information**: Data organized, formatted and presented in a way that facilitates decision making. All information is data.

**Information Resources (IR)**: Any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, 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 assistant (PDA), 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.

**Integrity:** The accuracy and completeness of information and assets and the authenticity of transactions.

**Internet:** A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

**Lead Researcher:** The person engaged in the conduct of Research with primary responsibility for stewardship of Research Data on behalf of an Entity.

**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 which 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 that is capable of receiving, transmitting, and/or storing electronic data and that is 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.

**Password:** A string of characters used to verify or "authenticate" a person's identity.

**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 (personal digital assistants), pagers, cell phones, Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs and similar storage devices.

**Research:** Systematic investigation designed to develop and contribute to knowledge and may include all stages of development, testing and evaluation.

**Researcher:** Lead Researchers, faculty, staff, graduate students, postdoctoral fellows, residents and visiting/affiliated scientists who are engaged in or responsible for Research activities.

**Scheduled Change:** Formal notification received, reviewed, and approved through the review process in advance of a change being made.

**Security Incident:** An event which results in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate.

**Sensitive Data:** 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 TAC 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, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, Biodefense, Homeland Security, DOD etc.)

**Server:** A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

**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. 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 UT System’s investment assets.

**UT 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 UT System who exchanges goods or services for money or other consideration.

**Worm:** A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network, using otherwise-unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system Owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.
RESPONSIBILITIES

Chancellor

- Budgets sufficient resources to fund ongoing and continuous information security remediation, implementation and compliance activities that reduce compliance risk to an acceptably low level.
- Ensures that appropriate corrective and disciplinary action is taken in the event of non-compliance.

Chief Administrative Officer

- Ensures the Entity’s compliance with this Policy.
- Budgets 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.
- Approves the Entity Information Security Program, or designate someone to provide this approval in accordance with 1 TAC 202.71(a).
- Ensures that appropriate corrective and disciplinary action is taken in the event of non-compliance.
- Designates an individual other than the Information Resources Manager to serve as the Information Security Officer (ISO) who shall serve in the capacity as required by 1 TAC 202.71(d) and with authority for that entire Entity.

Chief Information Security Officer (for UT System)

- Provides leadership, strategic direction, and coordination for the UT System-wide information security initiative including issuing security practice bulletins relating to standards and best practices.
- Establishes the UT System CISO Council and holds meetings at least quarterly.
- Develops and provides oversight for a UT System-wide Information Security Compliance Program.
- Provides guidance on the Entity Information Security Program including organizational duties and responsibilities, covered activities, authority to act, terminology definitions, standard methodologies, and minimum standards.
- Defines the risk management process to be used for all information security risk management activities.
- Explores and recommends the acquisition of tools and resources that can be utilized UT System–wide and how expertise can be shared among Entities.
- Establishes reporting guidance, metrics, and timelines and monitors effectiveness of security strategies at each Entity.
• Apprises the Chancellor and the Board of Regents quarterly on the status and effectiveness of the Information Security Compliance Programs and activities at each Entity.

**Custodian of Mission Critical Information Resources**

• Implements approved mitigation strategies and adhere to information security policies and procedures to manage risk levels for information resources under their care.

• Implements monitoring techniques and procedures for detecting, reporting, and investigating incidents.

**Department Head and/or Lead Researcher**

• Comply 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.

**Entity**

• Designates responsibility for the information security function by documenting key roles and responsibilities.

• Adopts change management processes to ensure secure, reliable, and stable operations to which all offices that support Information Resources are required to adhere.

• Performs annual risk assessments that identify Mission Critical Information Resources in the central and all decentralized areas.

• Develops Digital Data classification guidelines for Digital Data maintained in both central and decentralized areas.

• Develops a plan for identifying Digital Data that is Sensitive.

• Manages and protects the confidentiality and integrity of Sensitive Digital Data.

• Controls and monitors access to its Sensitive Digital Data based on data sensitivity and risk.

• Discontinues use of social security number as an individual’s primary identification number.

• Uses and collects social security numbers only as reasonably necessary for the proper administration or accomplishment of the Entity's business, governmental, educational and medical purposes.

• Assigns a unique identifier for each applicant, student, employee, insured dependent, research subject, patient, alumnus, donor, contractor, and other individuals who become associated with the Entity at the earliest possible point of contact with the Entity.
• Provides the notice required by Section 7 of the Federal Privacy Act of 1974 and by Section 559.003 of the Texas Government Code each time it requests that an individual initially disclose his or her social security number.

• Limits and monitors access to records containing social security numbers to those employees who need to see the number for the performance of the employees' job responsibilities.

• Follows procedures to report incidents involving computer security, as required by state or federal law.

