ULM Computing Center

Policies and Procedure Manual

This document is subject to change as Computing Center Policies and procedures are further defined and documented

Published 7/2008

Table of Contents

If you are viewing this document online, hold the “Ctrl” key and click on line in table of contents to go to that section of the document.

Hours of Operation

Scheduled Hours of Operation

Computing Center Main Office

The Computing Center main office (Adm. 198) follows the normal business hours of the University and is open on days that university business offices are open.

Computing Center Customer Service Area

The Computing Center Customer Service Area (Adm. 1-83) is open on days that university business offices are open. This area is open from 7:30 a.m. until 7:00 p.m. including Fridays.

Computing Center Call Center

The Computing Center Call Center is open on days that university business offices are open. Telephones (3333) are manned from 8:00 a.m. until 5:00 p.m. Monday thru Thursday and 8:00 a.m. until noon on Fridays. Web access for opening tickets is available 24 x 7.

Computing Center Help Desk

The Computing Center Help Desk (Adm. 1-83) follows the normal business hours of the University and is open on days that university business offices are open**.**

CICS Online

CICS Online is available from 6:00 a.m. until 6:00 p.m. and from 7:00 p.m. until 12:00 midnight Monday thru Sunday.

Arrow for Students and Faculty

Arrow is available from 6:00 a.m. until 6:00 p.m. and from 7:00 p.m. until 12:00 midnight Monday thru Sunday.

Employee Self-Serve

Employee Self-Serve is available from 6:00 a.m. until 6:00 p.m. and from 7:00 p.m. until 12:00 midnight Monday thru Sunday, except when payrolls are being run. Contact the Payroll Department for information on when payrolls are run.

Server Applications

Server Applications are generally available 24 x 7 except for systems maintenance. The Computing Center allocates 6:00 a.m. until 12:00 p.m. Saturday's to perform any system maintenance and reserves the right to use this time without prior notification. Special requests may be made if an event occurs where any system needs to be available during this time. These requests will be reviewed and approved or denied based on the severity of the maintenance needed. The following systems and services reside on ULM servers.

- Campus Email
- EPrint
- Flight Path
- Server file space
- My ULM Portal
- Text Book Ordering (webservices)
- Assessment (webservices)
- Course Evaluations (webservices)
- Dean & Dept. Evaluations (webservices)
- Student Elections (webservices)
- Foundation Scholarships (webservices)
- Policies Tracking System (webservices)
- Other small web applications – see a list of all web applications maintained at http://wiki.ulm.edu/computingcenter/)

Operational Support

The Operational Support area (Adm. 1-83) is open during normal business hours and from 5:00 p.m. until 4 a.m. each week day. Normal nightly batch jobs and backups are scheduled during the period from the close of the business day until 4 a.m. each weekday.

If system maintenance is required during hours that a system would normally be available the Computing Center staff will make every attempt to contact users and user departments to provide notice of down time and the estimated duration of the down time. This contact may be made by electronic mail, system notices or telephone.

After Hours or Special Support

Nightly Support

If a user requires that the scheduled evening processing be delayed, they should contact the Computing Center as early in the work day as possible. The Computing Center will work with them to obtain the needed approvals for delaying nightly processing. For FRS, LMS and HRS the delaying of regular scheduled processing can generally be left to the discretion of the Controller and the Computing Center Staff that support these areas. For SIS delaying regularly scheduled processing will likely impact the windows for when Arrow is expected to be available to students. This decision may require input from Business Affairs, Academic Affairs and the Registrars Office. After the requestor's work had been completed, it is important that they notify operations so that the nightly processes can resume as soon as possible.

Weekend Support

If a user requires weekend support, they should notify the Computing Center before noon Thursday to make sure that the system will be available. Since much of the system maintenance (software upgrades, equipment repairs, disk optimization, etc.) is scheduled for the weekends, it is extremely important that users verify that the system will be available during the time that they plan to use the system.

Holiday Schedules

With the exception of the Christmas Holidays, the Computing Center does not generally provide support during University Holidays. Due to the nature of our work, we do expect to provide some system availability over the Christmas Holidays. Any office that requires support during this time should notify the Computing Center two weeks before the last working day of the semester. This will allow the Computing Center to develop a schedule that will meet the needs of all departments with as little impact as possible on the holidays of Computing Center personnel.

User Support and Services

Overview

The information in this section is intended to provide guidance when reporting computing problems or seeking assistance from the Computing Center. The following is a list of various areas within the Computing Center and the type of support they provide.

- **Customer Service Area -** Located in Administration Building room 1-83.
    - **Test Grading**
    - **Help Desk –** Located with in the Customer Service Area. Some of the areas supported are:
        - Service and support of all university equipment.
        - Service and support of all UCC approved Operating Systems and UCC provided software
        - Support for university systems such as Webmail and Learning Management Supervisor (LMS)
        - Assists in the troubleshooting of technology related issues and fielding those issues to appropriate technicians.
    - **Operations –** Located with in the Customer Service Area.
        - Monitors mainframe
        - Runs batch jobs
        - Manages tape library
        - Handles printing of checks and reports produced by mainframe jobs.
- **Call Center** – This area logs service requests and reported problems into the Help Desk Database. They are able to resolve some problems at the time of the call. Those they cannot resolve get routed to the appropriate area for resolution. The Call Center manages the Help Desk Database
- **Network Support –** Located in Administration Building 1-155.
    - Handles network problems
    - Manages network expansions
    - Supports wireless access on campus
    - Supports internet access
    - Supports email
    - Account Administration
    - Server Administration

- **Mainframe Programming Group –** Located on the third floor of the Administration Building. This group supports all mainframe applications and their web interfaces (SIS, FRS, HRS, LMS, Inventory+). Also supports various Access and Paradox data bases. Supports ePrint.
- **Web Application Programming Group -** Located on the third floor of the Administration Building. This group supports web development, Flight Path, Text Book ordering and the ULM Portal. See http://wiki.ulm.edu/computingcenter for an updated list of all web applications this group maintains.
- **Technical Services –** Some of the areas support by this group are
  - Computing hardware installation and repairs.
  - Hardware upgrades and warranty repairs to eligible university computers
  - Fee based on warranty repair of computers

- **Telecommunications –** This Group supports the telephone equipment across campus.

The ULM Computing Center maintains various forms to assist you with your request. The most current version of these forms can be found on the ULM web at http://www.ulm.edu/forms/#anchor259518 .

Reporting Problems

Any computing problem may be reported to the Call Center by calling 3333. In some cases the Call Center will be able to resolve the issue. If they are not able to give you an immediate answer they will route your request for help to the appropriate area within The Computing Center.

Issues may also be reported using the ULM Computing Center's Helpdesk application for recording and tracking problems and request. This application may be accessed at http://computersos.ulm.edu/ .

Making Requests from the Computing Center

Security Access Request

Security access is covered in the Security of Data and Computing Resources sections of this document under Acquiring Security Access.

Request for Data

Request for data extracts or reports from university files maintained in the Computing Center must be in writing. Request may be submitted in one of three ways:

- Submit a work order. The work order form can be found at http://www.ulm.edu/forms/cc/ProgrammingWorkOrder.pdf
- Open a ticket on the Helpdesk System under "Mainframe" - http://computersos.ulm.edu/
- Send an email

You may only request data required for your area of responsibility. A "Data Request Authorization" form that has been signed by your department head must be on file in the Computing Center before data can be released to you. If the Computing Center does not have this form on file they will send you a copy of this form to get signed and returned before your file or report is provided.

Mainframe Programming Request

Request for mainframe support may be made in one of several ways.

- Open a ticket on the Helpdesk System under "Mainframe" http://computersos.ulm.edu/
- Submit a work order to the Manager of Application Programmers. The work order form can be found at http://www.ulm.edu/forms/cc/ProgrammingWorkOrder.pdf
- Send an email to the Manager of Application Programmers - reeks@ulm.edu

Web Application Programming Request

Request for Web application development may be made accordingly:

- Submit a work order by filling out and submitting a programming project request form at https://webservices.ulm.edu/computing_center/project-request.php
- Call or email to the Senior Web Programmer. Brian Taylor, ext. 5023, email taylor@ulm.edu

It may also be requested by opening a Helpdesk ticket under "Web Programming" at - http://computersos.ulm.edu/

Due to limited web programming resources and increased demand for web application development, all requests such requests must be approved and prioritized by Computing Center staff and upper level administration.

Other Programming Requests

Any programming request may be routed through the Call Center by calling 3333 or opening a ticket on the Helpdesk System at http://computersos.ulm.edu/.

Networking Request

Request for Equipment Connection/Reconnection

Request to connect or reconnect equipment should be sent to the Computing Center, room 1-98 in the Administration Building. The form for making this request may be found at - http://www.ulm.edu/forms/cc/ConnectionReconnectionForm.pdf.

Request may also be made by opening a Helpdesk ticket under "Networking" at http://computersos.ulm.edu/.

Note: Please be prepared to provide a budget code.

Software Request

- A form for requesting software can be found at - **http://www.ulm.edu/forms/cc/SoftwareRequestForm.pdf**

  Note: This form must be presented by the requesting party.

- Some software may be downloaded from the Computing Center web page - http://www.ulm.edu/computingcenter/

Obtaining Copies of Site Licensed PC Software

At ULM, Personal Computer software is available through a campus software site license. This software is available to any currently employed faculty or staff member. To secure a copy of any available site licensed software from the Computing Center the following steps are required:

1. Obtain a PC software Request form.
2. Have your department head validate the request.
3. Sign the form indicating adherence to the terms stated.

