Introduction ........................................................................................................................................ 4

SATS – Student Affairs Technology Services ................................................................................ 4

How to Get Technical Assistance ................................................................................................. 4

Equipment, Software and Security Standards .............................................................................. 5
  Password Security .......................................................................................................................... 5
  Administrative rights .................................................................................................................... 5
  Screen Saver Policy ....................................................................................................................... 5

Campus Systems ............................................................................................................................ 6
  OIT Account (a.k.a. NETID) ......................................................................................................... 6
  Administrative Computing Support Organization (ACSO) .......................................................... 6
  A & F Administrative Systems ..................................................................................................... 6

Training ........................................................................................................................................... 7

Requests for New Accounts and/or access to resources .............................................................. 7

Requests for Additional Hardware and Software ......................................................................... 7

General Guidelines for Use of SACL Technology Resources ....................................................... 7

  SECURITY EXPECTATIONS .......................................................................................................... 8
  INDIVIDUAL RESPONSIBILITY ................................................................................................. 9
  CARE OF RECORDS .................................................................................................................... 9
  ELECTRONIC MAIL ..................................................................................................................... 12
  DATA, COMPUTER SYSTEM/RESOURCE ABUSE ...................................................................... 13
  DEPARTMENTAL ADMINISTRATOR RESPONSIBILITIES .......................................................... 14

Employee Use of Social Networks ............................................................................................... 15

Remote Access .............................................................................................................................. 16

Laptops and Portable Devices ....................................................................................................... 16
  Synching portable devices to calendars ...................................................................................... 17

Website Standards and Guidelines ............................................................................................... 18
Appendix A – Data and Computing Policies, Standards, Procedures Summary for University Employees

Appendix B – Sensitive/Confidential Data

Appendix C – Campus and University IT Policies and Resources
- UMass Amherst - Data & Computing Policies & Procedures
- UMass Amherst – OIT – Policies
- UMass System – Data and Computing Policies
- University of Massachusetts Data Security Awareness and Education website
- OIT Resource – Data Security in Practice
- Dean of Students - FERPA
- FERPA Resources - Ferpa Tutorial
- OIT Services At A Glance

Appendix D – FERPA

Appendix E - Property Transfer Form
- Documentation of Movement of University Property to Off-Campus Location

Appendix F – Procedure for IT review of purchases
- University of Massachusetts/Amherst – Procedure for IT review of purchases

Appendix G – Web Site Guidelines/Standards
- SACL Acceptable Use Policy User Agreement
Introduction

The purpose of this document is to provide Student Affairs and Campus Life staff with information about the technology resources that are supported by Student Affairs Technology Services (SATS) within the Division; the guidelines for using these resources; how to get the support and tools you need; and expectations and responsibilities with respect to data and computer equipment.

The term “technology resources” means hardware and software systems provided by Student Affairs and Campus Life to assist you in performing your job. It includes such hardware as: workstations (PCs), networks, pda/smart phones, portable PCs (laptops, netbooks, tablets, iPads) various peripheral equipment (printers, scanners, and CD/DVD devices), as well as installed software, Ethernet services and calendar/E-mail.

The information, policies, and guidelines outlined here are applicable to all Student Affairs and Campus Life staff who use departmental and campus technology resources.

As a University employee, you are expected to use computing and information technology resources securely and responsibly as they apply to your job function and comply with University, Campus and Division data and computing polices and guidelines. Appendix A provides a summary of IT information for University staff and Appendix C links to a number of these guideline documents.

SATS – Student Affairs Technology Services

SATS is responsible to provide IT management and support around principles of standardization, centralization and enhancing resource efficiency. SATS is responsible for directing, managing and supporting Student Affairs and Campus Life’s technology resources.

SATS consists of full time staff as well as part time student staff that coordinate and manage computers, information systems, and technology initiatives for supported units within Student Affairs and Campus Life. We provide networking; database implementation, management and support of hardware and software support; technology purchasing, technology asset inventory, digital media and communications, training and residential cable tv services.

Additional information about our services can be found in the SATS Service Catalog.

SATS is comprised of 4 units – Help Desk/Networking, IT Infrastructure, Database/Applications, Communications, Training, and Electronic Systems. (Organizational Chart)

How to Get Technical Assistance

If you experience a problem with Student Affairs and Campus Life hardware, software or databases, or have a question about your computer or software, please call the SATS Help Desk:

- SATS Help Desk at 577-SATS (7-7287) or email SATS-hd@sacl.umass.edu.