• Reports significant information security incidents, as defined by the UT System Security Incident Reporting Guidelines, to the UT System CISO.

• Discloses in accordance with applicable federal and state law, incidents involving computer security that compromises the security, confidentiality, or integrity of Personal Identifying Information it maintains to any resident of Texas and Data Owners whose Personal Identifying Information was, or is reasonably believed to have been, acquired without authorization.

• Adheres to policies, standards and/or procedures governing the secure transmission of Confidential University Data via public networks.

• Provides computer security awareness training.

• Ensures that the protection of Information Resources (including data confidentiality, integrity, and accessibility) is considered during the development or purchase of new computer applications.

• Ensures that information technology contracts address security, backup and privacy requirements, and include right-to-audit or other provisions to provide appropriate assurances that applications and Data will be adequately protected.

• Monitors Information Resources in accordance with TAC 202.75 (7) (P).

Entity Offices with Designated Responsibility For Network and/or Application Account Creation

• Manages accounts in accordance with the Entity’s information security policies, standards, and/or procedures.

• Approves all access methods, installation of all network hardware connected to the local-area network and methods and requirements for attachment of any non UT System owned computer systems or devices to the UT System network.

Entity Office Charged With Supporting Information Resources

• Formalizes best practice change management processes into practice standards.

• Requires compliance from all individuals who manage Information Systems or applications.

• Provides support, guidance and problem resolution to department heads and Lead Researchers with respect to this Policy and applicable policies and procedures.
Information Security Administrator

- Implements and complies with all information technology policies and procedures relating to assigned systems.
- Assists Owners in performing annual information security risk assessment for Mission Critical Resources.
- Reports general computing and Security Incidents to the Entity ISO.
- Assists, as member of the ISA Work Group, the ISO in developing, implementing, and monitoring the Information Security Program.
- Establishes reporting guidance, metrics, and timelines for ISOs to monitor effectiveness of security strategies implemented in both the central and decentralized areas.
- Reports at least annually to the ISO about the status and effectiveness of information resources security controls.

Information Security Officer (at each Entity)

- Provides information security for all Information Systems and computer equipment maintained in both central and decentralized areas.
- Develops a full-scale Entity Information Security Program.
- Documents an information security risk assessment annually that identifies Mission Critical Information Resources in the central and all decentralized areas.
- Ensures an annual information security risk assessment is performed by each Owner of Mission Critical Information Resources.
- Requires each Owner of Mission Critical Information Resources to designate an Information Security Administrator (ISA).
- Establishes an Entity Information Security Working Group composed of ISAs and holds meetings at least quarterly.
- Documents and maintains up to date an Entity Information Security Program.
- Establishes reporting guidance, metrics, and timelines and monitors effectiveness of security strategies in both central and decentralized operations.
- Specifies and requires use of appropriate security software such as anti-virus, 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 by the ISO to provide appropriate information security across the whole of the Entity.
- Ensures that high-level information security awareness training is included in first-time Compliance Training and in every subsequent update for all employees.
- Ensures that ISAs and Data Owners are properly trained on information security requirements.
• Communicates instances of non-compliance to appropriate administrative officers for corrective, restorative and/or disciplinary action.

• Participates in the UT System CISO Council meetings.

• Reports quarterly to the UT System CISO the current status of the information security risk assessment and Information Security Program, including any significant incidents, situations of non-compliance, barriers to program execution, and planned remedies for the whole Entity.

• Reports, at least annually, to the Chief Administrative Officer or his or her designated representative(s) and copies to the Entity’s Chief Information Officer and Compliance Officer, and the System-wide Chief Information Security Officer on the status and effectiveness of information resources security controls for the whole Entity.

• Reviews the data security requirements and specifications of any new computer applications or services that receive, maintain, and/or share Confidential Data.

• Approves the security requirements of the purchase of required information technology hardware, software, and systems development services.

• Approves and documents any exceptions to information security practices within the Entity.

Institutional Compliance and Internal Audit

• Provide high-level monitoring of the Information Security Program through inspections and verifications of reported information and periodic audits respectively.

Owner

• Grants access to the Information System under his/her responsibility.

• Classifies Digital Data based on Data sensitivity and risk.

• Backs up Data under his/her responsibility in accordance with risk management decisions and secures back up media.

Owner of Mission Critical Information Resources

• Designates an individual to serve as an Information Security Administrator (ISA) to implement information security policies and procedures and for reporting incidents to the ISO.

• Performs an annual information security risk assessment and identifies, recommends, and documents acceptable risk levels for information resources under his/her authority.

