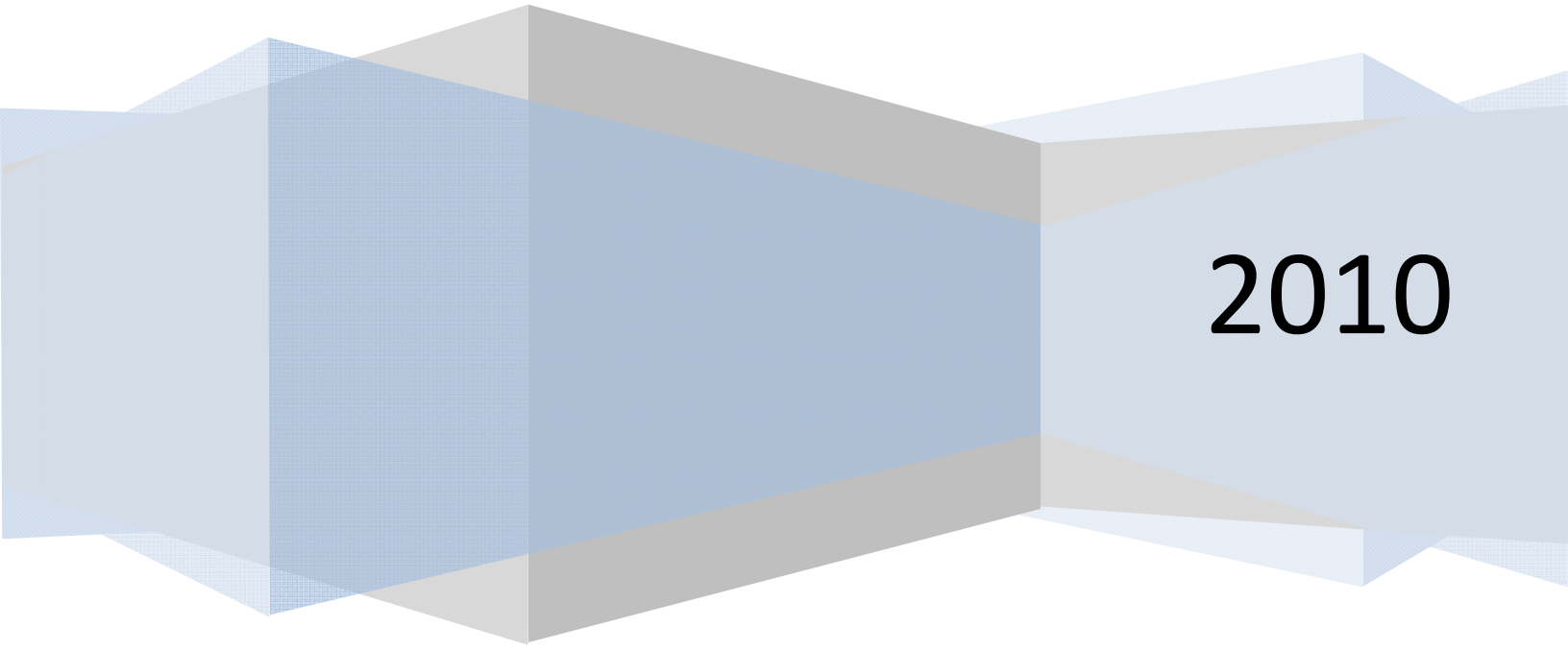
The University of Tennessee Martin

Standard Operating Procedures – Overall Operations

Information Technology Services

Prepared by: Shannon Burgin, Assistant Vice Chancellor and Chief Information Officer



2010

Standard Operating Procedures – Overall Operations
Information Technology Services
2010

Table of Contents

Overview

The Information Technology Services web site contains a significant amount of public information about our organization and services. Please refer to http://www.utm.edu/departments/its/index.php.

The Office of Information Technology Services is composed of 9 organizational units:

1. Application Development, Banner, Portal, and Imaging Administration, and Operations
2. Systems Administration and Server Infrastructure, Academic Computing, Security, and Video Network
3. Network Administration and Infrastructure, Telephone Services, Cable TV
4. Instructional Technology and Web Services
5. Technical Service Field Support, Classroom Technology, Multifunction Devices and Imaging
6. Helpdesk
7. Computer Store and Digital Printing Services
8. Budgets and Office Management
9. Planning and Leadership

Each organizational unit maintains its own Standard Operating Procedures as appropriate. A copy for each unit is stored in the shared folder under Computer Services Policies – 2010 Standard Operating Procedure.

This document contains the Standard Operating Procedures for the general ITS operation including Planning and Leadership.

The Office of Information Technology Services abides by all federal, state, and University of Tennessee policies.

UT Policies and Best Practices

All UT Policies

https://my.tennessee.edu/portal/page?_pageid=34,34235&_dad=portal&_schema=PORTAL

UT System Policies and Best Practices

Security Policies and Best Practices: http://security.tennessee.edu/policies.shtml

UT Acceptable Use of Information Technology Resources

UT Martin abides by the UT System Acceptable Use Policy listed below:
https://my.tennessee.edu/portal/page?_pageid=34,140536&_dad=portal&_schema=PORTAL&p_policy=IT0110

Mission, Goals, and Organizational Chart

Information Technology Services Mission Statement

See http://www.utm.edu/departments/its/about/index.php
Information Technology Services – About Us

The Office of Information Technology Services provides high-quality information technology and communications resources and services through shared resources, common infrastructure and functions in support of the academic and administrative activities of the University of Tennessee at Martin. This office provides centralized services in the areas of academic computing; server administration; administrative computing; application development; training and faculty development; technology consulting; information and network security; data, voice, and video networks; computer installation, upgrades, service, and support; helpdesk support for faculty, staff, and students on and off campus; computer hardware, software, and accessory configuration and acquisition; cable TV; telephone technical services; multifunction convenience copiers, printers, and scanners installation, configuration, and repair; digital printing services; and discounted prices for students on computer hardware, software, and supplies. These services are in place to provide a flexible infrastructure to meet the rapidly changing needs for instruction, all types of learning, research, and administrative functions.