Upon receiving your call, the Help Desk staff will first attempt to resolve your problem over the
phone or via email. If the problem cannot be resolved at that time, a site visit or referral to another staff member will be needed.

At the time of the call, you will be given an estimated time for when you can expect to be contacted to resolve the problem. Please note that high priority calls, such as network failures and critical database and printing problems, will take precedence over non-critical problems and other local software problems.

### Equipment, Software and Security Standards

SATS provide technical support for the standard hardware and software provided by Student Affairs and Campus Life to its staff for business use. Platforms may vary depending on the particular needs of staff to meet their job requirements.

**All computer, network hardware, software and technology purchases must be processed through, and approved by SATS to ensure appropriate licensing, compatibility, inventory, and installation.**

**Password Security** ([http://www.oit.umass.edu/accounts/password_security/rules.html](http://www.oit.umass.edu/accounts/password_security/rules.html))

**User passwords:**

- Must be between 6 and 16 characters.
- Must contain characters from 3 of the following 4 categories:
  - Uppercase characters (A - Z)
  - Lowercase characters (a - z)
  - Digits (0 - 9)
  - Special characters (limited to the following):
    - !, #, $, %, &, ' ( ) * + , - , / : ; < = > ? @ [ \ ] ^ _ ` { | } ~
- Cannot contain 3 or more adjacent characters from your NetID or username (e.g., if your NetID or username is jdoe, then your password cannot be 4xP/doe/876).
- Cannot contain the reverse of your NetID (e.g., if your NetID is jdoe, then your password cannot be 4xP/eodj/876).
- Should not be solely composed of English or foreign words or proper names.
- Passwords will initially be provided in a state where the user is required to immediately change it.
- For many systems passwords must be changed every 180 days

**Administrative rights**

The standard Student Affairs and Campus Life workstation configuration does not provide administrative rights to the workstation. Staff are provided the rights necessary to perform their duties.

**Screen Saver Policy**

All workstations and servers will be configured to lock after a period of inactivity. The default inactivity period will be 10 minutes and may be adjusted by request depending on the
circumstances, but not to exceed 20 minutes. The time may be adjusted down as needed for more sensitive workstations or servers.

You will need to re-enter your password to unlock.

**Campus Systems**

**OIT Account (a.k.a. NETID)**

The Office of Information Technologies (OIT) manages much of the technology provided for the Amherst campus. Your NetID serves as the **primary user name** for your Office of Information Technologies (OIT) account and gives you access to the campus network (wired and wireless), File Storage and Sharing (UDrive), Student Information System (SPIRE), OIT Email (UMail), and the Learning Management Systems (SPARK and Moodle). Your OIT account is a key to a wide variety of services offered by OIT to the UMass community. For information about the services provided, go to Account Services on the OIT web site (http://www.oit.umass.edu/accounts).

More and more systems are being configured to use the NetID for authentication, for example Parking Services and the PeopleSoft HR and Finance systems. This elevates the importance of strong, secure passwords.

You are expected to read and comply with the **OIT Acceptable Use Policy** that is included in Appendix C of this document. This policy is also available online at http://www.oit.umass.edu/policies/oit-policy-acceptable-use-computing-information-technology-resources.

**Administrative Computing Support Organization (ACSO)**

ACSO, a part of the Office of Information Technologies (OIT), maintains the Student Information System (Spire) that supports administrative functions for the Undergraduate Registrar, Graduate School, Bursar, Office of Financial Aid, Division of Continuing & Professional Education, Housing and Residence Life, Office of Institutional Research and Graduate and Undergraduate Admissions Offices.

Students, instructors, and authorized University staff use SPIRE to manage academic records, billing and financial aid information, housing assignments, as well as course and schedule information.

Access to these data resources must be applied for and approved by the appropriate data custodian and is based on your individual needs and request. Please contact your Technology group for additional information.

**A & F Administrative Systems**

A&F Administrative Systems, a part of the Division of Administration and Finance, is responsible for the PeopleSoft HR and Finance implementations for the Amherst Campus.

Access to these data resources must be applied for and approved by the appropriate data custodian and is based on your individual needs and request. Contact your Technology group for additional information.
Training

SATS provides or arranges training on email, general desktop applications, departmental systems and by request on special topics.

For information about offerings in Student Affairs and Campus Life, contact Scott Campbell at sjcampbe@umass.edu.

Other training opportunities are available through the Office of Information Technologies (OIT) (http://www.oit.umass.edu/workshops) and Workplace Learning and Development (http://www.umass.edu/wld/).