User Accessing UT System Information Resources
• Complies with this Policy.
• Formally acknowledges and abides by the Entity’s acceptable use policies.
• Does not share passwords or similar information or devices used for identification and authorization purposes.
• Adheres to prudent and responsible Internet use practices as outlined in the Entity’s policies associated with Information Resources acceptable use.

Vendor
• Adheres to all state and federal laws and Regents’ Rules and Regulations pertaining to the protection of Information Resources and privacy of Sensitive Data.
• Complies with all applicable UT System rules associated with this Policy, practice standards and agreements, and adheres to federal and state laws to which UT System must adhere.
• Represents, warrants, and certifies it will hold all UT System Sensitive Data in the strictest confidence.

PROCEDURES

1. Information Resources Security Responsibility and Accountability

1.1 All Entities must designate responsibility for the information security function by documenting key roles and responsibilities.

1.2 The Chancellor shall be responsible for the following:
   1.2.1 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
   1.2.2 Ensure that appropriate corrective and disciplinary action is taken in the event of non-compliance.

1.3 The Chief Administrative Officers at each Entity shall be responsible for the following:
   1.3.1 The Entity’s compliance with this Policy;
   1.3.2 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;
1.3.3 Approve the Entity Information Security Program, or designate someone to provide this approval in accordance with 1 TAC 202.71(a); and

1.3.4 Ensure that appropriate corrective and disciplinary action is taken in the event of non-compliance.

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

1.4.1 Provide leadership, strategic direction, and coordination for the UT System-wide information security program including issuing security practice bulletins relating to standards and best practices;

1.4.2 Establish the UT System CISO Council and hold meetings at least quarterly;

1.4.3 Develop and provide oversight for a UT System-wide Information Security Compliance Program. This program shall include UT System-wide and Entity action plans, training plans, and monitoring plans;

1.4.4 Provide guidance on the Entity Information Security Program including organizational duties and responsibilities, covered activities, authority to act, terminology definitions, standard methodologies, and minimum standards;

1.4.5 Define the risk management process to be used for all information security risk management activities;

1.4.6 Explore and recommend the acquisition of tools and resources that can be utilized UT System–wide and how expertise can be shared among Entities;

1.4.7 Establish reporting guidance, metrics, and timelines and monitor effectiveness of security strategies at each Entity; and

1.4.8 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.

1.5 The highest ranking administrator at each Entity charged with oversight of information technology at that Entity shall serve in the functional role of Information Resources Manager (IRM) as defined by 1 TAC 211.20 and will have authority for the entire Entity.

1.6 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 TAC 202.71(d) and with authority for that entire Entity. The responsibilities of the ISO shall include the following:
1.6.1 Provide information security for all Information Systems and computer equipment maintained in both central and decentralized areas;

1.6.2 Develop a full-scale Entity Information Security Program. This program shall include Entity action plans, training plans, and monitoring plans.

1.6.3 Document an information security risk assessment annually in accordance with 1 TAC 202.72 that identifies Mission Critical Information Resources in the central and all decentralized areas;

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

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

1.6.6 Establish an Entity Information Security Working Group composed of ISAs and hold meetings at least quarterly;

1.6.7 Document and maintain up to date an 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;

1.6.8 Establish reporting guidance, metrics, and timelines and monitor effectiveness of security strategies implemented in both central and decentralized areas;

1.6.9 Specify and require use of appropriate security software such as anti-virus, 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

1.6.10 Ensure that high-level information security awareness training is included in first-time Compliance Training and in every subsequent update for all employees;

1.6.11 Ensure that ISAs and Data Owners are properly trained on information security requirements;

1.6.12 Communicate instances of non-compliance to appropriate administrative officers for corrective, restorative and/or disciplinary action;

1.6.13 Participate in the UT System CISO Council meetings;
1.6.14 Report quarterly to the UT System CISO the current status of the information security risk assessment and Information Security Program including any significant incidents, situations of non-compliance, 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

1.6.15 Report, at least annually, to the Chief Administrative Officer or his or her designated representative(s) and copied to the Entity’s Chief Information Officer and Compliance Officer, and the System-wide Chief Information Security Officer on the status and effectiveness of information resources security controls for the whole Entity.

1.7 Owners of Mission Critical Information Resources at each Entity shall designate an individual to serve as an Information Security Administrator (ISA) to implement information security policies and procedures and for reporting incidents to the ISO. The responsibilities of the ISA shall include the following:

1.7.1 Implement and comply with all information technology policies and procedures relating to assigned systems;

1.7.2 Assists Owners in performing annual information security risk assessment for Mission Critical Resources.

1.7.3 Report general computing and Security Incidents to the Entity ISO;

1.7.4 Assist, as member of the ISA Work Group, the ISO in developing, implementing, and monitoring the Information Security Program;

1.7.5 Establish reporting guidance, metrics, and timelines for ISOs to monitor effectiveness of security strategies implemented in both the central and decentralized areas; and

1.7.6 Report at least annually to the ISO about the status and effectiveness of information resources security controls.

1.8 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.