Information Technology Services General Goals

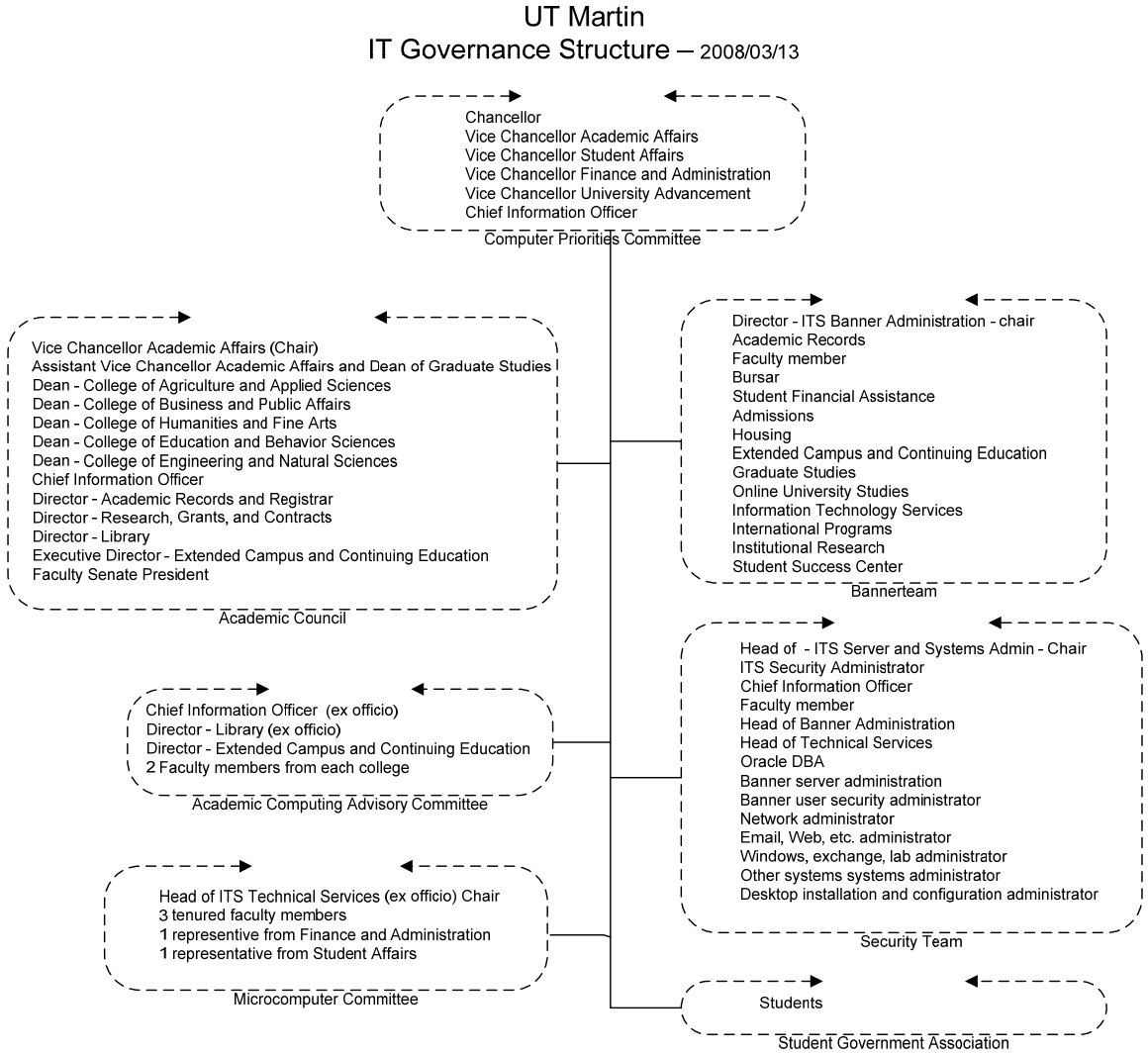
See http://www.utm.edu/departments/its/index.php
Information Technology Services – Home Page

- Keep UT Martin at the forefront of technology and communications
- Provide excellent services
- Make a difference in the way on-campus and distance education students learn
- Positively and proactively respond to change
- Provide a stable, reliable, state-of-the-art technology infrastructure

Information Technology Services Organizational Chart

See http://www.utm.edu/departments/its/about/index.php and click the latest Organization chart document
Information Technology Services – About Us – Organization Chart