Periodically, the Campus Chronicle also provides information on available workshops.

Requests for New Accounts and/or access to resources

SATS provides access to a variety of database systems and network locations. Requests for staff access should be submitted by their supervisor to sats-access@sacl.umass.edu. For questions, please contact the SATS Help Desk at 577-SATS (7-7287) or email SATS-hd@sacl.umass.edu.

Requests for Additional Hardware and Software

Requests for additional hardware or software should be made in writing or via e-mail and emailed to SATS – SATS-hd@sacl.umass.edu. Requests are reviewed with the manager of the specific department/area making the request. During the review process the following items are considered:

- the business need/purpose of the request
- SACL’s ability to effectively install, configure, train and support the requested hardware or software
- Compatibility issues
- Compliance with University contract requirements
- Cost/budget impact
- Availability of other resources to reasonably meet the need

General Guidelines for Use of SACL Technology Resources

SATS takes many measures to secure network resources (servers, data, files, email, etc.) from access by unauthorized users. To be successful, these measures rely on staff to take reasonable steps when using these resources to complete the security loop. The intent is not to control work habits but rather to provide secure and reliable network resources for everyone to share. Please take a few moments and read through these practices, as well as the Data and Computing Policies, Standards and Procedures Summary for University Employees that is included in Appendix C.
SECURITY EXPECTATIONS

- Only use computers and computing resources for their intended purposes.
- Only use computer systems, and access data and programs, for which you have been authorized.
- **Guard the secrecy of your password.** Do not share your passwords with others, or store or write a password down where another might find it. You are responsible for all actions taken by someone using your account whether or not they are authorized! You are responsible for proper password protection.
- Follow password security standards including periodically changing your passwords. Use passwords which are difficult to guess. Avoid using names, birth dates, repeating characters (e.g., 111111 or abababa), common character sequences (e.g. "123456"), or common words which might be guessed. You should also avoid using any personally related information (e.g., pet’s, child’s or spouse’s/partner’s name; favorite sports team or car; etc.) and always use a combination of upper and lower case letters, special characters and numbers.
- **NOTE:** If you set up login accounts on other systems (on and off campus), you should not use the same user ID or password that you use for Student Affairs and Campus Life and University accounts.
- Do not send passwords or pin numbers through electronic mail unless encrypted. Information regarding a password’s structure (e.g., Your password consists of your campus designation and the last 4 digits of your social security number – UMAxxxx) can be sent via electronic mail in clear text format
- Do not allow web browsers or applications to store passwords and login information as these features are easily compromised by hackers, and your IDs and passwords could be stolen. Take the few extra seconds it takes to enter your password each time you use the service.
- Do not to disable any University or department configured firewalls. The University recommends the installation of firewalls on all University owned systems and any computer accessing University computer and network systems. **Firewalls will be configured and managed by your department’s IT staff.**
- Guard the safety and accuracy of University data by protecting computer systems from theft, destruction, and unauthorized access. This includes employing appropriate physical security, implementing data access restrictions, and making good decisions about storing on portable media and/or printing.
- Obtain authorization from the appropriate Data Custodian before processing University data on home computer systems. Never move University data to personal computers or off campus devices.
- Do not leave your computer unattended when logged into the network, your email or
a campus system. To lock your workstation press CTRL + ALT + DEL and select Lock Workstation or press Enter.

INDIVIDUAL RESPONSIBILITY

- Do not log on for other people and allow them to access computer systems or data under your logon/operator id. It is possible both to look in your directory and to use your username for malicious purposes.

- Individuals shall not use University computer systems/resources or networks for personal business, monetary gain, commercial activities, or political activity.

- The fact that you can connect to a computer system or access an electronic file does not mean that you have authority to do so. Potential lack of security on a network does not mean that a computer system is open and available for use by anybody, or for any purpose.

- Possible loopholes in computer or network system security shall not be used to damage computer systems, obtain extra resources, take resources from another user, or gain access to any University computer system or any computer system networked to the University.

- Use proprietary information (e.g., text, images, audio, videos, icons, programs, etc.) retrieved from computer or network resources in conformance with copyright laws. Violating copyright and software licensing laws is prohibited.

- Ensure that antivirus software is installed, continuously enabled and up to date on any computer you use which will share information with any University computer or system.

- Respect University time and property – do not play web games, use personal social media, access audio and video content for non-business purposes, or surf the web on University equipment.

CARE OF RECORDS

- Electronic files may not be permanently removed from the University or destroyed, except in accordance with approved Record Management, Retention and Disposition Standards and schedules.