1.9 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.
1.10 All Users must comply with this Policy. Users who fail to comply are subject to disciplinary action in accordance with Section 28.

2. **Information Resources Acceptable Use**

2.1 All Entities shall have an acceptable use policy. All individuals accessing UT System Information Resources must formally acknowledge and abide by the acceptable use policy. Formal acknowledgment of the Acceptable Use Policy by all individuals accessing UT System Information Resources serves as a compliance and enforcement tool.

2.2 Users are responsible for exercising good judgment regarding the reasonableness of personal use in accordance with all policies associated with Information Resources acceptable use.

2.3 As a convenience to the UT System User community, limited incidental personal use of Information Resources is permitted.

2.4 Incidental use of Information Resources must not result in direct cost to the UT System or expose UT System to unnecessary risks.

3. **Account Management**

The UT System recognizes that proper management and use of computer accounts are basic requirements for protecting UT 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 UT 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:

- 3.1 Creating uniquely identifiable accounts for all Users. This includes accounts created for use by outside vendors (see Section 26);

- 3.2 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

- 3.3 Expiring or disabling passwords at least annually or more often if warranted by risk.

4. **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:

4.1 Acceptable use of administrative/special access accounts and intended administrative purposes;

4.2 Authorizing use of administrative/special access accounts;

4.3 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

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

5. Backup Recovery of Network Servers and Data

5.1 All UT System Data, including Data associated with research, must be backed up in accordance with risk management decisions implemented by the Data Owner (See Section 9.)

5.2 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:

5.2.1 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;

5.2.2 Assigning operational responsibility for backup of all servers connected to the applicable network;

5.2.3 Scheduling Data backups and establishing requirements for off site storage;

5.2.4 Securing onsite / offsite storage and media in transit; and

5.2.5 Testing backup and recovery procedures.

6. 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:

6.1 Formally identifying, classifying, prioritizing and requesting changes;

6.2 Identifying and deploying emergency changes;
6.3 Assessing potential impacts of changes;
6.4 Authorizing changes and exceptions;
6.5 Testing changes;
6.6 Change implementation and back-out planning; and
6.7 Documenting and tracking changes.

7. **Computer Virus Prevention**

UT 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 UT System owned and personal computers that connect to the UT System network must run all required protection software and adhere to any other protective measures as required by applicable policies and procedures.

8. **Classification of Digital Data**

8.1 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.

8.2 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 UT System Office of General Counsel.

9. **Risk Management**

9.1 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.

9.2 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.

9.3 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.
9.4 The confidentiality and integrity of Sensitive Digital Data must be managed as required by this Policy.

9.5 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.

10. Reduction of Use and Collection of Social Security Numbers

UT System recognizes the special risks associated with the collection, use and disclosure of social security numbers. Accordingly, the requirements of this Section 10 apply to social security numbers contained in any medium, including paper records that are collected, maintained, used or disclosed by any Entity except UTIMCO.

10.1 All Entities shall reduce the use and collection of social security numbers.

   10.1.1 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.

   10.1.2 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 their respective business, governmental, educational and medical purposes, including, but not limited to:

       10.1.2.1 As means of identifying an individual for whom a unique identification number is not known;

       10.1.2.2 For internal verification or administrative purposes; and

       10.1.2.3 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 11 of this Policy.

   10.1.3 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 Information Security Officer who will consult with the Office of General Counsel with respect to the interpretation of law.

10.1.4 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.

10.1.5 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.

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

- 10.1.6.1 Be a component of a system that provides a mechanism for the public identification of individuals;

- 10.1.6.2 Be permanent and unique within the Entity as applicable and remain the property of, and subject to the rules of, that Entity; and

- 10.1.6.3 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.

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

10.2 All Entities shall inform individuals when they collect social security numbers

10.2.1 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.

- 10.2.1.1 The notice shall use the applicable text from Appendix 4 of this Policy or such other text as may be approved by the Information Security Officer who will consult with the Office of General Counsel with respect to the interpretation of law.

- 10.2.1.2 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.
10.2.1.3 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.

10.2.2 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 Government Code, the individual is entitled to receive and review the information; and under Section 559.004 of the Government Code, the individual is entitled to have the incorrect information about the individual corrected.

10.3 Employees may not seek out or use social security numbers relating to others for their own interest or advantage.

10.4 All Entities shall reduce the public display of social security numbers.

10.4.1 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.

10.4.2 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.

10.4.3 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.

10.4.4 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).