Governance


UT Martin
IT Governance Structure – 2008/03/13
Chancellor
Vice Chancellor Academic Affairs
Vice Chancellor Student Affairs
Vice Chancellor Finance and Administration
Vice Chancellor University Advancement
Chief Information Officer
Computer Priorities Committee
Vice Chancellor Academic Affairs (Chair)
Assistant Vice Chancellor Academic Affairs and Dean of Graduate Studies
Dean - College of Agriculture and Applied Sciences
Dean - College of Business and Public Affairs
Dean - College of Humanities and Fine Arts
Dean - College of Education and Behavior Sciences
Dean - College of Engineering and Natural Sciences
Chief Information Officer
Director - Academic Records and Registrar
Director - Research, Grants, and Contracts
Director - Library
Executive Director - Extended Campus and Continuing Education
Faculty Senate President
Academic Council
Director - ITS Banner Administration - chair
Academic Records
Faculty member
Bursar
Student Financial Assistance
Admissions
Housing
Extended Campus and Continuing Education
Graduate Studies
Online University Studies
Information Technology Services
International Programs
Institutional Research
Student Success Center
Bannerteam
Chief Information Officer (ex officio)
Director - Library (ex officio)
Director - Extended Campus and Continuing Education
2 Faculty members from each college
Academic Computing Advisory Committee
Head of - ITS Server and Systems Admin - Chair
ITS Security Administrator
Chief Information Officer
Faculty member
Head of Banner Administration
Head of Technical Services
Oracle DBA
Banner server administration
Banner user security administrator
Network administrator
Email, Web, etc. administrator
Windows, exchange, lab administrator
Other systems systems administrator
Desktop installation and configuration administrator
Security Team
Head of ITS Technical Services (ex officio) Chair
3 tenured faculty members
1 representive from Finance and Administration
1 representative from Student Affairs
Microcomputer Committee
Students
Student Government Association

ITS Advisory Committees

Computer Priorities Committee: The Computer Priorities Committee is responsible for the establishment of administrative computing priorities for the campus. These include, but are not limited to, major software purchases and development projects, maintenance projects, and approval to modify to baseline software packages. All members are ex-officio. This committee meets on an as needed basis.

Academic Council: The Academic Council provides a platform for Information Technology Services to information the members of its activities. The members of the Academic Council provide advice with regard to academic computing priorities and to changes and enhancements to the student information system. All members are ex officio members. The council meets on a monthly basis.

Microcomputer Committee: The members of this committee represent faculty and administrative staff. This committee reports to the Chief Information Officer, and has the responsibility of recommending annually an approved list of microcomputer equipment for which full campus support will be provided, and of determining necessary exceptions to the approved list. The committee is chaired by the manager of Technical Field Support Services unit and includes representatives from the Vice Chancellor areas.

Academic Computing Advisory Committee: The committee meets at least once during each academic year to discuss academic computing priorities and makes recommendations, to the Vice Chancellor. The committee reviews the Technology Fee budget and allocates funds for the academic unit special technology projects from the Technology Fee. Two faculty representatives from each college are appointed by the Vice Chancellor of Academic Affairs to serve 2 year terms. The Director of the Library and the Director of Extended Campus and Online Services serve as ex-officio members. The Chief Information Office serves as an ex-officio member and chairs the committee. Committee information is communicated to the Chancellor's Staff, Deans and Department Chairs, the Academic Council, the Faculty Senate, and the Student Government Association.

The Bannerteam: The Bannerteam was established as part of the original installation of the Banner Student Information System. It continues to meet to disseminate information about changes between offices who utilize Banner. Because of the tight integration, changes in procedures and data in one office impact other offices. Communication and information is key. ITS provides members of the Bannerteam with project status updates. The Bannerteam assists in setting priorities. Open discussions about needs create synergy

and develop best practices that can lead to solutions and benefits for multiple areas. The Bannerteam meets on a monthly basis.

Strategic and Budget Planning Procedures

The planning process serves to align all technology plans with the missions of the university and the Martin campus and its extensions. Information for creating technology plans is derived from many sources including the Academic Council, SGA, meetings with academic departments, one on one meeting, surveys, RFP's, external resources such as Educause, SungardHE, Dell, government publications, and other campuses. The Information Technology Services Leadership Team meets on a weekly basis to discuss current and future projects and resource needs. The ITS Leadership Team consist of the Directors and Managers of the 8 units of IT and the CIO.

During the weekly IT Leadership Team meetings the IT Leadership analyzes the current activities of the various departments in Information Technology Services and decides what actions need to be taken place in order ensure that work is being done correctly and in efficient and effective manner.

Good communication between departments is enhanced, ideas are presented for improvement, information is shared, and essential planning takes place. Information from the Leadership Team meetings and the Strategic Plan are used to develop the yearly budget planning material and to project future needs for the next 3-5 years. Strategic plans are continually reviewed for completion and relevance. Information Technology Services Strategic plans are integrated into the UT Martin Strategic plans on a yearly basis. Strategic plans and updates are submitted to the Vice Chancellor for Academic Affairs Planning unit on a yearly basis. Budget Plans are submitted and presented to the Budgeting Planning committee on a yearly basis.

ITS also maintains a 5 year Technology Master Plan that feeds into the Strategic and Budget plans. ITS updates the Vital Statistics each fall to provide metrics related to services providing and changes being made. The Vital Statistics, as well as other planning reports, are located on the ITS website – About Us.

Information Technology Services staff meetings are held on the 2nd Friday of each month. During staff meetings the CIO presents information relative to the time period, such as planning for Performance Reviews, an overview of the Strategic Plans for the campus and Information Technology Services, Information Technology Services Budget Plans, policies and procedures, other employee development programs, and team building exercises. Staff members are encouraged to share information about current and future projects and resource needs.

Student Conduct in Student Computing Labs

The standards of conduct described in the Student Handbook and the Acceptable Use of Technology Resources Policy (UT Fiscal Policy IT0110) must be followed at all times.