- University employees have a duty to ensure that personally identifiable information relating to students, staff and other protected information (i.e., social security numbers, credit card numbers) is guarded against loss or theft. See Appendix B for more information.

- Access to Confidential information is granted based on an employee’s need for it, in connection with their official job responsibilities. This access should not be shared, transferred or delegated, unless the employee’s official job responsibilities require them
to do so.

- **IMPORTANT**: All staff that have access to student directory data and other student data should also read the section on *Guidelines and Responsibilities for Data Confidentiality and Access to Student Data*, Appendix C.

- Personal notes of employees are not subject to public record statutes, provided that they are maintained personally, and are not stored in university files, email or on university computer systems.

**DESKTOP/NETWORK**

- Only software appropriately licensed to Student Affairs and Campus Life is allowed on Student Affairs and Campus Life computers.

- Installing personal hardware on your computer is prohibited. Hardware includes but is not limited to flash drives, printers, DVD drives, hard drives, flash drives, webcams, cameras, Smart phone/PDA software and other portable media.

- Installing personal software on your computer is prohibited. Software includes but is not limited to application programs, games, fonts, utilities, and graphics. This includes software, games, utilities, shareware, etc. downloaded from the web or from some other electronic source.

- Installing/downloading/saving music that are not owned by the University or in the public domain on University technology resources is prohibited.

- Use of unencrypted communication tools such as FTP or Telnet is prohibited.

- The use of non-encrypted instant messaging software for business conversations that includes information that is not considered public is prohibited.

- Desktops, backgrounds, customized icons, etc. must be appropriately licensed, customer friendly, and appropriate for an office environment.

- SATS has installed antivirus software on all University purchased computers. If you have obtained authorization to use a personal device on the campus network, it is your responsibility to ensure adequate virus protection and other security considerations have been implemented according to University policy. You are also responsible for reporting any malware encounters to your departments IT staff/help desk immediately. Malware encounters include: strange emails (e.g. from people you don’t know or asking for personal confidential information) or pop-ups, web browser opening new pages or redirecting to sites unexpectedly, erratic mouse/cursor movement, virus notifications, or suspicious behavior on your computer.
Did you know that viruses are normally introduced into a system by a voluntary act of a user (e.g. installing an application, downloading/copying a file, reading an email, etc.)

This is why our prevention policies focus on limiting the introduction of potentially infected software and files.

- Student Affairs and Campus Life technology resources are provided for University related activities only. Incidental or occasional personal use is allowed provided that it does not interfere with an employee’s job function and is supported by the appropriate supervisor/manager.

- Use of University resources to engage in activity that is illegal (such as, illegal downloading of copyrighted music or video) or is in violation of departmental or University policy is also prohibited.

- **If you have access to division/department network** drives, all work related files should be stored on the network. Secure your work and protect it from loss, **save your files to the server and not on a local drive on your workstation**. Network data is backed-up nightly.

- If you do not have access to a Student Affairs and Campus Life network be aware that data saved to a local drive can be accessed by anyone who has access to your computer. If you have to save to your local drive, remember to periodically make copies or back up important data.

  **NOTE:** If for some reason you run out of space on your hard drive, call your Help Desk for assistance. Do not try and create space on your hard drive by deleting files that you don’t recall ever using or are unfamiliar to you. They may be important files for some other system purpose.

- Computer activity may be logged and monitored for operational, security, auditing, and investigative purposes.

  **NOTE:** The campus is subject to power fluctuations and campus network interruptions on occasion. One slight brown out is all that it takes to damage data or a database, such that you lose your work. Saving your work often and logging off the network when you are going to be away from your desk can avoid this situation. Most users do not believe in this practice until it happens to them—then they become firm believers in it.
ELECTRONIC MAIL

- E-mail is made available to employees for the purpose of conducting University-related business. Occasional social/personal use is allowed providing it does not interfere with an employees’ job function or performance.

- University email is considered an educational record and as such can be made available to students under FERPA and Public Records requests.

- Users of electronic communications are cautioned not to write anything in an email that they would not feel comfortable putting in a memorandum.

- The University treats personal e-mail messages as private correspondence, however the University has the right to look at any documents and files including emails stored, sent or received on University computer systems and networks if necessary for University business.

- Electronic messages are University records, no less than paper memoranda. The emails of university employees are public records, and e-mail users shall remove mail from their mailbox only in a manner that is consistent with University record retention procedures.