The PC Software Request Form may be obtained from the administrative office of the Computing Center, Administration Building 1-98 or the Customer Support desk in Administration Building 1-83 or now online at http://www.ulm.edu/forms/cc/SoftwareRequestForm.pdf.

The requester should bring the completed form to the service desk in Administration Building. 1-83. At that point the requested software will be distributed to the requester. In the event that the requested software is temporarily unavailable, a date and time for pickup will be given.

The user is expected to install the software package. If assistance is not available within their department, the Computing Center will provide some assistance but resources are limited so assistance may be minimal.

The software request form must be completed for each individual using the software. The reason for this is that the Microsoft Office products are licensed so that it can be taken home and loaded onto an employee's personal computer. The software must be removed from the home computer when an individual terminates employment with ULM.

NOTE: For those responsible for lab support, a separate form is available to document the number of PCs, locations, etc. This is at http://www.ulm.edu/computingcenter/itsupport/softwarerequest/

***A list of software available is located on the ULM Computing Center website.

***Note:** various departments and colleges within the university may have **other software licenses** than those listed on the web site.

Other Networking Request

Other networking request may be made by opening a Helpdesk ticket under "Networking".

Request for Data Transfer

Data transfer request may be made by opening a Helpdesk ticket under the appropriate group - http://computersos.ulm.edu/

Request for Archived EPrint Report

Reports are kept on ePrint for two years and then archived as encrypted files on CD/DVDs. Request for access to archived reports should be made to the Computing Center Mainframe Programming Group.

Training Services/Support

The number of computer users at ULM has grown dramatically in recent years. This fact strictly limits the amount of individual assistance that can be provided. In an effort to lessen the need for one-on-one assistance and to facilitate more effective use of resources, the Computing Center will assist the Human Resources Training Coordinator in training of faculty/staff in the use of PC, Learning Management Supervisor and/or mainframe software supported by the Computing Center.

The Computing Center cannot guarantee assistance for faculty/staff using unsupported equipment and software.

Training is provided with the following provisions:

1. Pre-registration is required for all workshops.
2. The Computing Center reserves the right to reschedule workshops in the event of low enrollment.
3. The Computing Center reserves the right to limit the number of participants in a single workshop. Limits will be based on the availability of equipment required for the training.
4. One copy of the appropriate training materials will be furnished to each participant. Additional copies of documentation will not be provided, however those attending workshops are welcome to duplicate documentation at their expense.
5. On-site training will be considered if;
    a. The department requesting on-site training can provide an appropriate training area,
    b. All required hardware and software is available, and,
    c. An acceptable number of attendees will be present. ("Acceptable number" to be determined by the workshop instructor.)
6. As-needed support will be provided based on the availability of a person who is able to assist.

<u>Other request</u>

Any other request not covered above may be made by opening a Helpdesk ticket under the appropriate group - http://computersos.ulm.edu/

Computing Center Test Scoring System

The ULM Computing Center, with the help of on-campus educational researchers, has designed and developed a test scoring and test analysis program for objective tests. This system utilizes a Scanning Systems optical scanner to capture the raw data on magnetic media whence it is processed.

The sheets used to record test answers are available to the faculty from their department heads or the bookstore. Due to the large variety of scanning sheets available commercially, it is highly recommended that any special scanning sheets be cleared with the Director of the Computing Center before they are purchased and the data collected.

Scoring and Analysis Output

There are eleven different types of output produced by the test scoring and analysis program (referred to as the "program" hereafter). The first four are standard and are produced for all jobs. The last seven are options and are produced according to request.

To obtain the service, you must fill out a request sheet indicating, among other things, your name, department, course, date of test, number of answer sheets, number of questions, and options required. Please include you telephone number so that you may be contacted if a problem occurs.

Standard Output

1. Copy of the information on the request sheet. This not only confirms your request but also serves as a cover sheet for the remainder of the report.
2. Listing of the test key.
3. Listing of the weight given each question. (The program allows you to assess each question a weight of one to five).
4. Listing of test grades consisting of:
    a. Student name
    b. Student identification number
    c. Percent score
    d. Number omitted
    e. Invalid questions
    f. Number correct.

If a student fails to give a correct student number and name, he will appear on this listing the way that he marked his answer sheet. Sheets with more than one mark per line in any of the student number, name, or answer sections will be rejected.

Optional Output

1. Grade distribution analysis. The program produces a histogram of the test scores, the average number correct, and the standard deviation of the number correct.
2. Right/wrong analysis by question. For each question of the test, the program produces the percent of students with a correct answer. It also gives the distribution of answers given by the students on each question.
3. Detailed list of questions missed by each student consisting of student name, student identification number, and the question numbers he missed.
4. Split-halves Kuder-Richardson reliability coefficient. This coefficient is an indicator of a test's internal consistency. It is obtained by comparing two sets of scores resulting from one administration of the test which is scored in two equivalent halves. The range of values is -1 to +1, and generally speaking, the higher values indicate a better test. For further information see Measurement and Evaluation in Teaching, Norman E. Grond, MacMillan Co., New York, 1968.
5. Listing of student name, student identification number, percent correct in rank order.
6. Listing of student name, student identification number, percent correct, and rank in class. The results are listed in ascending order by student number.
7. Listing of student name, student identification number, and standardized Z-score in rank order. The average percent score and standard deviation are also given.

Job Submission Requirements

The following must be observed when submitting a job for processing.

1. Data sheets and request forms must be submitted in a letter-size folder or large envelope. Loose forms, or forms held together with rubber bands, paper clips, staples, etc. will not be accepted.

2. The order and content of the forms is:
    a. Test Scoring Analysis Request - This form is available at the service counter and must be filled out completely. It must be the first sheet in the folder.
    b. Test Key - On the first scoring sheet, the instructor is to make the key for grading the test. It is very important that the student number field be left blank on this sheet. Teacher’s name, with the appropriate boxes marked may be put in the area marked "LAST NAME FIRST INITIAL SECOND INITIAL". No other marks are to be made on this sheet except for the correct answer for each question, maximum is 150.
    c. Question Weight - If the instructor desires to give questions relative weights from one to five, he must complete this form. In the spaces for name, this can be left blank. The boxes for student number must contain all 1's. To give the question its relative weight the instructor marks position "a" for a weight of one, "b" for a weight of two, and so on. If the instructor elects to give weight to certain questions, he must give weight to all other questions. An error of omission here will cause the question to be omitted since it will receive a weight of zero. (NOTE: If an instructor wishes a question to be omitted, this gives him the vehicle for doing so). If the instructor elects that all questions should have a weight of one, this sheet is to be omitted.
    d. Student Answer Sheets - The student answer sheets are the last items in the folder. All sheets must be oriented in the same direction, with no folded or torn sheets.

       The student must put his student number or some identifiable code in the spaces of the student number field. **NOTE:** Student number must not be all 1's, all 2's or all 9's.

       Student’s name should be put in the student name field.

       The student's answers are to be clearly marked within the area given, with no extraneous marks on the paper. It is also imperative that no marks be made on the left side of the paper near the column of timing marks. Any marks in this area may cause the sheet to be rejected.

Notes to Users

Through experience, we have found that there are many common errors made which either inhibit or prevent processing of the data sheets. The following is a list of Do's and Don’ts for the instructor to follow:

DO

1. Do put the proper identification on each sheet and insist that your students do likewise. A student answer sheet without proper identification will be rejected by the program and not graded, and improperly marked key will cause the entire job to be canceled.
2. Do keep your sheets clean. Avoid any smudges or other dirt. Be sure all erasures are complete. A partially erased answer may be picked up by the scanner and counted as an incorrect or invalid reply. Any marks along the left edge of the page will cause the entire sheet to be rejected.
3. Have a contingency plan for test grading. Mechanical systems do, at times, fail and require repair.

DON'T

1. Don't allow sheets to be folded, bent or torn.
2. Don't secure the sheets together with rubber bands, paper clips, staples, hole punches, etc.
3. Don't allow the students to use anything but a number two pencil to mark their sheets. The softer lead pencil marks are easily smeared and are hard to erase and the harder lead pencil marks are too light to read. NO INK PENS OR MECHANICAL PENCILS can be used.
4. Don't allow the students to do "scratch" work on the sides or back of the scoring sheets.
5. Don't reuse the worn scoring sheets. Improper handling in passing out and taking up of exams plus repeated usage of the paper makes the sheets very difficult to read.

Submission Procedures

Test packages, as described above, are to be turned in to the Computing Center Customer Service counter attendant. (Administration Building 1-83.) Customer Service is open from 7:30 a.m. to 7:00 p.m., Monday through Friday during summer, spring and fall semesters.

You will receive a numbered card from the counter attendant. For your protection, the card is used to prevent unauthorized collection of test results, and the package will be returned only upon presentation of the claim card.

Normally, you may expect the results within 1hour. However, during peak loads, such as six-week intervals and near the end of the semester, the number of jobs sharply increases, resulting in a longer time for processing. The Computing Center has no on-site repair capability for test-grading equipment.

ULM Email/Collaboration System

Email Access

Employees are provided with a University email address upon start of employment. This email address is the property of ULM and is to be used for University business only. It is not to be used as your personal email, for sending/receiving jokes, family pictures, or personal business not related to the University. The Computing Center reserves the right to audit email for violations of this policy.

Pending a May-June migration of email to the Zimbra Collaboration Suite, employees will be given a 1 GB quota for their online mailbox, which will be accessible via Webmail, Outlook, or iMail. This quota will be monitored by the Computing Center staff and necessary actions will be taken when this quota is exceeded. Once the quota is exceeded, no new mail will be delivered to that person. Employees can also store email on their desktops via PST files, but the Computing Center will not be responsible for backing up this data. Upon termination of employment, the email account will be deleted. No forwarding will take place unless approved by the employee's direct manager and if approved, will be active for no longer than 3 months.