No conduct which interferes with the work of others in the laboratories is allowed. This includes excessive talking or talking in an unusually loud manner or otherwise making loud noise.

Without prior authorization, software or data files shall not be placed on any fileserver, hard disk, or other University-owned storage medium. Laws of the United States and the State of Tennessee must be observed fully. This includes copyright laws as well as laws regarding unauthorized use or modification of computer programs and data stored on computer systems.

Students working on projects related to academic achievement take priority over students using computers for social and entertainment purposes.

Hardware or software that is not working properly should be reported to the Helpdesk at 7900 or **helpdesk@utm.edu**.

General Access Student Lab Reservation Procedure

The general access student labs are intended to be utilized primarily for academic use by students outside of the classroom, but related to university class assignments. If an instructor desires to have a class meet in a computer lab, then every effort should be made to schedule the class in a departmental lab belonging to their college. If this is not possible, then one of the general purpose student labs may be reserved for one or at most two class meetings according to the guidelines stated below, which vary depending upon the time of year the lab is needed.

In order to provide the students the courtesy of letting them know that the lab will not be available at a particular date and time, the Office of Technology Information Services allows no reservations unless the reservation is made at least three days prior to the date to be reserved. Classes must not be regularly scheduled in the general access labs. Short seminars and/or workshops are not normally allowed during regular operating hours, and none will be scheduled without the express consent of the Chief Information Officer or his/her designated representative.

Call the Information Technology Services Help Desk at 881-7900 to make lab reservations. The Help Desk manager will note whether the facility is available at the requested time and will make tentative reservations if it is available. The Help Desk will provide signs in the reserved lab stating when the facility will be unavailable for general use.

Summer Session

Because of decreased usage during the summer, there is a bit more flexibility for using some of the labs for special purposes. Long-term users include the Governors School for the Humanities and the Kid College. These groups will receive top priority immediately after the regularly scheduled classes approved for the facilities.

School not in Session

This is the time that workshops, seminars, training sessions, etc. may be scheduled in the labs.

Standard operating hours can be found at **http://www.utm.edu/departments/its/labs/index.php** or Information Technology Service – Computer Labs.

Standard Operating Procedures – Overall Operations
Information Technology Services
2010

Microcomputer Purchase Policy and Procedure

The University of Tennessee at Martin has an obligation to obtain computing resources in fulfillment of its mission, and to maintain these resources in a professional manner. This policy has been established for the purpose of providing guidance for the maintenance of existing microcomputer equipment and for the purchase and provision of maintenance for new microcomputer equipment.

Support for Existing Microcomputer Equipment:

Maintenance and repair will be provided for all items on the approved list purchased through the UT Martin Computer Store. Existing equipment will be maintained at a level as good or better than commercially available. Items which have reached obsolescence, or which cost more to repair than new equipment costs, will be subject to review for continued service.

New Microcomputer Equipment:

The University is supporting several kinds of equipment. The approved list is attached. If purchases are made from this list, then you can expect the following service at no charge to your department:

- Hardware maintenance will be provided.
- The technical capability to attach to the campus network will exist.
- Your department will be protected from future increases in maintenance costs.

The list is considered good until July 1 of the following year. The list will be developed and revised (if necessary), at least annually, by the Microcomputer Committee. The duties and authority of this committee are described in the procedure accompanying this policy.

Exceptions:

Any department, which determines that equipment on the list is inadequate for its needs, must first have the approval of the appropriate member of the Chancellor's staff to purchase a non-approved item. The department shall follow Standard University purchasing procedures to purchase the equipment and provisions for long term maintenance with the vendor or their

service provider. Central funds will not be available to increase the departmental budget for the purpose of maintenance.

Microcomputer Policy: PROCEDURE

This procedure applies to the purchase of microcomputer equipment with a purchase price of more than $500.

Approved Items:
Approved items shall be purchased through the Computer Store. Installation and maintenance shall be provided through Microcomputer Maintenance.

Exceptions:
If a department requires equipment not on the approved list, a memo must be submitted to the appropriate member of the Chancellor's Staff requesting an exception. If that member of the Chancellor's Staff agrees that an exception is warranted, the request may be forwarded to the Microcomputer Committee for verification that no item on the approved list will perform the required function.

The Microcomputer Committee

This committee shall consist of six members. Three shall be tenured faculty members appointed by the Vice Chancellor for Academic Affairs. One shall be appointed by the Vice Chancellor for Business and Finance and one by the Vice Chancellor for Student Affairs. The supervisor of Microcomputer Maintenance shall chair the committee. The chair has all privileges of membership with the exception of voting. The committee's reporting channel is through the Chief Information Officer.

The committee will annually recommend an approved list of microcomputer equipment, for which full campus support will be provided. It is expected that the committee will arrange for vendor demonstrations of equipment, examine trade publications, and be familiar with the available equipment, and the campus needs.

The committee has the authority to advise members of the Chancellor's Staff, at their request, of necessary exceptions to the approved list. The committee will have the authority to recommend modification of the approved list to the CIO.

In the case where the CIO is not in a position to accept the recommendation of the Committee, the CIO will meet with the Committee in an attempt to resolve differences. If the differences cannot be resolved at that level, the Vice Chancellor for Academic Affairs will resolve the

difference. If resolution is not possible at that level, he/she will take the matter to the Chancellor's Staff for resolution.

Faculty Computer Rotation General Procedures

As of fiscal year 2011, the Faculty Computer Rotation has become a permanent recurring budget allocation of $150,000 and is no longer subject to budget availability on a year to year basis. The Faculty Computer Rotation was established to provide the University of Tennessee at Martin faculty with up to date computers that will provide continuously expanding tools and resources and assist in broadening instructional methods.