- Individuals are prohibited from using an e-mail account assigned to another individual to either send or receive messages, unless it is a workgroup or departmental email account designed for such use.

- If it is necessary to read another individual’s mail (e.g. while they are on vacation, leave, etc.), proxy or message forwarding should be utilized. Proxy capability is provided in some email systems so that a staff member can provide access to any combination of E-Mail, Appointments, Tasks, Notes, or Phone Messages to another staff member. In lieu of sharing a password with someone else, the staff member should forward his or her E-Mail to another account. Please contact your IT staff/Help Desk for assistance with either of these options.

- The University cannot control the content of electronic mail. If you receive electronic mail that you consider harassing, threatening or offensive, you should contact your supervisor/manager.

- Authorized users are prohibited from sending, posting or, publicly displaying or printing unsolicited mail or materials that is of a fraudulent, defamatory, harassing, abusive, obscene, or threatening nature on any University system. Individuals with e-mail IDs on University computer systems are also prohibited from sending messages which violate state or federal law, or University policy. The sending of such messages/materials will be handled according to University codes of conduct, policies and procedures.

Remember to value, protect, and properly maintain University records and computer data! It is up to you to keep them safe, accurate, and complete!
DATA, COMPUTER SYSTEM/RESOURCE ABUSE

You can expect to lose your computer account; be disconnected from the network; and be subject to university disciplinary action for the following abuses. Some of the following actions are also illegal:

✓ Attempting to discover or tamper with user passwords.

✓ Accessing data, computer systems, or email accounts without authorization.

✓ Accessing or copying files (whether paper or electronic) without prior consent from the file owner or records custodian. Accessing the private files or personal correspondence of others without permission, even if those files are unprotected, is prohibited. Altering another user's files without their express or implied permission is vandalism and destruction of University property.

✓ Disclosing private or confidential records to the public or to outside agencies unless such dissemination is required by law, or by the individual's job at the University.

✓ Deleting or copying files from another person's computer or email account without authorization.

✓ Posting, sending, printing, or publicly displaying materials that violate law or University policies. Such material includes material that is fraudulent, obscene, defamatory, harassing, abusive, or physically threatening in nature. The University has special concern for incidents in which individuals are subject to harassment or threat because of membership in a particular racial, religious, gender or sexual orientation group.

✓ Repeated sending of unsolicited mail (spamming).

✓ “Rebroadcasting” information obtained from another individual, that the individual reasonably expects to be of a confidential nature, to others not involved in the issue (e.g. posting the confidential information to a newsgroup, emailing it to others not materially involved in the confidential matter, or creating a link to the information from a publicly available Web page).

✓ Using University computers, networks, or web sites for monetary gain, political purposes or illegal activities. This includes using University Internet resources to create or maintain web pages for personal business gain, or to endorse or otherwise support a specific political campaign, candidate, party or referendum.

✓ Illegally using copyrighted materials including print, audio, video and software.

✓ Using personally owned software on University computer systems/resources unless the software is properly licensed for such use and system administrator approval has been obtained.
DEPARTMENTAL ADMINISTRATOR RESPONSIBILITIES

Department heads should ensure that departmental system administrators understand and comply with applicable Data and Computing Standards, Data/System Administrator Responsibilities and System Requirements, Records Management, Retention & Disposition Standards, etc.

Asset Tracking
SATS is responsible for tracking and managing all IT assets (hardware, software licensing, cameras, etc.)

Vendor Access
Third party network and application access such as those to vendors and consultants should be treated very carefully and on a case-by-case basis. Access for vendors should be on an as needed basis and depending on the situation monitored. Contracts with vendors needing access to sensitive or confidential information must include appropriate contract language concerning their responsibilities. If there is not contract then the vendor must sign a University Provided Confidentiality agreement prior to being granted access.
Employee Use of Social Networks

There are several ways an organization can benefit from using external(public) social networks such as Facebook, MySpace, LinkedIn. SACL supports the use of social media by employees to connect with students, fellow faculty and staff, business colleagues and alums to further department and division goals. **Personal use of social media should be separate from professional use.**

Business uses of social networks include:

- Use of social networks for outreach purposes and to create groups to support campus recruiting efforts;
- Use of social networks to monitor public opinion about an organization, process or service;
- Use of social networks like LinkedIn for professional networking and maintaining contacts with professional or standards organizations.

Social media usage is governed by the same policies that govern all other electronic communications.