Calendar Sharing

Pending a May-June migration of email to the Zimbra Collaboration Suite employees will also be provided with calendar sharing and resource control through the Collaboration system. Calendar sharing can be enabled by Employees and can also be made available to share with Students. Resource control, such as conference room scheduling, will also be made available.

Upon special request, Employees can request a "special use" email to use for ULM business only. This email will be limited to Webmail access only and have a 150 MB quota. This quota will be monitored by the Computing Center staff and necessary actions will be taken when this quota is exceeded. Once the quota is exceeded, no new mail will be delivered to the account. The Computing Center reserves the right to audit email for violations of this policy.

ULM SPAM Control System

The ULM Computing Center maintains a SPAM control system which reduces the amount of SPAM that enters the campus, and prevents certain types of attachments from entering the ULM system from the outside. This system is frequently monitored and tuned for maximum effectiveness.

No SPAM control system is perfect and a certain amount is inevitable. If an employee is receiving too much SPAM, they may open a “Server” Helpdesk ticket to have the problem investigated.

If an employee has not received an email, they may open a Helpdesk ticket to request a lookup and release if the SPAM control system has falsely identified their email as SPAM.

An employee can request certain email addresses be added to the “white list” to always allow those emails through the system.

Student Access

Students are provided an assigned Email (LDAP) account upon accepted application to the university. This account provides access to the following systems:

- Email/Calendar Sharing
- ULM Portal System
- LMS (Moodle, Blackboard)
- Wireless
- GoPrint (Lab print controls)

Access to this account can be checked by selecting “Help” on my.ulm.edu (portal).

Student workers in some of the administrative offices will be assigned duties that require access to online mainframe screens. They will be required to fill out and submit the same security access request forms that all ULM employees submit for access to mainframe resources. The student worker’s supervisors should instruct them on the access they will need and assist them in submitting the required forms.

ULM Portal System

The MyULM web Portal is an interactive web application which allows users to control the layout and functionality of their online experience. The portal provides targeted notifications, targeted information and single sign-on access to campus web applications such as Zimbra, Moodle, Arrow, etc. The software running the portal is uPortal 2.6.0.

Students and employees are assigned a MyULM account along with creation of their new email address. Access MyULM by visiting https://my.ulm.edu and entering their email address (without @ulm.edu suffix) and the same password used for accessing email.

ULM File Storage/Drive Shares

Employees are granted the use of drive shares that are to be used to store ULM work-related documents. These shares are considered to be protected storage that is fault-tolerant and backed up daily. Each employee will have a personal share (1 GB quota) that only will be accessible to them, and also a group share (agreed upon quota) that will be accessible from anyone in their group. Other shares can exist as needed. These shares are to be used to store ULM business information only and are not for storing personal information, such as family pictures, music, or any non-work related items. These shares are also not to be used to store backups of desktop/laptop hard drives, or older files that are only needed for archival purposes. These restrictions will be strictly enforced and audited on a regular basis.

VPN Access

Employees are granted the use of the ULM VPN System, which allows access to campus resources from any Internet/Broadband connection. Employees who use the VPN must ensure their computer meets specifications, such as recent patches and virus control software, before accessing the VPN. Employees are not allowed to give others access to the VPN through their login.

Employees may access ULM VPN System at https://vpn.ulm.edu/webvpn.html. The system requires the employee to sign on with their email user name and password.

Wireless Access

Employees are granted the use of the ULM Wireless System in areas designated as wireless access. Contact Adam Taylor (3354) for more information.

Computing Center Overview

The Computing Center supports several general areas. The work of these areas sometime overlaps and is always interrelated which makes defining a particular area or functions difficult at best. For the sake of this document we will discuss the policies and procedures that support the Computing Center functions of Mainframe Support, Technology Support, Web Development and Telecommunications. This discussion is about function and not necessarily the reporting organization of the department.

Mainframe

The administrative systems for the university are purchased software provided by SunGard. These applications are housed on an IBM Mainframe and include the following:

- Student Information System (interfaces with Web for Students and Web for Faculty)
- Financial Records System (includes Purchasing System)
- Human Resource System (interfaces with Employee Self Serve)
- Loan Management System

Online CICS applications and web interfaces allow for real time data entry and data lookup but most processing in done by batch jobs in batch mode. Reports are created out of batch jobs.

In addition to the purchased administrative systems the Computing Center supports a few homegrown legacy applications, in house developed reporting and extracts to feed various applications that are external to the mainframe environment.

Technology Support

This function supports the academic and administrative technology network required at ULM. Some areas covered are:

- Access to mainframe applications from across campus as well as from remote locations.
- ULM internet access
- Email services
- Access to server applications and data stored on servers
- Server maintenance and support
- The Help Desk
- The Call Center
- DBA services
- Technical services

Web Development

Web applications are becoming a vital part of what the Computing Center does. Web Development supports the following applications:

- Flight Path – an advising degree planning tool
- Text Book Ordering System – web system for ordering textbooks
- My ULM – campus portal application
- Assessment and Evaluation
- Go Print
- See http://wiki.ulm.edu/computingcenter for a complete list.

Telecommunications

This function supports telephone equipment and services across campus. The Telephone Office is located at the rear of the Clark Williams Student Success Center. Telephone support is available primarily thru calling extension 5555.

Mainframe Operations and Processes

Mainframe Production Schedule/Production Job Requests

The production job schedule requires coordination between Data Control, operation and the requesting department. Jobs become part of the production schedule in one of the following five means.

1. The job is on the "day of week" preprinted schedule to be run without any further request. (Must request not to run)

2. The job is on the semester (or month) calendar to be run without specific request from the department. Most departments will map out their needs and provide the Computing Center a semester or other logical time frame of projected processing requirements. Data Control will transfer the jobs from the various user departments' schedules to the monthly processing schedule.

3. The job is on a periodic (daily, weekly, or monthly) request sheet completed and submitted by the requesting department on the day that it is processed.

4. The job is requested by submitting an individual job request that was specifically designed for the job.

5. The job is requested by submitting a "laundry list" type job request sheet which has the requested items checked.

Performance Monitoring

Information reflecting various measures of system performance is routinely captured for on-line and batch analysis. The systems and operations staff interactively monitors system performance in order to assure optimum use of resources.

Monthly performance reports are run for further analysis by the system staff and the Director of the Computing Center. These reports show a summary of programs executed, CICS transaction by user ID, CICS utilization and response profile that show volume of transactions, number of I/Os, and CPU cycles. Similar information is collected and reported on the academic computing system.

In addition to the utilization information, data is also captured and analyzed pertinent to the services and interventions requested of and performed by the ULM Computing Center.

Information compiled and circulated within the Center includes:

- Weekly Status of Programming work orders
- Weekly Outstanding Problems reported
- Monthly training log

Other items that are routinely reviewed by the Operations Manager, the Systems Manager, Applications Manager and the Director of the Computing Center include:

- Console operators run job logs
- samples of request sheets
- critical outputs from jobs

Backup and Recovery Procedures

IBM System Backups

In an effort to provide a reasonable amount of backup security on the IBM system at ULM, the following backups are generated on a weekly basis:

Monday -	Full volume backups of all volumes
Tuesday - Friday -	Incremental backups of all volumes

One month (4 generations) of full volume backups are kept for each volume. Two weeks (8 cycles) of incremental backups are kept for each volume. The exceptions are volumes ULMCAT and ULMLG1. Full volume backups of these two DASD volumes are made every night.

A second copy of each volume backup is made every morning. This second copy is made from COPY1. To facilitate full system recovery in the event of a disaster, all COPY1 backups are transported to an offsite vault.

At the end of every fiscal year (June 30) a set of full volume backups are made permanent and kept in an offsite vault. The End-of-Fiscal-Year backups are retained for at least five years.

Volumes which might contain confidential employee and student information are encrypted.

Due to the nature of the administrative systems at ULM and the need for synchronization of data within these systems, when making batch updates, application systems generate independent backups to simplify restoration, if the need arises.

Disaster Recovery

Disaster Recovery Plans for the University are kept in electronic form on a local server. Hard copies of the Computing Centers disaster recovery plans are kept in the offsite vaults. Disaster recovery testing is done minimally twice a year for the mainframe.

Application Data Backups

Backups of application files are made at key points during the daily production cycle to facilitate recovery in the event of an ABEND or other problems that require rerunning jobs or cycles.

- Online files for all applications are backed up after they are closed for batch processing and before daily batch processing begins. They are backed up again at the end of batch processing and before files are reopened for online processing.
- Online files may also be backed up between processes such as daily, weekly and monthly processing or any time online files are updated.
- Transaction files are backed up as part of the batch process.
- Applications work files are backed up at various points to facilitate easy restart or rerunning of processes.
- Monthly, quarterly, fiscal year end and calendar year backups are made of key financial files, payroll files and student loans.
- Fiscal year end and calendar year backups are made of SIS files.
- Quarterly, fiscal and calendar backups are made of Inventory files.

Application Data Restores

Restore jobs exist within each application for restoring productions files from backups. These jobs will restore an entire application to the point in time that the backup was made.

Mainframe Standards and Codes

Mainframe Definitions

Application Code – three position alpha codes used to identify an application. Currently defined application codes are:

ACT– ACT Testing
FRS – Financial Reporting System
HOU – Housing
HRS – Human Resource System
INV – Inventory System
LMS – Loan Management System
PAS – Pure & Applied Science advising system
SIS – Student Information System
TES - Test Grading
VEH – Cardinal Ticket Track
WHI – Warehouse Inventory
GTS – Graphic & Technical Services
ZSS – SCT Z Support Software

Sub Application Code – a one-position code used in names for job and programs that identified a sub application. Codes are assigned by SCT for their software.