- Each year prior to the end of the spring term, Information Technology Services will review its database of tag #'s for computers that are due for rotation, 3 years old.
- Faculty rotation computers are rotated by tag #.
- They must be assigned to a full time permanent faculty member.
- The CIO, Computer Store, and Technical Field Support Services meet to select the standard systems for the new rotation, based on current contract vendors, pricing, repair rates, and faculty input from the previous year. Budget amount and number in the rotation batch are also considered. The numbers will vary based on the full time permanent faculty hires for the year.
- An electronic list is compiled by the Computer Store and Technical Field Support Services. The list contains the tag #, computer description, last known faculty assignment name and department.
- The list is shared with the CIO, the Administrative Assistant in Academic Affairs, and the Budget Manager for Academic Affairs. Because of changes in faculty status, turn over, and other unknown changes, the list is reviewed for accuracy and full-time permanent status. It usually requires updates.
- Once the list is approved, an email will be sent to department chairs and faculty scheduled to receive a new computer with instructions on selecting from the standards or requesting an exception. Exceptions are discouraged unless there is an instructional or research need. The more exceptions the greater the cost. Standards usually include a Mac and pc and a desktop and notebook. Examples of exceptions are the tablet computers, additional memory, faster CPU, additional hard drive space, larger monitor, etc.
- The request submission period ends by the end of the spring term. The Computer Store compiles the requests and develops a pricing estimate. The new list is submitted to the CIO, Budget Manager for Academic Affairs, and the Vice Chancellor for Academic Affairs for approval to proceed with ordering.
- Orders are placed for delivery after July 1, the start of the new fiscal year.

- Once the systems are delivered and processed through the Computer Store, the Computer Store coordinates with Technical Field Support Services to schedule installations with the faculty. We do the best we can to make sure faculty members who request delivery prior to the beginning of the term receive their systems.
- Department Chairs for new faculty hires or replacement full time permanent positions, where the rotation was delayed because of an unfilled position, can request a rotation computer by emailing the Computer Store. The Computer Store will verify the request with the CIO, Budget Manager for Academic Affairs, and the Academic Administrative Assistant.

Procedures for Determining Technology Fee Expenditures

The Technology Fee was established in 1997 to address four main areas:

- Enhanced student access to computers
- Increased student computing support
- Replacement of obsolete equipment
- Improved classroom instruction

The Chief Information Officer for Information Technology Services is charged with the responsibility of preparing a technology fee budget for each year, as well as presenting an annual expenditure report. The Office of Business Affairs is responsible for collecting the technology fees from the students and for transferring the income to the appropriate technology fee account. Technology fees and the expenditures are kept separately for the UT Martin McNairy County Education Center. This was written into the agreement for UT Martin to manage the McNairy County center.

Early in each spring semester the CIO, in conjunction with the Information Technology Services Leadership Team in the appropriate areas, determines which equipment must be replaced for the established three-year rotation and then prepares a budget draft showing the mandatory expenditures (for salaries and student wages, for faculty development funds, etc.) and also which funds will remain available for other expenditures. The CIO then sends a request to academic departments asking for proposals for spending the unbudgeted funds that remain. After these have been gathered, the CIO convenes the Academic Computing Advisory Committee. The committee tentatively approves a budget. Input is also gathered from the SGA and the Academic Council.

Once the budget is approved by the Vice Chancellor for Academic Affairs, the CIO is responsible for communicating the budget to the academic departments, the SGA, and the Chancellor's staff. The CIO is responsible for making sure that the expenditures are made in keeping with the approved budget.

1. **Enhanced student access to computers (technology)**
    a. Computers
        i. General Purpose labs
        ii. Residence Halls
        iii. Departmental labs
    b. Internet and LAN access
    c. Staffing support

   d. Student email, web services, file storage
2. **Increased student computing support**
   a. Staffing for support
   b. Infrastructure of support
3. **Replacement of obsolete equipment**
   a. Computers
      i. General Purpose labs
      ii. Departmental labs
      iii. Electronic Classrooms
   b. Staffing support for executing replacement
   c. Internet and LAN access
   d. Projectors
   e. Replacement supplies such as projector bulbs, batteries
   f. Replace furniture in General Purpose labs (facilities fee now takes care of furniture)
   g. Pay-for-print Printers and print stations, may occur if not covered by print charge revenue
      i. General Purpose labs
   h. Student email, web services, file storage
4. **Improved classroom instruction**
   a. Computers for electronic classrooms
   b. Internet access and LAN access
   c. Projectors for electronic classrooms
   d. Staffing support
   e. Security and door access
   f. Smartboards
   g. Sympodiums
   h. Sound Systems in MULES/COWS
   i. Faculty Development

The Technology Fee does not cover:

- Printing or printers in departmental labs
- DL equipment
- Sound Systems that are not part of the classroom technology components
- VCR's
- TV's
- Whiteboards
- Screens for projection
- Calculators
- Stolen equipment in classrooms or departmental labs
- Food

Guidelines for Recycling Computers Purchased with the Technology Fee or with the Faculty Computer Rotation Funds

The costs associated with the recycling of computers (i.e., redistributing computers which have been replaced by newer computers) are known to be measured in hundreds of dollars. Because of having numerous computers available for recycling, these guidelines are being established to provide an orderly process for redistributing those computers that were purchased originally by technology fee funds, or by Academic Affairs funds for the faculty computer rotation program.