Requests for employee/program/department use of social networks should be submitted to the department head or designee for review and approval. This step ensures that we have a coordinated and deliberate use of these services. Department social network pages must be appropriately branded, regularly monitored and kept current.

Use of social networks such as Facebook and MySpace using University credentials for personal use is prohibited.

Department social media accounts should be created using a dedicated [subsidiary OIT account](#). Include a statement on the page that states you reserve the right to remove any inappropriate content.

Monitor comments daily.

Downloading and installing plug-ins for social network sites is not allowed unless supported by your IT support group.

Information published on your social media site should comply with the University’s confidentiality and disclosure of proprietary data policies. This also applies to comments posted on other blogs, forums, and social networking sites.

Your online presence reflects the University. Be aware that your actions captured via images, posts, or comments can reflect that of our division.

*Be active, Be timely, Remember everything you do on-line will live forever…*
Remote Access

Make requests for remote access to University resources by sending request and business need to sats-access@sacl.umass.edu.

Laptops and Portable Devices

(Laptops, smart phones, pda’s, & personal handheld devices)

Many staff have departmental and personal laptops and portable devices to support their work. This portability increases our security exposure. SATS offers the following support for laptops and portable devices.

Each employee issued a laptop and/or portable device is responsible for the security of the device and the information stored on it regardless of where the device is at the time of use – office, home, hotel, airport, etc. Upon allocation of laptop or portable device the staff member must review and sign the Student Affairs and Campus Life Property Transfer Form indicating their agreement to the information contained therein. A sample can be found in Appendix E.

Laptops are for your use in the performance of your work. Do not share your laptop with anyone including family or friends.

The laptop may only be used for activities falling within the scope of your employment with Student Affairs and Campus Life. You may not use the laptop for personal or commercial use.

Laptops issued by the University after 2010 will have encrypted hard drives.

Any device, University-provided or personal, that has data access to University resources must have the password feature enabled.

Users may not install third-party software, or otherwise alter the configuration of the laptop, unless expressly permitted by SATS. Any software not installed by or explicitly authorized by SATS is subject to deletion without notice. This includes screen savers, games, software downloaded from the Internet, personal software and digital media.

Do not write down your password and store it with your laptop and do not store your password on the laptop hard drive.

Do not copy sensitive data to non-secure, non-encrypted portable media such as usb drives, cd or dvd. Instead, move data to properly secured folders on the network or UDrive.

All uses and disclosures of sensitive information must be in accordance with University Sensitive Data Guidelines http://www.oit.umass.edu/security/compliance/securing_data.html

You must report any security incidents involving your laptop. This will enable SATS and/or OIT to investigate, and take steps to mitigate the risk to any confidential data maintained on the laptop.
If your laptop was lost, stolen or vandalized while being used on University property contact SATS as soon as possible. Next, contact your Supervisor who will help coordinate the investigation of the security incident according to University procedures.

If your laptop was lost, stolen or vandalized from your car or home, or when you were at any other non-University property, you must immediately file a police report with local police authorities, and must cooperate in any investigation conducted relating to the loss, theft or damage. Be sure to get a copy of the police report which you will need to provide to your supervisor. Upon return to work, contact the appropriate SACL IT staff, and then your supervisor.

Staff with University-issued laptops and iPads will be required to bring the device to SATS for updates at least twice per year for maintenance. Additionally, University-issued laptops or desktops should be left online and plugged in overnight at least once per month to ensure that the latest patches and security updates are pulled down to the system. If the device is not on the campus network the device should also be connected to the campus VPN for this patch window to ensure that the system is able to obtain the updates.

**Synching portable devices to calendars**

SATS will provide, install and support software to synchronize staff department owned portable devices to their departmental calendar, tasks and address book/contacts.

For personal devices that meet the department standard, SATS will do their best to assist. The staff member will provide the device, the software for the device and cradle/connection to computer (if required). SATS will provide an overview of the set up and synchronization process for the departmental email and calendar system.

The device must be Blackberry or Apple, depending on the standard provided by the SATS. SATS staff will be happy to consult with staff prior to the purchase of a device concerning compatibility.

Synchronized devices must be password protected.

SATS can only support synching to the department’s calendar system. SATS will not support synchronization to other third party calendars such as Google Calendar in order to maintain the security of sensitive information and prevent information regarding University business from leaving campus.

If software installed by a staff member on a personal device conflicts with synching, SATS will make a reasonable effort to identify and/or resolve the problem, however we may determine that the device is not supportable.

Synchronization of E-Mail can be complicated. SATS will support this on a business need and time available basis by request.