A-Base System
G-Budget in FRS
B-Billing & Receivables in SIS
D-On Course
E-Payroll & Human resources
F-Financials
H-Housing
N-LMS
M-Admissions
P-Purchasing
R-Student Records
S-Financial Aid
T-Fixed Assets
V-Accounts Payable

Library Code – A code used for naming libraries. The Library Code will have a corresponding Application Code but not all Applications have corresponding Library codes. Some Library Codes may contain multiple Application Codes. Libraries will hold elements for one or more application.

UCC – Legacy applications developed in-house
FRS – Financial Reporting System
HRS – Human Resource System
LMS – Loan Management System
SIS – Student Information System
ZSS – SCT Z Support Software

Environments

- **Production Environment** – All libraries, screens & files used for production. Changes to this environment should be moved from the Primary Test Environment after testing has been completed.

  In emergency situations where quick changes are required in the Productions Environment, changes may be installed without first going into the Test Environment. The modifications should be installed in the Test Environment as soon as possible.

- **Primary Test Environment** – All libraries, screens and files used for testing. The goal will be to keep the primary test environment a mirror of production except for current changes that are being tested before they move to production. The Primary Test Environment should contain a test version of all production JCL and datasets. The JCL should point to the test versions of all datasets.

  SOURCE, BLINKLIB, CLINKLIB, CLIST and PARMLIB should contain only members that have been changed and are being tested. In the JCL the test libraries will be concatenated before the production libraries. Changes in the Production Environment should be moved to the Primary Test Environment for testing before being moved to production. Once changes have been moved to production the elements should be removed from the test libraries.

  Production jobs should never pull elements from test libraries.

- **X Test Environment** – All libraries, screens and files needed for testing or restoring an application to some point in time for reporting or problem resolution. This environment will be used for special test needs that do not fit in the Primary Test Environment. Applications within the X Test Environment may not always be in sync due to changes for multiple applications being worked simultaneously. These changes should move to the Primary Test Environment for Integration testing before moving to production.

  Production jobs should never pull elements from the release libraries. Only one set of test libraries for each Library Code will be supported. When a new release comes in, the prior release should be archived before loading out the new release.

Levels of Testing

- **Unit Testing** (UT) – testing changes to a single element (running the one step that involves the change).
- **System Acceptance Testing (SAT) or Integration Testing** (IT) – testing changes to one or more elements by running entire job streams including feeds from and to interfacing systems.
- **User Acceptance Testing (UAT) –** Testing done by user to confirm system changes have been made as requested or to become familiar with a new release of software. User testing could be done in the Primary Test Environment or the X Test Environment. At this point no separate User Test Environment is planned.

Procedures for Mainframe Application Programmers

Change Control Procedures

Change Control Auditor

The Change Control Auditor is someone other than the programmer making the changes. They should review changes before they are moved to production. If the one making the changes is not the primary support for the system, the primary support should audit the changes before they are moved to production. If the primary support is making the changes, then the backup support, program manager or another programmer would review the changes before they are moved to production.

Change Control Process

1. Obtain written documentation of requested changes. This may come from the user requesting the change or in the case of purchased software from the vendor.
2. Write up functional specifications for user request. Users should review functional specifications and give written confirmation that requested changes are correctly represented in functional specifications.
3. Make a list of all elements to be changed (programs, copybooks, parameter cards, JCL etc). If changes are coming from the vendor, review in-house code to identify additional elements that must be changed along with vendor changes.
4. Check with other programmers to make sure no one else is working on elements to be changed.
5. Write up technical specifications for changes and review these with the Change Control Auditor.
6. Make changes and complete unit testing in test.
7. Once all changes have been completed perform system testing.
8. Work with users to insure adequate UAT is completed.
9. Work with Change Control Auditor to review changes before installation.
10. Send email to Programmer Group and users to alert every one of changes.
11. Move changes from TEST to PROD.
12. Be available the first time jobs run in case there is a problem with your changes.

Testing Procedures

- Written Test Plan
- Unit testing
- Integration Testing
- User Acceptance Testing

Release Procedures

- Backup current Release Region to tape. Include backup date in name of tape.
- Backup ZSS because elements in ZSS are sometimes updated in a release to other applications. If your changes had to be backed out, ZSS would also need to be restored.
- Load new release into Release Region
- Make all needed changes before installation
- Move to TEST for SAT and UAT
- Move from TEST to PROD
- Store TOS in folder on server under TOS number and date.

Project Documentation

Functional Specifications - Description of proposed functional changes. This document should focus on communicating changes in terms that can be understood by user community.

Technical Specifications – Technical description of proposed changes to be used primarily by the programming staff.   They should include list of all elements that are to be changed.

Project Schedule – Should include milestones and/or deliverables with projected dates and names of person/areas responsible for task. A Project Schedule template can be found on Mainframe Programmers\Shared Files\Forms Templates

Programmer Security Access

- Program Manager and all programmers should have view access to all libraries and files.
- Program Manager and all programmers should have alter access to all test files and all libraries.
- Production Files - Programmers should not have access to productions files. See security sections for further discussion on security of production data.

Application Documentation

Two folders have been created on the programmers shared drive for storing application documentation. "ULM Mainframe Documentation" is used for storing all documentation on mainframe applications. "ULM Non Mainframe Documentation" is used for storing documentation on applications that are not on the mainframe. Each of these folders contains sub folders for storing various types of data.

Vendor Documentation – The latest electronic version of all vendor supplied documentation should be available in the documentations folders on the programmers shared drive.

In-House Documentation – All support notes, documentation, instructions etc. that have been developed at ULM should be available in the documentation folders on the programmers shared drive. This would include anything that could be helpful to someone supporting an application.

Recovery Documentation – Each application should have instructions for recovering data and restarting jobs/cycles in the event of problems. These instructions should include the names of jobs for restoring backup files or fixing data for restart. Recovery documentations should be stored in application subfolder under a file name that includes RECOVER as part of the name.

On Call Responsibility

A first and second call has been designated for each application supported by the Applications Programmers Group. This list is stored on the programmers shared drive as "Abbreviated Application Support List" and is shared with the operations area and others across campus that needs this information.

A second more comprehensive list of all mainframe production jobs has been developed for use within the Computing Center. This list includes a first and second call for each job and assigns responsibility to the primary and secondary programmer with the application area of that job. All members of the mainframe programming staff are assigned responsibilities on this list. This list is stored in the "ULM Mainframe Documentation" folder as "Combined Job List".

Programming Standards

- Document all changes at the top of programs and JCL. Include what was changed, who made the change and when it was made.
- Use comments generously through out coding to explain what code is doing.

Technology Support Operations and Processes

Network Procedures

ULM Monitoring System

The Computing Center employs several monitoring systems to monitor critical systems and processes. When an alarm is triggered, the proper Computing Center staff is notified and will respond promptly.

Servers

Server Backup/Disaster Recovery

Server Backup and Disaster Recovery procedures are documented elsewhere. Those documents can be located on \\spock.ulm.edu\ucc\shared\disaster recovery

ULM Server Patches

The Computing Center will adhere to policy set forth by the state OIT department regarding recommended and required patches to be applied on servers.

Call Center Procedures

Receiving Calls

When a call is taken, answer the phone with the greeting, "Hello. University Computing Call Center. May I help you?" Record the callers name, email address, and telephone number.

Directing Calls

The following steps should be taken to determine the nature of the problem. When dealing with people off-campus preface all phone numbers with a "342" prefix.

Step One:
Determine whether the call is related to internal computing center operations or another campus resource. For transfer calls use the list under **Transfer Areas** below to determine how to route the call. Transfer the call to the other resource using the telephone transfer command on your telephone. See **Transferring Calls** below.

If you are unsure where to direct a call, create a ticket so there will be a record of the request. Those techs who view the tickets can make the determination if the call needs to be moved or if other people need to get involved.

Step Two:
For non-transferred calls, determine which Computing Center help entity should receive the call. Using the Helpdesk software, enter the ticket for the appropriate department. Obtained the following information from the customer:

- Customer Name
- Customer Email
- Customer Location/Office
- Customer Phone (where they can currently be contacted)
- Location of the problem (lab, office, Smart Classroom etc.) Note - the area of the problem may not be the area where the customer is usually contacted.
- How long the customer will be at the current location
- Type of technology being used (Windows, Macintosh, Smart System, etc.)
- Description of the problem
-

Try to be as accurate as possible. See **Interviewing the Customer** section below for further instructions.

Call Transfer Protocol

When a call comes into the center, it must be either transferred to a party that will directly deal with the issue or a ticket must be created for later review. Use the list below to determine whether to direct the call or create a ticket. If unsure about a call, make a ticket!

Inquiries to Specific Staff Members
Direct calls to staff member's telephone (use department telephone list)

General Faculty Members
Use the ULM Search utility (http://www.ulm.edu/- search quick link) to obtain faculty name

Specific Department
Use the phone list and give the customer the phone number

Transferring Calls

The button used to transfer a call will vary by telephone set. On some telephones there is a "FLASH" or "TRANSFER" button. On other telephone you must use the "Hang Up" switch. To transfer a call, briefly press which ever button or switch your telephone set uses and dial the 4 digit extension where the call will be transferred. Hang up the phone after dialing. Use the "Transfer Log" sheet and make a tally of each call transferred and to whom it was directed. Write in special persons or departments not usually found on the tally sheet and update the transfer count for them.