10.4.5 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.
10.5 All Information Systems acquired or developed must comply with the following:

10.5.1 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;

10.5.2 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;

10.5.3 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

10.5.4 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.

11. Management of Sensitive Digital Data

11.1 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 UT System’s computing devices.

11.2 All Entities shall control and monitor access to its Sensitive Digital Data based on Data sensitivity and risk (as determined in accordance with Section 9 of this Policy) and by the use of appropriate physical and technical safeguards.

11.2.1 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.

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

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

11.2.3 Employees may not disclose Sensitive Digital Data to unauthorized persons or entities except:

- As required or permitted by law;
- With the consent of the individual;
- Where the third party is the agent or contractor for the Entity and the safeguards described in Section 11.2.4 are in place to prevent unauthorized distribution; or
As approved by the Office of General Counsel.

11.2.4 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 which 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.

11.3 All Entities shall implement security safeguards to protect its 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.

11.3.1 Sensitive Digital Data shall be secured in accordance with each Entity’s security plan and with this Policy.

11.3.2 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.)

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

11.3.3.1 It is secured against unauthorized access in accordance with this Policy;

11.3.3.2 It will not compromise business or Research efforts or privacy interests if lost or destroyed; and

11.3.3.3 The Entity has specific procedures in place that address this subsection.

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

11.4.1 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
11.4.2 In accordance with the applicable Entity’s records retention schedule.

11.5 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.

12. 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.

13. Incident Management

13.1 Incidents involving computer security will be reported as required by state or federal Law.

13.2 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.

13.3 All Entities shall require employees to report promptly unauthorized or inappropriate disclosure of Sensitive Digital Data, including social security numbers; to their supervisors, Information Security Officer, and/or Entity’s compliance hotline.

13.4 Custodians of Mission Critical Information Resources shall implement monitoring techniques and procedures for detecting, reporting, and investigating incidents.

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

13.6 All Entities shall disclose in accordance with applicable federal and state law, incidents involving computer security that compromises the security, confidentiality, or integrity of Personal Identifying Information it maintains to any resident of Texas and Data Owners whose Personal Identifying Information was, or is reasonably believed to have been, acquired without authorization.

13.6.1 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.

13.7 Entities’ Incident Management Procedures must incorporate procedures for the following:
   13.7.1Formally identifying, reporting, and classifying incidents;
   13.7.2 Responding to incidents;
   13.7.3 Assessing potential damage of incidents;
   13.7.4 Gathering and preserving physical and electronic evidence;
   13.7.5 Assigning responsibility for gathering, maintaining, and reporting detailed information regarding incidents of local and UT System-wide significance; actions taken to remediate; and documentation of a management action plan to prevent a recurrence in accordance with Section 1 of this Policy;
   13.7.6 Notifying appropriate System Administration officials, residents of Texas, Data Owners, and consumer reporting agencies as required by applicable state and federal law and UT System policy;
   13.7.7 Determining the timing requirements for incident disclosure and notification; and
   13.7.8 Determining the appropriate medium to provide notice based on incident significance and number of individuals adversely impacted.

14. Internet Use

14.1 The UT System recognizes that there are risks associated with the posting or consuming of information on the Internet. To mitigate these risks, UT 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.

14.2 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 the following:
   14.2.1 Encrypting all Confidential University Data or any specific Data identified as confidential by federal and state law transmitted over the Internet.

15. 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 UT 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 UT System.

16. Network Access

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

16.2 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 UT System owned computer systems or devices to the UT 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.

17. 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.

18. Passwords

18.1 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 UT System Identity Management Federation Member Operating Practices (MOP) and applicable policies, standards, and/or procedures governing password management. The Entity’s policies, standards and/or procedures must incorporate procedures for the following:

18.1.1 Vetting User identity when issuing or resetting a password;

18.1.2 Establishing password strength;

18.1.3 Changing passwords;

18.1.4 Managing security tokens when applicable; and

18.1.5 Securing unattended computing devices from unauthorized access.
18.2 Users shall not share passwords or similar information or devices used for identification and authorization purposes.

19. Physical Access

19.1 All Information Resources must be physically protected, based on risk, as determined in accordance with Section 9 of this Policy, and associated risk management decisions as part of the overall security program for the UT System.

19.2 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:
   19.2.1 Protecting facilities in proportion to the criticality or importance of their function and the confidentiality of any impacted Information Resources affected;
   19.2.2 Managing access cards, badges and/or keys;
   19.2.3 Changing and/or removing physical access to facilities to reflect changes on User role or employment status; and
   19.2.4 Providing access to facilities to Visitors and Vendors.