SATS is not responsible for calendar synchronization on personal/home computers.

SATS is not responsible for loss or corruption of information or damage to personal devices.

These are electronic devices and they sometimes fail, so please sync your device regularly. In the event that a hard re-set is necessary you will loose all information on the device. Your next sync will update the information from your workstation.

In the instances where troubleshooting or syncing results in duplicate entries, it is the staff member’s responsibility to remove unwanted entries.
Website Standards and Guidelines

Attached as Appendix G.
Appendix A – Data and Computing Policies, Standards, Procedures Summary for University Employees

Created: November 29, 2007

University of Massachusetts
Data and Computing Policies, Standards and Procedures Summary
University Employees – Faculty and Staff

This Summary is provided to give faculty and staff an overview of the University’s data and computing policies and standards. All employees are advised to review the University’s Data and Computing Policies/Standards/Procedures complete acceptable use and other data and computing requirements. The University’s Data Security Awareness and Education website is another good source of information. It includes a comprehensive Frequently Asked Questions (FAQ) section to clarify policy, standard/guideline, and use questions.

In support of the University’s mission of teaching, research, and public service, the University provides networking, computing, and a wide array of information technology to students, faculty and staff. These technology related services provide the foundation and backbone upon which all University business is conducted.

I. General

The University expects all members of the community to use computing and information technology resources in a responsible manner, respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, state and federal laws, and University policies and standards.

All University administrative records are owned by the University Board of Trustees regardless of their physical location, even when in the possession of individuals.

Employees contacted by law enforcement to answer general questions about University systems, services, processes, etc., should refer such questions to University General Counsel.

If the law enforcement official presents a search warrant the agent or officer may begin a search as soon as the employee responding to the order has looked at the warrant and determined its scope. University employees on whom a search order is served should immediately contact their supervisor, University legal counsel and the Designated University Official at the applicable campus to inform them that a court ordered search has been requested or initiated.

The community as a whole and each individual user has an obligation to abide by the following standards of acceptable and ethical use:

- Use only those information technology and computing resources for which they are authorized.
- Implement security in their daily interactions with people, data, systems, and facilities. Each person should be alert and conscious of the environment around them and notify the appropriate security/system administrators if they notice any security vulnerability.
- Use computing and information technology resources only for their intended purposes. Staff are given access to perform their job functions or other University sanctioned activities.

- Safeguard the integrity, accuracy, and confidentiality of University data by taking all reasonable steps to protect University data and computer systems/resources from theft; destruction; unauthorized access, creation, alteration or exposure; or any form of compromise resulting from inappropriate intentional, negligent acts, or omissions. This includes implementing appropriate physical security and data classification procedures, and periodically "refreshing" downloaded data to ensure you are working with accurate, up-to-date data.

- Properly create, access, use and dispose of University data based on the data's classification (see Attachment 1 - Data Security, Management, Use, And Disposition Requirements Based On Data Classification). Users shall access University data for approved purposes only, and shall understand the data they are accessing and the level of protection required. Databases containing Operational Use Only or Confidential data should be secured. Extracts of Operational or Confidential data should be secured at the same level as the file/database from which the data was extracted. Aggregates of data should be classified as to the most secure classification level (e.g. when data of mixed classification exist in the same database, file, report, etc., the classification of that database, file, or report should be that of the highest level of classification). Reports containing Operational Use Only or Confidential data should be disposed of properly. Paper and microfiche/film should be shredded. Disks/hard drives should be erased so as to be irretrievable.

- Appropriately backing up data (e.g., business, personal/instructional, etc.), and computer system and applications software to allow for recovery if there is a disruption.

- Using antivirus software on any computer system they use which accesses University data or computing systems/resources.

- Obtaining authorization for the processing of University data or conducting University business on home computer systems from the appropriate Data Custodian.

- Only performing remote/distributed access to administrative or research computer systems via a virtual private network (i.e., VPN).

- Notify the appropriate system, network and/or security administrator(s) of any suspected or actual security violations/incidents.

- Be aware that the University disclaims any loss or damage to software or data that results from its efforts to enforce this and other data and computing Standards.