Locating a Customer Email or Phone Number

From the ULM home page (http://www.ulm.edu/) click "**Search**", found in the upper right hand corner of the home page, to display the search utility. The search utility will allow you to search for an individual using first and/or last name or by department for faculty and staff. It will also allow you to search for the person's name on the web

Search by Name

Enter the name in the top box of the search utility. Click the button to signify whether the customer is a “student” or “faculty/staff” member and submit the entry. All entries that match your search criteria will be displayed. Scroll down until the correct name of the person is found. An email and phone number should be listed next to the name.

Search by Department

Click the drop down arrow in the second box. Select the department and submit the entry. All members of the department will be displayed.

Interviewing the Customer

Ask questions and get answers. Record all pertinent details in the call ticket.

Make sure you correctly understand who is calling and making the request. Make sure you understand the nature of the problem. Make sure you know to whom the call should be directed. Repeat the name of the intended recipient to the caller to be certain.

You should ask the customer questions that will tell you the whole problem. Ask questions like:

- How long has this problem been occurring? Has anyone in particular helped you with the specific problem in the past?
- How did it work before the problem and how does it work now? What has changed?
- When did you first notice there was a problem?
- What program are you using when the problem happens?
- What does the error message say exactly?
- Can you recreate the problem if asked?
- When are you are available for our Techs to contact you

Get correct information. Repeat back and verify the information as necessary.

*Be polite***.**

Policy Notes

Customers Expected Availability

In order to maximize the time of Computing Center personnel and insure optimal support across campus the Computing Center request that customers be available to let Computing Center personnel into their offices. This eliminates the time consuming task of hunting down and returning office keys. Having the customer available also eliminates any problems of getting past screen saver passwords or other security features that may be installed on the equipment. The customer should also be available to answer any question that may arise during the evaluation and resolution of the problem.

Customers Should Report Their Own Issues

The Computing Center requests that problems be reported by the individual experiencing the problem. Computing Center personnel often need to speak with this person to get specific details. They will also need to coordinate a time when the individual will be available to open their office (see previous note).

Dorm Lab Problems

A ticket should be opened for all Dorm Lab issues (paper, hardware issues, etc.).

Dorm Issues

For dorm area issues not related to a dorm lab (rooms, etc.), the caller should be directed to contact the Residence Hall Association or their local Residence Hall Assistant (RA)

Wireless Internet/Road Runner is provided by Time Warner. Student should contact them or their RA for additional assistance.

Surveys Requiring Login

Students should login to surveys using their CWID and PIN. The CWID may be obtained through ARROW. The default PIN is the month and full year of their birthday.

Faculty should login to surveys using their CWID and PIN. These should be the same as they use for WebCT, Web for Faculty (when entering grades) or Employee Self.

ULM employees with lost a PIN or CWID should contact the Human Resource Department.

Students with a lost PIN or CWID should contact the Registrars Office.

Helpdesk Software

CallTech Software

The call technician should use the Mozilla/Firefox tabbed browser to open several tabbed windows. They should use one of these windows to open the PMOS Helpdesk (http://computersos.ulm.edu/).

In another of these windows they should open the ULM search page. This will allow them to easily move back and forth between these software areas.
These two software areas are the ones most commonly used and need to be readily accessible.

Logging on

Log on to the Helpdesk software by accessing the log on page at http://computersos.ulm.edu using a web browser such as Mozilla or Internet Explorer.

Creating a Ticket

1. Enter Customer Information.
    a. At the Customer Lookup Table click the drop down arrow to choose the customer's name. Entering a letter of the alphabet will cause the customer list to advance to names beginning with that letter. Select the customer's name and click "submit query". The form that is displayed should be pre-populated with information on the customer.
    b. If you cannot locate the customer's name, click "Submit Query" without choosing a customer record. A blank form will be displayed where information on the customer may be manually entered.
    c. If the customer record was selected previously, most of this customer information will already be filled in. Verify the accuracy of the contact information with the customer to ensure everything is correct. If no record was selected, get the information from the customer and enter it manually into the form. The following information should be collected:
        i. Name - customer actual name
        ii. Email - customer's email address
        iii. Building - the building where this call originated
        iv. Room - the room where the call originated
        v. Phone Number - the customer's phone number
        vi. Availability – when customer will be available for technician to visit.
        vii. Title – customers title
        viii. Customer Area – customer's department or area of responsibility
        ix. Tech Code - the code for the operator taking the call; every operator has a different Tech Code.
2. Enter Equipment Information – For equipment problems or malfunction, enter LA Tag, Serial # and Dell Tag # if possible.
3. Enter Department – Based upon the nature of the call choose a department from the drop down box for department. Most entries will be for the Helpdesk.
4. Enter Subject – a brief description of the problem.

5. Enter Message - a detailed description of the problem
    a. It should have the correct information
    b. It should contain detail information about the problem. See section **Interviewing the Customer** for guidance in gathering information from the customer.
    c. It should be comprehensible; any average reader should understand the general nature of the problem
    d. Should you question the comprehension of your ticket, get a fellow worker to proofread it for you.
6. Enter Priority - the relative severity of the problem. Assume Low unless otherwise instructed.

Note: the ticket software will require an email address in the correct email format (username@server.domain).

The software will display the ticket number upon successful creation of a ticket.

The Four Line Rule

Every call ticket needs to have at least four lines of content in the body. By requiring four lines, every Calltech is challenged to get more complete information from the customer on the phone. Phone communication is difficult; ambiguities arise when information is incomplete or unclear. This rule hopes to make things clearer by requiring the Calltech to ask for enough information to fulfill this four line requirement.

Customers Requesting Tickets be Made

Make a ticket for any customer that requests one. Even if you need to transfer a call to another entity, all requests for a ticket should be honored without question.

Tech Code

The tech code is a unique identifier given to all call center and tech personnel. It should be included on the ticket form to show who took the call. The code is used to reflect the person in the position without identifying the name to the customer. Internally, technical staff will know about the code and who is using it.

Ticket Priority

Use low priority as default for all calls. Use medium priority for calls that need more immediate attention but affect a small number of people such as a smart classroom problem. Use high priority for those instances when the problem is immediate and affects a large number of people (email server is down) or when specific VIP requests are made.

If anyone questions why their call ticket priority is listed as LOW, please inform them that the call priority field is not really used. Calls are handled as best we can according to personnel on hand, available schedules, and ability to provide service. The field may be set to any value because the ticket will be treated the same regardless of how the priority is set. Since the software defaults to Low Priority, we usually keep it set there.

Rapidity of Service

There is no guaranty that any problem will be solved in any specific time frame. We attempt to handle all problems as they arise and often this means that some customers must wait until an available tech becomes free.

Any customer who calls demanding to know why a ticket has not already been handled should be reminded that every ticket is not handled immediately. You may offer to make another ticket for the customer if that seems to calm them.

Customer Availability

Customers should be asked about when they will be available for our techs to intervene. Many places on campus are locked and inaccessible to us. We often need somebody to be onsite to open doors and get us into places where we can be effective.

Please remind customers that providing a time of availability does not mean that a tech will be available at that time. Usually, the customer will be contacted prior to a service call to ensure the time and place are correct.

Involved Agents

If a customer calls about an existing problem that a tech is handling, please find out who has been providing assistance. This information may make future interventions more successful since we can question whoever was involved.

Problem Calls or Irate Customers

If a customer becomes angry or abusive:

- Remember that in most cases, the customer is frustrated and does not mean to take out those frustrations on you; Remind the customer that you are attempting to help and they need to be calm when speaking to you;
- Ask customers to speak slowly and clearly;
- If the customer continues to be abusive, warn him that you will need to terminate the call if abuse continues;
- If abuse continues, indicate that the incident will be reported to a supervisor, and then terminate the call.

Abuse consists of: customers yelling, screaming, cursing, name-calling, banging the phone, or other extreme behaviors designed to enrage, humiliate, or harm workers attempting to help.

Once the call has terminated, if the incident needs to be reported or the customers requests supervisor involvement, create an email directed to Danny Hutton (hutton@ulm.edu). In the email, explain the incident. Give all available details (customer name, email, time and date of incident, circumstance, attempted resolution, etc.) The supervisor will investigate the incident and may contact you later for additional information.

A Specific Tech is Not Available

If a call comes in for a specific tech that is currently unavailable, please encourage the customer to leave a voice mail message on the recorder so that the tech can return the call as soon as possible. Offer to make a ticket for the customer on the chance that some other tech can intervene and provide service.

Transfer Areas

Info
Blackboard Inquiries, Passwords, Email, Tribe Accounts

Requestor needs to appear in person for reasons of security and identity confirmation

Contact:
Helpdesk Office:
Admin 1-96
Email: helpdesk@ulm.edu Phone: 5031

TaskStream
Portfolio System for Education Majors

Contact:
Dr. Thilla Sivakumaran
Office: Strauss 266
Email: sivakumaran@ulm.edu Phone: 1270

Arrow
For student registration, drop/add, viewing grades, paying tuition and fees, etc

Contact:
Registrar
Phone: 5262

Employee Self Service
Employees view check stubs, employment information, vacation hours, sick time, etc.

Contact:
Human Resources
Phone: 5140

CICSPLUS - Logon, password, access information

Contact:

Ruth Nichols (Tu-Th)
Phone: 5024

Connie Reeks
Phone:5036

CICSPLUS - Screen access

Cannot access screen XXXX

Contact:

Janice Guyton
Phone:5038

Connie Reeks
Phone: 5036

Software Requests or Checkout

Contact:

Helpdesk/Sheau Yun Choo
Phone: 5031/5032

Exchange email or calendar issues

Cliff McManus
Phone: 5019

Flightpath

Contact:

Joe Mansour
Phone: 3370

Special Applications

(Occasional not constant)

Student Elections
Faculty Evaluations

Contact: Call Center

Other Information Areas

General ULM Information
ULM Web Page - Quick Links
http://www.ulm.edu

Faculty/Staff or Student
Phone or Email ULM
Web Page - Search Tab

Antivirus Software and info
http://antivirus.ulm.edu

UCC Phone List

Web Application Programming Operations and Processes

Web Standards and Practices

New Code migration procedure

- All new code additions or modifications are done on a (non-production) development server. This applies for both database and web servers.
- The new code is tested before being moved to production.
- When applicable a staging server may be used to further test programs that are large in scope and/or require community testing or feedback.
- Once testing is complete and the code has been stabilized it is moved to a production server.