20. Portable Computing and Remote Access

20.1 To preserve the integrity, availability, and confidentiality of UT System information, Users accessing the Entity’s infrastructure remotely must do so in accordance with Section 3 and all policies on Information Resource acceptable use.

20.2 All Entities must develop policies, standards and/or procedures governing remote access and wireless connectivity.

21. Security Monitoring

In accordance with Section 1 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 Information Security Officer.

22. Security Training

22.1 All Entities shall deliver security awareness General Compliance training in accordance with the following schedule, or more frequently as determined by that Entity:
22.1.1 Training of all Users with access to the Entity’s Information Resources shall take place at least yearly; and

22.1.2 To each new, temporary, contract, assigned, or engaged employee or worker 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.

22.2 All Entities shall provide appropriate technical training to employees providing information technology help-desk or technical support as determined by that Entity.

23. **Server and Network Device Hardening Standards**

To protect against malicious attack, all Servers on UT System networks will be security hardened based on risk analysis and must be administered according to policies, standards procedures prescribed by the Entity, as applicable, and must incorporate procedures for the following:

23.1 Managing the testing and installation of security patches; and

23.2 Setting baseline security “hardened” configuration standards for all network device types (examples: routers, laptops, desktops, and PDA’s.)

24. **Software Licensing**

All software installed on UT 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 UT System.

25. **System Development and Deployment**

25.1 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 minimum, incorporate procedures for the following:

25.1.1 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

25.1.2 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 Information Resources Manager.

25.2 The Entity ISO must review the data security requirements and specifications of any new computer applications or services that receive, maintain, and/or share Confidential Data.
25.3 The Entity ISO must approve the security requirements of the purchase of required information technology hardware, software, and systems development services for any new computer applications that receive, maintain, and/or share Confidential Data.

25.4 Information technology 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 UT System policies pertaining to the protection of Information Resources and privacy of Sensitive Data.

26. Vendor Access

The UT 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.

26.1 Vendors contracts must require that vendors comply with all applicable UT System rules associated with this policy, practice standards and agreements, and address all federal and state laws to which UT System must adhere to ensure that UT System remains in compliance with such law.

26.2 All Entities shall control Vendor access to its Sensitive Data based on data sensitivity and risk (as determined in accordance with Section 9 of this Policy) and by the use of appropriate measures. Such measures must incorporate the following:

26.2.1 Vendor shall represent, warrant and certify it will:

26.2.1.1 Hold all Sensitive Data in the strictest confidence;

26.2.1.2 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 FERPA;

26.2.1.3 Not otherwise use or disclose Sensitive Data except as required or permitted by law;

26.2.1.4 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);

26.2.1.5 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

26.2.1.6 Comply with the Vendor Access Requirements that are set forth in this section.
26.2.2 To the extent that the Sensitive Data includes Protected Heath Information ("PHI") as defined in 45 CFR § 164.501, if required by an Entity, Vendor shall execute a HIPAA Business Associate agreement in the form required by UT System.

26.2.3 Entities shall require the following from the Vendor:

26.2.3.1 If an unauthorized use or disclosure of any Sensitive Data occurs, the Vendor must provide:
   26.2.3.1.1 Written notice within one (1) business day after Vendor’s discovery of such use or disclosure and
   26.2.3.1.2 All information UT System requests concerning such unauthorized use or disclosure.

26.2.3.2 Within 30 days after the termination or expiration of a Purchase Order, Contract or Agreement for any reason, Vendor shall either:
   26.2.3.2.1 Return or destroy, as applicable, all Sensitive Data provided to the Vendor by Entity to Vendor, including all Sensitive Data provided to Vendor’s employees, subcontractors, agents, or other affiliated persons or entities; or
   26.2.3.2.2 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.

27. Right to Monitor

Entities have the authority and responsibility to monitor Information Resources in accordance with TAC 202.75 (7) (P):

27.1 To ensure compliance with this policy and state laws and regulations related to the use and security of Information Resources; and
27.2 To ensure that information resources security controls are in place, are effective, and are not being bypassed.

28. Disciplinary Actions

Violation of this policy may result in disciplinary action for faculty, staff and students in accordance to 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.
SPECIAL REQUIREMENTS FOR INITIAL IMPLEMENTATION OF POLICY

This Policy is based on public policy and privacy issues and not on convenience or past practices. Nevertheless, the UT System recognizes the financial burdens and the potentially disruptive nature of securing, reprogramming and immediate conversions of business, research, and information systems.

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 the conduct the business of the UT System and the provision of services to its many constituencies or negatively affect UT System's commitment to engage in high-quality, innovative Research that entails the discovery, retention, dissemination, and application of knowledge in compliance with UT System policy and state and federal laws and regulations.