These guidelines provide for the return of funds to the technology fee account for purchase of additional new equipment and services for student use, and to the Office of Academic Affairs for the purchase of additional equipment and services for departments in Academic Affairs. There is a small amount given to the UT Martin Computer Store for the service of moving computers, refurbishing the computers, redistributing them, and processing the paperwork. Although the amount given to the Store does not cover the costs of recycling these computers, other personnel in the Office of Information Technology Services will supply assistance so that the Store does not have to absorb the additional costs of the recycling process.

Guidelines

1. The Office of Information Technology Services (ITS) will maintain a database of computers which are available for recycling, or which are soon scheduled to be available.
2. The ITS will also maintain a database of departments that have requested computers and of the type of computers desired.
3. Departments have 1st choice on paying $200 and retaining a rotation computer for their department. After that the computers will be allocated on a first-come, first-served basis.
4. There will be a charge of $200 for each computer that is recycled. Of that amount the Computer Store will take $50 for processing the request. For a computer that was purchased with the technology fee funds, the remaining $150 will be credited to the technology fee account to be used for further allocations of technology fee funds. For a computer that was purchased for the faculty computer rotation, the remaining $150 will be credited to the Office of Academic Affairs.

5. A request to enlarge an existing computer lab or to establish a new lab MUST go through the Academic Computing Advisory Committee. No such request will be granted unless it is approved by the Chief Information Officer.

Statement for Technology Purchased with Grant Dollars

Faculty/staff who are considering submitting any grant proposal that seeks funding to purchase technology (e.g., computers, software, network, rotation, matching requirements, etc.) and/or technological services as match against the grant must involve the Chief Information Officer - Information Technology Services and the Director of Research, Grants, and Contracts in the development stage of the proposal. Further, in the event faculty/staff seek to modify an existing grant contract to purchase technology and/or technological services with any grant monies, the Chief Information Officer - Information Technology Services and the Director of Research, Grants, and Contracts must be contracted prior to the submission of a contract modification. Submissions for approval should include plans outlining the timelines, technology resources being requested, and expectations for assistance. ITS will evaluate the request and apply a monetary estimate to IT resources required.

Procedure for Determining Salary Recommendations

The Chief Information Officer makes salary recommendations to the Vice Chancellor for Academic Affairs after thorough discussions with the Information Technology Services Leadership Team and study of the annual evaluation forms. Each leadership team staff member submits recommendations for his/her area. All recommendations are consistent with the evaluations. Equity increases are based on comparisons with salary surveys such as CUPA and HEITS and with other UT employees in similar IT positions. Market information is also collected. Merit adjustments are based on the yearly evaluations.

Each leadership team staff member is expected to conduct an annual evaluation of each employee that they supervise in accordance with UT Policy and Human Resources procedures. These evaluations are conducted using the standard personnel forms supplied by the Human Resource Office during the spring term.

Other individual recommendations for salary increases are based on UT Policy.

Procedures for Hiring new IT employees

In addition to the standard hiring procedures developed by Human resources and utilized by ITS, ITS has discovered the importance of Google searching candidates prior to interview. It is also important that that we prepare all interviewees for the background checks that will be coming if they are hired. All interviewees for ITS positions are asked to complete the release form for a background check. A background check with be requested, by the ITS Business Manager, through Human Resources, for each new employee. The background check needs to be completed prior to the end of the new employee's probation period.

Procedure for Reviewing Contracts Containing Technology Components

The purpose of this procedure is to reduce the risk of information security breaches, insure adequate technology support resources, and reduce duplication of services.

- ITS will review all contacts that involve software, data, or technology related services
- The UT Martin Purchasing Office and Contracts Officer will assure that ITS is involved in the contract review process
- The appropriate IT Director(s) or CIO will complete the review
- The review will consist of:
  - Ability to complete technology work required by the contract
  - Impact on other technology services
  - Information Security

Allocation of User Accounts Procedure

Most user resource access to UT Martin computer systems is authorized through Active Directory. Active Directory accounts are created by role specified in Banner for students, faculty, and staff. Requests for services can be made through helpdesk@utm.edu or by calling 7900. Please see the separate Helpdesk unit procedures and the Systems Administration unit procedures for additional details.

With certain exceptions, computing through ITS is provided at no charge to the user. Exceptions include, but are not limited to, projects funded by external grants or other grants which provide for computing expenses.

Projects that use central services and are CPU intensive, network intensive, or that require large amounts of storage, etc. must be coordinated through Information Technology Services.

Student accounts on the central student computing facilities are established for all students who enroll at UT Martin. The accounts remain active as long as the students are enrolled. The account provides access to the myUTMartin portal which connects to other services. The account name is usually set up as the first three letters of the student's name, followed by the middle initial and then by the first four letters of the last name. Student email accounts provided through our contract with Google Apps for Education provides a life long email account @ut.utm.edu. Students who are no longer enrolled may continue to access their Banner information by entering Banner Self-Service directly from the UT Martin homepage quick links. Additional information on student account removal procedures can be found in the System Administration unit procedures.

Faculty and staff members obtain access to the myUTMartin portal, which connects to available UT Martin services, by processing the appropriate information with Human Resources and Academic Affairs which is loaded into IRIS, Banner, and then into Active Directory. Department heads must process forms through the Helpdesk to request special access to Banner Administrative. Accounts will remain active until termination, change of position, or other notification by the department requesting changes in access.