Web Application to Database Access Controls

- Access to production database server restricted to authorized users from a specified location (IP).
- User accounts are created for specific databases based on the required privileges for the particular application's user(s) requirements.
- ALL db connection functions used by custom applications are stored on the web server, in a non public directory, in the WSconnections file. In order to access the required data the custom application must:
    1. Insert the include(../WSconnections) statement.
    2. Call the specific db connection function. (Connection information is stored in the function, rather than within the application itself)
    3. If function is accessed properly then permission to data granted to the application (only).
- Connection functions will not to be hard coded directly into a web application.

Custom Web Application Templates

- All script Output is collected into a $pageContent variable
- Once all form processes have completed, the data contained in $pageContent is passed to a separate template file (rather than echoing or printing out the template each time).
- Templates are stored in the ws_templates directory of the webserver. The specific template must be called using the php "include" or "require" command.

- There are currently 3 standard templates which all *new* applications will be required to use: modern_template_1, modern curves, and survey_template_1. At any point any of these templates may be updated.

Web Form Input Validation and Processing

- User provided input is validated and cleaned from GET and POST variables. This is done for security purposes in an effort to reduce the risk of hacking.
- All user logins are synchronized with Arrow / Web-for-faculty logins.
- Passwords are stored in an encrypted state, not clear text.
- CSV files (and other output files) are created dynamically, and not left on the web server. This is method is used to prevent unauthorized users from accessing data stored in a CSV file
- Most applications should contain some basic logging functions including IPs and date-times. This is done in an effort track unauthorized or inappropriate use of the application.
- Backups of development work are made nightly by an automated script and transferred to another server (sirius). Development backups are kept for a period of 1 week before being overwritten.

Security of Data and Computing Resources

System Security/Confidentiality of Information

ULM faculty, staff and students who use ULM's computing resources must be sensitive to issues pertaining to system security and confidentiality of information. With ULM's hookup to Internet, the need for security awareness has increased more than ever. With greater availability comes added responsibility. Not only can a user of the ULM systems access local data but, via networks, data and systems throughout the world. Anyone (faculty, staff and students) accessing these systems has a responsibility to the University and to other users to see that these facilities are used in a proper manner.

Only properly authorized and approved persons may access network or computer facilities. Proper authorization is provided by Computing Center staff in the form of an 'account', 'id' or 'sign on' issued in the name of the authorized person. Users are responsible for all activities that occur through an account that has been issued to them. By applying for and using an account on University computer systems, a person agrees to abide by the following statements. These statements are listed on the 'Application for Accounts' and are applicable to all computer resources at the University.

- I will use the ULM Computing Center facilities for purposes associated with my official duties or studies at the University, only.
- I will not allow other persons to use my account.
- I understand that I have an obligation to protect University hardware, software, and data. I will not attempt to gain access to accounts, data or systems for which I have no authorization.
- I understand that abuse of equipment or violation of security will result in loss of privilege to use the system and that serious offenses will result in more serious disciplinary action.
- I understand the ULM Computing Center is co-owner of all files on the system and has all rights to those files.

Users may not permit other persons to access a network or host computer via their account. If you believe that the account has been compromised by another party, you should report this concern to the Computing Center staff immediately.

It is important that all users understand the Computing Center is co-owner of all file(s) on University computer systems and accordingly has all rights to its files. From time to time, it may be necessary for Computing Center staff to access individual user file(s) to provide system maintenance or user support. The Computing Center will make every effort to minimize this type of access, but due to the nature of its services, it is inevitable that some access of this type will be required.

Due to the nature of an individual's work assignment and the information which is stored on ULM computer systems, employees (faculty, staff, and student workers) may have access to information which is private and confidential in nature, i.e., grades, financial information, payroll information, etc. It is the responsibility of people who have access to this type of data not to disclose this information except on a "need to know" basis.

It is the shared responsibility of Computing Center staff and the department that "owns" the data to insure that information stored on University systems is protected. The Computing Center provides the access security software. For the IBM mainframe that software is RACF (Resource Access Control Facility). The head of the department that owns the data or their designated representative will determine the level of access issued an individual. For example, the Registrar will determine who may access student information. The Controller will determine who may access financial information, etc.

Adhering to the following guidelines should facilitate proper system security.

- Memorize your password(s). DO NOT write passwords down and post in easy to find locations. If you must write a password down, do so in a discrete manner and keep in a secure location.
- Do not share your password with anyone not even someone from the Computing Center. If someone needs access to your device, (ex. to verify that it works) log on for them. If you ever receive a call from anyone asking for your access code in order to verify something, require them to come to your office and verify the process in your presence.
- If an unfamiliar person wants to use your device, be certain to verify their identity and whether they have authority to use the system. If you are currently logged on to a system, log off before allowing them on.
- Do not leave your device unattended and logged on in an area available to unauthorized users. If you must leave for an extended period and there is a chance someone can access your device who should not, log off.

- If you suspect that someone knows your password, set a new one before your data can be compromised.

Sensitive Data on Portable Media

Sensitive data stored on laptops, diskettes, CD, DVD, tapes, jump drives, or other portable media should be encrypted and password protected.

Paper reports containing sensitive data should be protected and when no longer needed they should be shredded.

ULM Firewall & Static IP Addresses

The ULM Campus is protected by a redundant firewall system that both protects the campus from the outside world and also protects servers that are on the DMZ network. Requests for firewall rule changes are to be made via the Helpdesk System. Requests can be made for static IP addresses and will be reviewed by the Computing Center for approval.

ULM Passwords

The Computing Center will adhere to policy set forth by the State Office of Information Technology (OIT) department for password management.

ULM 3rd Party Server Access

When an outside entity/company/vendor requires access to a ULM server resource the ULM department they are working with must request this access. Someone in the department should contact the Computing Center Server Administrator or open a ticket with the Help Desk requesting access. When approved, the access will be temporary (no longer than 24 hours) and monitored by Computing Center staff. Any violations to this policy will cause their access to be denied.

Acquiring Security Access to ULM's Mainframe Applications

Most applications supported by the Computing Center require a user to validate their identification and rights to access the application. This is generally accomplished by the use of one or more sets of IDs and passwords. This section is intended as guidance to anyone needing to establish access rights to an application. Security access to the following applications is covered in this section:

- TSO - Time Share Option
- SIS – Student Information System
- FRS – Financial Resource System
- HRS – Human Resource System
- LMS – Loan Management System
- Email – Spock account
- EPrint - Electronic Report Storage

The following information should provide guidance when requesting user accounts. The ULM Computing Center maintains various security forms that may be found on the ULM web at http://www.ulm.edu/forms/#anchor259518 .

Pulling these forms from the web at the time they are used is recommended. This will insure that you have the most current form and will facilitate a faster response to your needs. Please discard any old forms you may have in your department. Completed forms should be submitted to the Computing Center, Administration Building 1-98, unless otherwise instructed. Forms may also be faxed to 5018 unless otherwise instructed.

The following instructions should help University employees understand how to request the security authorization needed to do their jobs.

Definition of WEB Security Forms

Information is listed below on the various university access forms that are available on the **web.** These forms require the employee's signature as well as approving signatures from the employees Dean/Department Head/Director. Some also require an approval signature from the department responsible for the data being accessed. The employee is responsible for getting their Dean/Department Head/Director's signature on the form. The Computing Center will obtain any additional signatures that are needed.

The required forms should be printed, filled out and routed to the Computing Center in Administration Building 1-98. Once all required signatures are obtained and the requested access is set up, the Computing Center will contact you with information about User IDs, Operator IDs and passwords.

Listed below are the University Access Forms along with a brief description of each.

Security Access Application **-** This is the basic form required for all new employees requesting access to mainframe applications, email or ePrint. It must be signed by both the Dean/Department Head/Director and the employee. If generic access to an application has been defined for the employee's position, requesting access to the application on this form will cover the set up of that generic access.

Security Access Change – This form is required if an employee has changed departments.

Security Access Termination – This form should be used when an employee is terminated or leaves the university.

FRS Account Access (Controller's Office) – Access request list for **F**inancial **R**esource **S**ystem screens needed only by employees of the Controller's Office. This access requires the approval signature of the ULM Controller.

FRS Account Access (non-Controller's Office) – Access request list for FRS screens needed by employees that are not part of the Controller's office. This access requires the approval signature of the Controller.

HRS Account Access – Access request list for **H**uman **R**esource **S**ystem screens. This access requires the approval signature of either the Controller or Director of Human Resources.

LMS Account Access – Access request list for **L**oan **M**anagement **S**ystem screens. This access requires the approval signature of the Assistant Controller for student account services.

Purchasing Access – Access request lists for Purchasing System screens. This access requires the signature of the Director of Purchasing.

SIS Account Access – List of request forms for the multiple areas of the **S**tudent **I**nformation **S**ystem.