FORMS AND TOOLS/ONLINE PROCESSES

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

APPENDIX

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: Pre-approved Text for Notice Required by the Federal Privacy Act of 1974

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

Bulletin #2 Corresponding Documents

- UT System Information Security Program Elements
- UT System Information Security Program Metrics Reported to UT System
- Institutional Information Security Program Quarterly Status Report Template

Keywords: acceptable use, security, information technology, internet, email, social security numbers, confidentiality, data, research, computers, computer, technology, internet, IT, information technology (IT), social security number, web, password, passwords, compliance, internet usage
Institutional Animal Care and Use Committee - UTDPP1014

Policy Charge

Animal Care and Use

Policy Statement

The Institutional Animal Care and Use Committee is a University-wide Standing Committee appointed by the President not reporting to the Academic Senate of The University of Texas at Dallas.

The Committee operates under the Principles for Use of Animals, the U.S. Department of Health and Human Services "Guide for the Care and Use of Laboratory Animals," the U.S. Department of Agriculture Animal and Plant Inspection Service, the Animal Welfare Acts, and other applicable laws and regulations. The Committee is charged to maintain oversight of the University's animal care program, annually advise the University on policies and procedures with regard to its animal care program and assure the humane care and use of animals used or intended for use in all research, research training, experimentation, teaching, or biological testing or for related purposes involving live, vertebrate animals. In keeping with this charge, no research or other activities involving the use of animals may commence without the written approval of the Committee. The Committee is also charged to assure the humane care and use of animals used in projects awarded to the University by the National Institute of Health (NIH). In addition, the committee is charged to perform the following duties:

1. Inspect University facilities and review procedures for the care and use of animals at least twice each year to ensure that the University is in compliance with the Animal Welfare Act, the NIH "Guide for the Care and Use of Laboratory Animals," and U.S. Department of Agriculture Animal and Plant Inspection Service.
2. Receive and review questions or complaints from any source concerning the welfare of University animal subjects. If the conduct of a specific project is to be reviewed, the quorum will not include any member having an active role in the project.
3. Semi-annually make written recommendations to the Vice President for Research regarding any aspect of the University's animal program.
4. Review and approve, require modification in (to secure approval), withhold approval of, or suspend any research or activity, new or ongoing, including but not limited to proposals submitted to funding agencies, that involves the use of animals.
5. Notify investigators, University and appropriate funding agencies, through the Vice President for Research, of its decision to approve or withhold approval or suspend any research or instructional activity, new or ongoing, that involves the use of animals.

Members of the Institutional Animal Care and Use Committee must have appropriate education and experience to perform their duties with respect to the types of animals and species used and the kinds of projects to be undertaken. One member of the Committee must be a Doctor of Veterinary Medicine,
with training in laboratory animal science and medicine. One member of the Committee must be a
community person, not affiliated with the University in any way other than as a member of the
Committee, and not a member of the immediate family of a person who is affiliated with the University.
One member of the Committee must be a person whose primary concerns are in a nonscientific area.
One member of the Committee must be a practicing scientist experienced in research involving animals.
Any individual who meets the requirements of more than one of the categories listed above may fulfill
more than one requirement.

The Committee shall be composed of no fewer than six members appointed by the President. The terms
of office of the Committee members shall be for three years and members may be reappointed by the
President for additional terms. If for any reason a Committee member resigns, the President shall
appoint another qualified individual to serve the remainder of the unexpired term. The Vice President for
Research and the University Chief of Police serve as ex officio members with vote. Changes in
membership will be reported annually to the Office of Protection from Research Risks, NIH. The Chair
and Vice Chair of the Committee shall be appointed annually by the President.

The Vice President for Research shall be the Responsible University Official for the Committee, with
oversight of all animal facilities. All information concerning Committee activities, reports, and other
related documents and approvals shall be housed in the Office of the Vice President for Research. The
Vice President for Research shall be responsible for the submission of annual reports to appropriate
government agencies.

Policy History

- Issued: August 1, 1979
- Revised: September 1, 1981
- Revised: September 1, 1983
- Revised: May 3, 1991
- Revised: June 1, 1994
- Editorial Amendments: February 2, 1998
- Editorial Amendments: September 1, 2000
- Revised: June 24, 2002
- Editorial Amendments: April 10, 2006
- Editorial Amendments: January 11, 2007
- Revised: June 4, 2009
- Revised: August 17, 2011

Policy Links

- Permalink for this policy: http://policy.utdallas.edu/utdpp1014
- Link to PDF version: http://policy.utdallas.edu/pdf/utdpp1014
- Link to printable version: http://policy.utdallas.edu/print/utdpp1014
Date: August 21, 2013