Security Incident Response Procedure

This document provides specific requirements for dealing with information systems security incidents and suspected information technology resources abuses. This document is meant to provide the UT Martin Information Technology support personnel with a systematic approach for handling the discovery of and response to an abuse or security incident. The process is developed to achieve the following goals:

- Confirm whether an incident or abuse has occurred
- Promote the accumulation of accurate information
- Establish controls for proper retrieval and handling of evidence
- Minimize disruptions to business functions and network operations
- Allow for legal (to include criminal and/or civil) actions against perpetrators
- Provide accurate reports and useful recommendations

This document outlines the processes for dealing with security incidents and/or resource abuses from any source connected to or transmitting information using UT Martin's information technology resources.

Scope
This process applies to all members of the UT Martin Campus community (including but not limited to, staff, faculty, students, contractors, consultants, and visitors) while using UT Martin's information technology resources. All users are required to know and comply with this process. This process applies to all applications, operating systems, and network operating systems. See Appendix A for a glossary of terms.

Responsibilities
The purpose of this section is to describe the roles and responsibilities that each member of the UT Martin Campus community has in relationship to resource usage and security. All users, system administrators, information technology support personnel, and security support personnel must understand their role in relation to this process. The Chief Information Officer (CIO) is responsible for maintaining and overseeing this process. See Appendix B for more detail covering the responsibilities of specific personnel.

Incidents with Sensitive Information
It is important to note that a suspected compromise of any system that stores, processes, or transmits information considered sensitive must be reported immediately to the UT Martin Information Security Officer or CIO. Sensitive information includes, but is not limited to, social security numbers, credit card numbers, personally identifiable information, or information covered by Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), and Health Insurance Portability and Accountability Act (HIPAA).

Event Detection and Incident Confirmation Process
The purpose of this section is to outline the methods used to detect events. Events can be detected through a variety of technical and procedural mechanisms. Technical mechanisms include intrusion prevention systems (IPS) and firewalls which produce alerts when suspicious network activity occurs. Procedural mechanisms include system log reviews, observations of abnormal resource utilization and suspicious account activity. Additionally, sources external to the university may detect issues by recognizing unauthorized activity or abnormal behavior on their systems and reporting the activity to the university.

The following activities on their own can represent a security event and thus require action:

- A system alarm or similar indication from an intrusion prevention tool
- Suspicious entries in system or network accounting (e.g., a UNIX user obtains privileged access without using authorized methods)
- Accounting discrepancies (e.g., someone notices an 18-minute gap in the accounting log in which there is no correlation)
- New user accounts of unknown origin
- New files of unknown origin and function
- Unexplained changes or attempt to change file sizes, check sums, date/time stamps, especially those related to system binaries or configuration files
- Unexplained addition, deletion or modification of data
- Denial of service activity or inability of one or more users to login to an account; including admin/root logins to the console
- Unauthorized operation of a program or the addition of a sniffer application to capture network traffic or usernames/passwords
- Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program)

A combination of the following activities can represent a security event and thus require action. Although observing one of these symptoms is generally inconclusive, observing one or more of these symptoms in conjunction is motivation for further scrutiny:

- Unsuccessful logon attempts
- Unexplained system crashes
- Unexplained poor system performance
- Port scanning (use of exploit and vulnerability scanners, remote requests for information about systems and/or users, or social engineering attempts)
- Unusual usage times (statistically, more security incidents occur during non-working hours than any other time)
- An indicated last time of usage of an account that does not correspond to the actual last time of usage for that account

Notification

Unless evidence collection and network monitoring is immediately initiated, critical information may be destroyed before investigators have a chance to review it. Furthermore, the UT Martin information technology support personnel have the responsibility to inform affected individuals/organizations in a timely fashion. All users should contact the UT Martin CIO, the Security Administrator or call the Helpdesk. The CIO, the Security Administrator or the Helpdesk will then gather the necessary information to appropriately record the security event. The contact numbers for the Office of Information Technology representatives are as follows:

Helpdesk
(731) 881-7900
CIO
(731) 881-7890
Security Administrator
(731) 881-7882

Reporting
Depending on the type of incident or abuse, a report needs to be created by the affected user or the UT Martin Security Administrator. If it is unsure whether a report is needed, contact the CIO or the UT System Information Security Office for guidance. Answers to the following questions should be included in this report:

- What is the associated monetary cost?
- Did the incident disrupt ongoing operations?
- Was any data irrecoverably lost, and, if so, what was the value of the data?
- Was any hardware damaged?
- Was there unauthorized access to sensitive or critical information?

Each report is disseminated to the owners of the information and the support personnel for their records. A copy of each report shall be forwarded to the ISO for review and storage.

Analyzing the cost of the incident - Work should be conducted within the organizational tree to quantify the personnel time required for dealing with the incident (including time necessary to restore systems). Deriving a financial cost associated with an incident will help those who may be prosecuting any suspected perpetrators, and will aid in the justification of funding for future security initiatives.

FOLLOW-UP
Performing follow-up activity is one of the most critical actions in responding to incidents. This helps the UT Martin Campus improve their incident handling processes as well as aiding in the continuing support of any efforts to prosecute those who have broken the law or abused University of Tennessee at Martin information technology resources. If it is unsure whether a follow-up is needed, contact the CIO or ISO for guidance. Follow-up actions include the following:

- Define the "lessons learned"?

- Analyze what has transpired and what was done to intervene.
- Was there sufficient preparation to prevent the incident?
- Did detection occur promptly? If not, why?
- Could additional tools have helped the detection and recovery process?
- Was the incident sufficiently contained?
- Was communication adequate, or could it have been better?
- What practical difficulties were encountered?