- Admission's Office – access request list for Admissions SIS screens. Requires the approval signature of the Director of Admissions.
- Billing/Receivable – access request list for Billing/Receivable screens. Requires the approval signature of the Head of Student Receivables
- Departmental – list of SIS screens that need only the approval of the Dean/Department Head/Director for inquiry access. Any update access to an SIS screen will require the appropriate approval signature.
- Financial Aid – access request list for Financial Aid screens. Requires the approval signature of the Director of Financial Aid.
- Housing – access request list for housing screens. Requires the approval signature of the Director of Housing.
- Registrar's Office – access request list for the Registrar's Office SIS screens. Requires the approval signature of the Registrar.

Explanations and Instructions

The following documents are provided on the web for additional reference.

- Accessing ULM's Applications – Brief instructions for getting on the Mainframe and into CICSPLUS applications. Limited instructions for Email and basic instructions for accessing ePrint.
- Acquiring Security Access – Explains how to acquire needed access.
- ePrint Instructions for FRS, HRS, LMS, SIS – Detailed instructions for each.
- Mocha Telnet for Windows XP – Instructions for loading Mocha Telnet for Windows XP.
- SIS Screen Cross Reference – Cross reference of SIS screens and SIS Account Access Approval list. Designed to help employees identify which access forms include the screens they require access to.

Generic Application Access Lists

A generic access is a predefined list of mainframe CICS screen that an employee will need in a particular position. These lists have been pre-approved by all the responsible parties. Employees requesting access to an application may be given access to the screens on the generic access list defined for their position without submitting additional security forms.

Generic access lists are subject to change as needs change. Changes are not necessarily retroactive. An individual's access will not automatically change when the generic access list is changed. Changes to an individual's security will require manual intervention. If an employee's access does not get updated after the generic access list has changed they can request and receive the update by contacting the Computing Center at 3333.

The following are some of the generic access lists that have been established.

- Academics – Screens that have been approved for access by all academic areas. This list consists of both SIS and FRS screens.
- Financial Aid Student Workers – SIS screens approved for access by Financial Aid Student Workers.
- FRS non Controllers Office Access – FRS screens approved for all non Controllers Office employees with budgeting responsibility. (Access to individual accounts is controlled by value based security which is set up by the Controllers Office).
- Purchasing with approval – Purchasing screens approved for anyone with approval authority for purchases.
- Purchasing without approval - Purchasing screens approved for anyone with purchasing responsibilities without approval authority.
- JPI Housing Student workers - SIS screens approved for student workers in Housing
- University Police – SIS screen approved for access by members of the University Policy
- JPI Employees – SIS screen approved for access for JPI employees in Housing
- Late Registration Student workers – SIS screen access for temporary workers who are helping with late registration.
- Student Success Center – SIS screen access for Student Success Center counselors.
- LACAP – SIS screen access for LACAP employees.
- Computing Center Tech Support – SIS screen access for Computing Center Technical Support personal.
- Library Circulation Desk – SIS screen access for personal working the library circulation desk.

Mainframe Access to Production Data

Production files should be modified in only one of two ways; through CICS transactions or by a batch job. Computing Center Personnel should not have access to alter productions files.

When a production problem makes it necessary for Computing Center Personnel to modify a production file they may be given temporary access to update the file in TSO. This should be well documented and the access should be removed as soon as the fix is in. If at all possible other methods of fixing the problem should be used. Access to production files is controlled through RACF security which is maintained by The Computing Center Security Officer.

Access to the system requires multi-levels of password sign-on security. Deans/Department Heads/Directors must determine whether or not each subordinate needs access and the extent of access and types of actions required. They must sign security forms submitted by employees in their organization indicating their approval of the access being requested.

Deans/Department Heads/Directors are responsible for notifying the Computing Center when an employee leaves their department. This allows the Computing Center to remove access from employees that are leaving the university. If the employee is transferring to another department their current mainframe access will be terminated. They will need to submit new security forms signed by their new Dean/Department Head/Director.

The RACF security system protects initial log-on to the system. This system requires a user to have an account established by the security officer. The user’s Dean/Department Head/Director must sign the application to the Computing Center security officer to establish the user’s account. This application form bears a security certification that must be signed by the applicant. The user must identify him/her self by entering a password to gain access to the system. This password expires automatically every 180 days and the user is forced to choose a new password. The system keeps track of the last five passwords used. The new password may not be one of the last five used.

See section “Acquiring Security Access to ULM’s Applications” for detailed instructions and forms needed to request mainframe access.

CICS Transactions

For an individual to gain read or update access to specific accounts, screens, or screen elements, approval is required by the supervisor responsible for those accounts (e.g., controller is responsible for FRS files). The individual must submit a Security Authorization and have a RACF account established before they can be given access to CICS. Computing Center personnel routes this form to the appropriate approving agent who authorizes the requested access. Once the requested access is authorized, the Security Authorization form is routed to the Application Programming staff to set up the second level access maintained within the SunGard product. Users are assigned a four digit user number and a password by the programming staff.

The Financial Records System also uses Value Based Security. This security controls the accounts a user is allow to access. The Controllers Office is responsible the maintenance of Value Based Security records within FRS.

Batch Jobs

Batch jobs may be submitted in one of several ways.

1. User turns in a run sheet to the Operations area of the Computing Center requesting a job be run. The Operations area submits the job.
2. User submits the job from a menu developed by the programming staff for their area of responsibility. User must be granted security access to their menu by the Computing Center security officer.
3. Jobs that are run at regular intervals, daily, monthly etc, are placed on a run list. The Operations area submits these jobs at the appropriate times.
4. Some users submit jobs using TSO. To run jobs the user's account, established by the security office, must be set to allow the user to submit a job. This account also controls which files a user may access and/or update using a batch job. Audit reports can be produced on jobs run by users.
5. Programmers submit jobs. Jobs that programmers submit must have a unique userid supplied by the security officer. Audit reports are run on all jobs that are submitted with that userid.

Terminating Access

Three levels of notifications exist for alerting the Computing Center when an employee leaves the university and should have their access terminated.

1. The departing employee's Dean/Department Head/Director should notify the Computing Center when an employee leaves their department.
2. Human Resources will send the Computing Center a copy of the HR Exit form of exiting employees who go through the exit interview process. Employees sometime depart without going through the HR Exit interview so not form exist to be sent to the Computing Center.
3. Monthly reports are run to identify employees that no longer have an active assignment record in HRS but still have system access. This process is designed to catch departing employees who were missed in the first two levels of notification. Missed employees are generally a result of employees that decide over the summer not to return for the fall semester.

Once the Computing Center is aware that an employee has left the university the RACF Security Administrator revokes their account. As a user must have a RACF account which maps to the SunGard application, this effectively removes all their access to the mainframe. In addition their application access is also removed.

Security of the Operational Area

Unescorted access to the printers and the tape library is limited to Computing Center operators and supervisors. Tape and disk files are kept in the operations area. Access to the area is limited to two doors that are normally locked and one entrance under surveillance by Data Control and Operations staff. Internally stored documentation is protected from unauthorized access by the RACF system. Keyless entry has been added so records can be created for Machine Room accesses. The main server area of the Machine room is behind locked doors controlled by keyless entry with access granted on a need basis.

ePrint Security

Reports are stored in ePrint within repositories. Security records from CICSPlus applications are used to control access to ePrint repositories. Groups within each repository further control who may view each report. Reports and users are assigned to Groups. A user may view only the reports that have been assigned to the groups to which he has been assigned.

Access to some financial reports is further controlled by value based security. A user will be able to view only the pages of the report that relate to the accounts that value based security allow them to access in FRS online.

The following is a list of production repositories and the application security used with them:

• Student Information System	Uses SIS security
• Financial Records System	Uses FRS security
• Human Resource System	Uses HRS security
• Loan Management System	User LMS security
• SCH Reporting	Uses SIS security
• Inventory Reporting	Uses FRS security

When the Computing Center is made aware that an employee has left the university all access they have to the ePrint system is removed.

Reports are kept on ePrint for two full years and then archived to CD/DVDs. Reports stored on CD/DVDs are encrypted and require the encryption software and a password for de-encryption. Two copies of the reports are stored at our offsite facilities and two copies are kept onsite. If an archive report is needed Computing Center personnel will take the encrypted volume to the user’s office and download the needed report to the user’s hard drive.

Arrow Security

Web for Students, Web for Faculty and Employee Self Serve use the same security file. The first time an individual is added to any of these systems they are assigned a Campus Wide Identification Number (CWID) and a default PIN. The first time they sign on to the system they are required to reset the PIN. They are also required to create a PIN question and answer. If they forget their PIN and can correctly answer the question they are allow to reset their PIN. A PIN cannot be reused if it is one of the last ninety-nine that the individual used.

Personnel in The Human Resources Department, The Registrars Office and Admissions have access to the ZEK screen where the PIN may be reset. Neither the PIN or the PIN questions and answer are ever displayed on a screen.

A flag may be set within Arrow to force a PIN change the next time an individual sign on to Arrow. Current plans are to force PIN changes once a semester in Web for Students.

In-House Web Security - Identity Management

All In-House Web Applications

All applications which require user authentication use the same user identifier (CWID and PIN) as Arrow, Web for Faculty and Employee Self Services. User information between Sungard Web Applications and In-House Applications is synchronized at least once daily, more often during heavy use periods (registration, advising, etc).

FlightPath

Faculty and Staff access privileges are assigned by the Coordinator of Advising Support. All undergraduate students are granted access to view their own records.

Textbook Clearinghouse

Deans and Department Heads privileges are assigned automatically. Other Faculty and Staff requiring administrative access are granted privileges by the Auxiliary Enterprises Coordinator.

MyULM

Students are granted access upon admission to the University. Faculty and Staff access is not yet available.

Assessment

Deans and Department Heads privileges are assigned automatically. Other Faculty and Staff requiring administrative access are granted privileges by the Director of Assessment and Evaluation.