To: Murray Leaf, Ph.D.
   Speaker, Faculty Senate

From: Margaret Tresch Owen, Ph.D.
   Chair, Academic Program Review Committee

Re: Annual Report, Academic Program Review Committee
   2012-2013

In the 2012-2013 academic year, participating members of the Academic Program Review Committee were Dean Bert Moore and Drs. Mark Lee, Xinchou Lou, Margaret Owen (chair), and Ross Roesser. Members of the committee served on internal review teams for three academic program reviews held this past year. Additional members serving on the internal review teams were Dean Denis Dean and Drs. Carlos Aiken, Alexander Braun, John Ferraris, Elena Katok, Robert Lowry, Alice O'Toole, Marion Underwood, and Anvar Zakhidov. Outside review committee members and additional details on each of the reviews conducted are shown in the attached Table.

The programs reviewed in 2012-13 are listed below.

<table>
<thead>
<tr>
<th>Geosciences:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Policy and Political Economy</td>
<td>PhD</td>
</tr>
<tr>
<td>International Political Economy</td>
<td>Masters</td>
</tr>
<tr>
<td>Public Policy</td>
<td>Masters</td>
</tr>
<tr>
<td>Geospatial Information Systems</td>
<td>PhD &amp; Masters</td>
</tr>
<tr>
<td>Materials Science &amp; Engineering</td>
<td>PhD &amp; Masters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Arts &amp; Humanities:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>History Desk Review</td>
<td>Masters</td>
</tr>
<tr>
<td>Aesthetic Studies</td>
<td>PhD &amp; Masters</td>
</tr>
<tr>
<td>History of Ideas</td>
<td>PhD &amp; Masters</td>
</tr>
<tr>
<td>Studies in Literature</td>
<td>PhD &amp; Masters</td>
</tr>
<tr>
<td>Humanities</td>
<td>PhD &amp; Masters</td>
</tr>
</tbody>
</table>

Reports for each Program Review were submitted to the Provost and final meetings with the Provost were held. Copies of each Program Review Report were forwarded to the Office of Academic Affairs of the University of Texas System and to the Coordinating Board.
Date: August 26, 2013
To: The Academic Senate
From: Peter K. J. Park, out-going Chair
    Committee for the Support of Diversity and Equity
Re: Annual Report of the Committee for the Support of Diversity and Equity, 2012-2013

I. Membership:

The members of the Committee for the Support of Diversity and Equity were: the Chair Peter Park (AH), the Vice Chair Yang Liu (ECS), Cindy De Frias (BBS), Sherry Li (EPPS), Mandy Maguire (BBS), Alex Piquero (EPPS), Karen Prager (IS), Monica Rankin (AH), Orlando Richard (JSOM), Li Zhang (NSM), Abby Kratz (admin), Sherry Marek (admin), Eloise Square (admin), Yolandé Evans (staff), Lisabeth Lassiter (staff), Danny Cordova (staff)

II. The Report:

There was a near crippling problem for this Committee at the beginning of school year. We did not know the names of the three or so members from staff who were supposed to be appointed to this Committee until far into the semester. I was not able to convene the first meeting of this committee until about 8 weeks into the fall semester. It was discovered that the problem was a failure of the normal means of communication. No one was able to reach the president of Staff Council via email because her email program had gone bezirk. I would advise that, toward the beginning of the next academic year, somebody (either the administrative assistant, the Senate speaker, or the new chair of the Diversity and Equity Committee) telephone Rochelle Pena or seek her out in person, to get the names of the staff appointees. We did not have many meetings during 2012-2013; we met on Nov. 8, Jan. 24, and March 1. Not all members were able to attend all meetings because of schedule conflicts, but this is as usual.

Regarding the Faculty Diversity Council Liaisons, recall that it was created a year ago with input from the Committee for the Support of Diversity and Equity. This Council has been conducting its business in coordination with the Associate Provost for Faculty Development, Emily Tobey, and has had two meetings during 2012-2013. It operates independently of the Committee for the Support of Diversity and Equity. The latter received reports from Emily Tobey on her work in the area of faculty development, including her work with the Faculty Diversity Council.

There were no specially urgent issues that this Committee took up. In the Chair’s view, it was the usual. Many of the university’s concerns and priorities for staff and faculty development have been taken up by whole departments and officials created in recent years to support or professionally develop our staff and faculty. There was a lively discussion earlier in the year of the on-going effort to create an on-site child-care facility. The results of this discussion were disseminated to the officials who have been all along working on this project, including President Daniel. In the next year, the Committee for the Support of Diversity and Equity should ask for an update from the Subcommittee on Childcare.
Abby Kratz (former Chair) and I would like to pose this question: Is it possible to add student members (maybe two) to the Committee for the Support of Diversity and Equity?