The follow-up phase ensures continuing improvement to the quality of the IRP.

APPENDIX A
UNIVERSITY OF TENNESSEE INFORMATION TECHNOLOGY SECURITY GLOSSARY OF TERMS

Acceptable Use Practice (AUP) – The AUP implements the general principles established by UT Fiscal Policy FI0805 regarding the appropriate use of information technology equipment, software and networks.

Applicable Laws of the State of Tennessee and the Federal Government – Any law in the state of Tennessee or from the federal government that applies to security and information technology, information technology resources or electronic information transmission technologies.

Computer System – An electronic device that uses common storage and executes code for designated data manipulation that is user-written. This includes all portable devices including, but not limited to, laptop computers, personal digital assistants and all mobile email devices.

Electronic Information – Refers to information in electronic form and the information technology resource on which the information resides. This does not apply to information in paper form.

Event – An occurrence that has not been verified as a security incident.

Family Educational Rights and Privacy Act (FERPA) – The Family Educational Rights and Privacy Act of 1974, commonly referred to as the Buckley Amendment, protects the rights of students by controlling the creation, maintenance, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.

Gramm-Leach-Bliley Act (GLBA) – Requires financial institutions to protect the confidentiality and integrity of their customer’s information.

Health Insurance Portability and Accountability Act (HIPAA) – Creates a standard for healthcare providers and institutions to protect the confidentiality and integrity of personal health information.

Incident Response – Is the process where information technology professionals respond to information technology resources compromises, vulnerabilities, and attacks.

Information Security Office – The entity that is responsible, under the UT Chief Information Officer (CIO), for the information technology security oversight and administration for the University of Tennessee.

Information Technology Resources – Includes any computers, computer systems, network devices, telephony systems, or software applications.
UT Martin Campus – The University of Tennessee at Martin Campus including all programs offered through UT Martin and Extended Campus and Continuing Education.

Security Incident – A security incident is an irregular or adverse event that occurs on any part of the network. Specifically, incidents include computer intrusions, denial-of-service attacks, insider theft of information, copyright violations, and any unauthorized or unlawful activity that requires support personnel, system administrators, or computer crime investigators to respond.

System Administrators (SA) – UT Martin Campus employees that are responsible for Information Technology Systems security within a department or group.

Users – Refers to all students, faculty, staff and others while accessing, using, or handling the University of Tennessee at Martin's information technology resources. "Others" includes, but is not limited to, subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities granted access.

APPENDIX B

UNIVERSITY OF TENNESSEE INFORMATION TECHNOLOGY SECURITY DEFINITION OF RESPONSIBILITIES

Helpdesk – The Helpdesk is the first level of interaction for users experiencing security events. It is the Helpdesk's responsibility to alert the UT Martin Security Administrator and/or the UT Martin CIO if a suspected incident occurs. The Helpdesk is also responsible for contacting the appropriate UT Martin Campus personnel to disable and re-enable a user's access to the network.

Information Security Office – The Information Security Office (ISO) is responsible for coordinating computer security efforts within the University of Tennessee. In addition, the ISO is responsible for actively monitoring key intrusion detection and intrusion prevention systems, assisting in vulnerability assessments, and performing forensic investigations. When necessary, the ISO or CIO will mobilize an Incident Response Team (IRT) to review the incident and respond according to the SOP. The ISO will coordinate the response with System Administrators, the Helpdesk, Network Services, security personnel, and other agencies as necessary (including but not limited to Campus Police, Student Affairs, University Relations, General Counsel, and the Federal Bureau of Investigation). The ISO is also responsible for notifying the Chief Information Officer (CIO) regarding security incidents to obtain additional direction as necessary.

Information Technology Support Personnel – In this document, applies to all employees within the Information Technology Services Department and any individual at the UT Martin Campus that supports information systems devices.

Network Services (NS) – The Network Services team will work in conjunction with the UT Martin Security Administrator and the ISO in order to identify, analyze, and respond to suspected and verified security incidents. Such responses may include disabling or re-enabling network ports, port scanning, and altering router access control lists or firewall policies.

Security Analyst or Security Administrator – Serves as the technical resource, proposing countermeasures for hardening various systems and platforms supported within the university. This will typically be a member from the ISO or the ISO's designee.

System Administrator (SA) – The SA is the first level of interaction for users whom they support that are experiencing a security event or incident. It is the SA's responsibility to coordinate incoming information, advise users on handling security events, forward information to the UT Martin Security Administrator, and disseminate information to users and other SA's as appropriate. The SA shall not reboot, disconnect, or otherwise alter the system when an event has been discovered, unless directed by the UT Martin Security Administrator/ ISO or the incident is unlikely to be prosecuted and additional forensic information gathering is unnecessary. Otherwise, collection of valid evidence is negatively impacted by losing critical information stored in system memory. The SA is responsible for monitoring the systems within their

department to identify unusual behavior or symptoms, which may indicate a security incident. These indications are further outlined in the detection portion of this document.
Users – Responsible for monitoring unusual system behavior, which may indicate a security event. The indications of a security event are further outlined in the detection portion of this process. Users are responsible for reporting events to the UT Martin Helpdesk or the Security Administrator immediately. The user shall not reboot, disconnect, or otherwise alter the system when an event has been discovered, unless directed otherwise by the UT Martin Security Administrator, the ISO, or the Helpdesk; otherwise, collection of valid evidence can be negatively impacted by losing critical information stored in system memory.