Course Evaluations

Students are granted access upon enrollment in a class within the current term.

Elections

Students are granted access upon enrollment in a class within the current term.

ULM Policies

Deans and Department Heads privileges are assigned automatically. Other Faculty and Staff requiring administrative access are granted privileges by the Director of Assessment and Evaluation.

Server Security

Some server based applications that augment administrative functions of the SunGard comprehensive system are maintained by the University. These systems run as stand-alone entities, and communications to the mainframe system occur in batch feeds monitored by the user departments for completeness and accuracy.

The administrative processes on this system are further protected by several means of controlled network access. A pair of redundant connected firewalls protects the overall campus network from undesired Internet intrusions. Also this particular system/server subnet is allocated behind a more restrictive firewall connection that only allows campus access to the Mainframe via Telnet, FTP and Web4 processing. Since the Mainframe is only directly accessible from the Campus network, VPN access is provisioned to Faculty/Staff for off-campus access via their assigned LDAP login. The VPN connection provides access to most services on the Campus network that wouldn't normally be accessible via a regular Internet (off-campus) resource. Furthermore, there are no direct communications from the Mainframe environment to anything outside the Campus network.

Miscellaneous Information and Instructions

Data Sanitization

The purpose of this document is to provide information to assist university faculty and staff in matters pertinent to the transfer of computer storage media. It is not intended to replace or supersede detail policy and procedure of property transfer, but to provide details related to removal of security-sensitive data. This procedure is a joint venture between Computing Services and Property Control.

Process:

- The transferring agent will fill in appropriate forms to have equipment transferred from their department.
- Property Control will inform Computing Center personnel of need for data sanitization of media.
- Computing Center personnel will determine appropriate method of sanitization as per OIT Policy IT-POL-003 Data Sanitation and perform such process on the media.
- Transfer document will be updated to show method and date of sanitation.
- Document will be returned to Property Control for subsequent disposal and/or movement of property.

Guidelines to Assist with Purchasing Computing Equipment

The purpose of this document is to provide information to assist university faculty and staff in matters pertinent to the acquisition of computer hardware. It is not intended to replace or supersede detail policy and procedure of approving agents and affected departments governing the procurement cycle, but to provide a concise overview of essential steps that must be considered when planning or executing a computer related acquisition.

In order to move through the various stages of the procurement cycle, (from planning through procurement, receipt, and installation to daily operation and use), it is necessary to interact with numerous campus departments. Through proper planning and efficient coordination with other units, it is possible to streamline the process of procurement, installation, and operation of computer equipment.

1. Identify the need for the proposed acquisition

   The first step in deciding what type and model of computer you wish to buy is to define the function(s) that the proposed equipment will be required to perform. Consideration should be given to the connectivity to other equipment and availability of future upgrades.

2. Develop the technical specifications

   Personnel in the Computing Center are available to provide technical assistance in preparing specifications.

3. Physical facilities considerations

   The requesting department is responsible for determining if there are adequate electrical outlets, air conditioning, ventilation, and other physical considerations. The department is also responsible for providing a sturdy desk or table to hold the equipment.

   When connecting the equipment to a network, every effort should be made to use existing cables and/or wiring provided with the campus telephone system. If this wiring is not available or inadequate, the requesting department must provide detail specification and justifications for cabling. Any modifications or additions must be initiated by a work order to the Physical Plant.

4. Designate funds to finance the procurement

   Prior to issuing the purchase requisition, the department is responsible for ensuring that sufficient money is available in the account to cover the proposed acquisition. If you have any questions regarding this matter, contact the Budget Office.

   It is important to remember that the hardware price is not the only cost involved in this acquisition. Software purchases, user training, facility preparation, and future maintenance costs must be considered. Supplies such as surge protectors, diskettes, paper, and printer ribbons will also create an extra expense. Another consideration is the cost of future upgrades.

5. Follow the standard purchasing procedures

   Standard purchasing procedures for the University apply to the acquisition of computer equipment. A Purchase Requisition containing all of the specifications should be submitted to Purchasing. All requisitions for computing equipment are then sent to the Director of the Computing Center for technical review. Acquisitions over $100,000 must be submitted to State Purchasing in Baton Rouge.

6. Proper notification of receipt and request for assistance

Computer hardware should be shipped to the Customer Service area of the Computing Center. Here is will be checked out and loaded with the needed software. The Customer Service area will be available to assist you with the installation and setup of your equipment. If your new equipment has not been tagged, please contact Property Control immediately to tag the item.

Copyright and Compliance Policy

1. The unauthorized copying of any software which is licensed or protected by copyright is theft, and therefore unethical.

2. Failure to observe software copyrights and/or license agreements may result in disciplinary action by this institution and/or legal action by the copyright owner.

3. No University-owned computing resources should be used for unauthorized commercial purposes.

4. This University does not tolerate plagiarism, and it does not allow the unauthorized copying of software, including programs, applications, databases and code.

It is the responsibility of each Department Head to ensure compliance with these regulations. All departments will be subject to spot checks and state and/or vendor audits.

Remote Broadband Access for Staff

Acknowledging the advantage of having broadband access from home, the University is providing for joint payment of cost associated with such access for approved individuals.

Requisites: (All must be reviewed by Computing Services)

- An employee or their supervisor must show an advantage to the University for Broadband Access.
- Employee must have personal computer equipment, or have assigned ULM equipment, necessary to avail of broadband access.
- Employee must insure that antiviral software and personal firewall software is installed and current on equipment to be utilized (as per OIT Standard IT STD-019 Wireless Technical/Authentication).

Process:

- Employee fills out form ULM CC-8 Remote Broadband Access Request.
- Approval is granted by appropriate Dean or Vice President.
- Employee contracts with service provider to install broadband access.
- Computing Center Staff will provide telephone support in attempting to resolve issues. If they can not resolve such via telephone, services may be required of the service provider, at an additional cost to be paid by the employee.

Cost:

- Recognizing the fact that not all access from home will be work related, the University will only pay half of all related cost. (Exception being the President)
- To be reimbursed quarterly upon receipt of a copy of the bill from the provider.
- A copy of terms is to be provided to the Controller's office in order to verify re-imbursement amounts. (Rebates and/or waived installation fees must be considered).
- Installation fees can also be considered in the first quarter's reimbursement.
- Those employees with existing service plans that wish to be reimbursed for installation cost must produce an original bill. No monthly fees will be paid for services prior to this agreement.

Project Review, Recommendation, and Prioritization

The purpose of this document is to provide information to assist university faculty, staff, and subcontractors in matters pertinent to the acquisition of Information Technologies that must be supported by or interface with Computing Center facilities. It is not intended to replace or supersede detail policy and procedure of approving agents and affected departments governing the procurement cycle, but to augment these procedures and assure that new acquisitions blend with existing technologies on campus. It is vital that Computing Center staff be involved with selection of Information Technologies from the onset of this process.

In order to move through the various stages of the procurement cycle, (from planning through procurement, receipt, and installation to daily operation and use), it is necessary to interact with numerous campus departments. Through proper planning and efficient coordination with other units, it is possible to streamline the process of procurement, installation, and operation of information technologies.

These steps will be followed for new application development/acquisition. Please consult UCC at any point in the processes for assistance and clarification of your request.

1. Submit a plan document to the Computing Center Director for review. This document should provide basic information technology concerns such that UCC staff can perform an evaluation of compatibility.

2. UCC conducts adequate research to determine product requirements and availability.
    - Can the UCC assist with or create similar applications in-house?
    - Is a comparable "open source" product available?
    - Is a similar product already in use at ULM?
    - How does this product or idea integrate with existing ULM Technology resources?
    - What levels of training may be required?
    - Can server resources be housed in the UCC Sever room (preferred campus location) and/or can product co-exist on UCC virtual server facilities?
    - Is off-site hosting possibly the best solution for this resource?
    - Does sufficient network bandwidth exist to support this application?
    - How is security controlled via this application?

- Will environmental facilities require upgrading to support this application?
- Who and how will this system be backed up and what level of disaster recovery is available?
- Will there be a need for data sharing with other campus facilities and if so how is that to be accomplished?

1. Product must be ODBC (open database connectivity) compliant and therefore capable of working in one or more databases supported by the UCC staff.

2. Once the plan has been evaluated by UCC it will be presented to the Information Technology Review Panel (ITRP)* so that:
    - An assessment can occur of project validity.
    - Determine that adequate thought has been given to future maintenance and support requirements.
    - Determine that project cost is reasonable and complete.
    - Assurances provided that it can co-exist with other ULM applications.
    - The rest of the campus becomes aware of the application and the potential usefulness campus-wide.
    - Determine the specific Network and Server resources required. **NOTE:** Your application demands could negatively impact Network performance and/or Server resources requiring other resource enhancements.

1. At this point, approximate timetables are created to view placement of proposed application into existing staffing loads. This will dictate how soon the application can be made available (in-house design and/or 3rd party). We will provide as accurate an estimate of installation as possible; however, the Administration reserves the right to override the scheduling of a project if in their opinion other systems are more critical to the needs of the University. If this does occur an updated schedule will be provided.

2. Given this information the Requestor should then proceed with necessary steps toward procurement and/or grant submittal.

3. Once procurement is initiated, anticipated installation data is to be communicated back to UCC so that an official placement can be secured within UCC scheduling.

* In conjunction with the implementation of this policy an Information Technology Steering Committee has been formed. This committee is responsible for making recommendations to the Administration on IT directions for the campus. A subcommittee of this group (Information Technology Review Panel (ITRP)) is to be charged with reviewing all IT request, as provided by the Computing Center, for the campus and assuring that standards are maintained fairly.