University departments and staff create, maintain and handle Confidential data on a daily basis to fulfill necessary University business needs. Confidential data includes personally identifiable information and protected information:

- **Personally Identifiable Information (i.e., PII)** is assigned a security classification of CONFIDENTIAL and includes University data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or University contracts. PII includes, but is not limited to:
An individual’s first name and last name or first initial and last name in combination with one or more of the following data elements: social security number, driver’s license number or state-identification card number, or financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account. (Massachusetts Law Chapter 93H)

Individually identifiable health information (i.e., information relating to past, present or future physical or mental health or condition of an individual; provision of healthcare to an individual or payment for the provision of healthcare to an individual; Individually identifiable health information may include, but is not limited to: name, telephone/fax number, email address, social security number, driver’s license number, internet address or any other unique identifying number, characteristic or code). Some, but not all, health information is protected under the Health Insurance Portability and Accountability Act of 1996 (i.e., HIPAA).

Student education records not defined as student "directory information" (e.g., student number, grades, courses taken, etc.) by the University and its Campuses are protected under the Family Educational Rights and Privacy Act (i.e., FERPA).

“Customer” records such as names, addresses, phone numbers, bank and credit card account numbers, credit histories, or social security numbers as they related to student financial aid information are protected under the Graham Leach Bliley Act of 1999 (i.e., GLB).

Protected Information is assigned a security classification of CONFIDENTIAL and includes University data whose disclosure would not result in any business, financial or legal loss BUT involves issues of personal credibility, reputation, or other issues of personal privacy. The security and protection of this data is dictated by a desire to maintain staff and student privacy. Protected data includes an individual's first name or initial and last name in combination with one or more of the following data elements: their birth date, mother’s maiden name, state employee salary, employee identification number, electronic signature, fingerprint, photograph or computerized image, physical characteristics or description, or passport number.

University employees have a duty to ensure that personally identifiable and protected information created, collected, used, maintained, or disseminated in the process of providing services to the public and the University community must be safeguarded against loss or theft.

The University recommends the installation of personal firewalls on all University owned systems and any computer accessing University computer and network systems. Several Campuses offers inexpensive personal firewall software to all employees for work and personal use.

Staff loaned or using University owned/funded computers (e.g., PCs, laptops, PDAs, Blackberries, etc.) shall make every reasonable effort to secure and safeguard the physical integrity of the computer and to comply with all University Data and Computing Standards.

University records may not be permanently removed from the University or destroyed except in accordance with approved Record Management, Retention and Disposition Standards and schedules. Records management is a joint responsibility of the record creator and users. All University employees who handle University records are responsible for knowing and following laws (e.g., Public Records, FERPA, etc.), University policies, guidelines/standards and campus procedures that govern these records.
Personal notes of employees are NOT subject to public record statutes, and can be maintained personally, not in "official" files.

Employees whose job functions include the transfer, donation, sale or salvage/destruction of computer hardware and/or electronic storage devices shall follow the requirements stated in the Standards for the Redistribution and Disposition of Computer Equipment and Electronic Storage Devices in addition to any campus procedures related to equipment transfer, donation, sales or recycling/destruction.

II. Individual Responsibility

Users must protect the confidentiality of personal identification codes and passwords, guard against unauthorized access to computer accounts, software, files, and other IT resources.

Authorized users are presumed to be responsible for any activity carried out under their University Logon IDs/Operator IDs/Accounts. All activity should be conducted in accordance with their role and responsibilities at the University.

Any person attaching a wireless client to any University network (wired or wireless) is responsible for the security of the device and for any intentional or unintentional activities from or to the network pathway that the device is using.

Individuals accessing University data and/or computer systems shall only access the data and/or computer systems for which they have been given authorization. This access should not be shared, transferred, or delegated.

The University makes e-mail facilities available to staff. E-mail is made available to employees for the purpose of conducting University-related business. Information resulting from communication on University computer systems is University property. Occasional social/personal use is allowed providing it does not interfere with an employees’ job function or performance. Staff may use their access to University computers to use worldwide networks such as the Internet. Employees who access University or Campus networks for private purposes should subscribe to a commercial service provider.

Employees' may have personal web pages on University networks as long as they only provide information about the individual that is relevant to that individual's role at the University.

III. Security

Passwords are required on all computer systems (e.g., desktops, laptops, PDAs, etc.) in which Confidential or critical data is stored or maintained.

Never share your password with anyone or type your password when someone is watching. This includes logging on for another person and allowing them to access computer systems under your logon/operator id. Never allow anyone to access computer systems under your Account/Logon/Operator IDs. Never write down passwords or store them in batch files, automatic login scripts, terminal function keys, or in other locations where another person might discover them. Do not hard-code passwords or pin numbers used to protect access to University data in software or scripts.

Follow password security standards including, but not limited to periodically changing your computer system passwords, selecting a password that is difficult to guess and when possible, includes letters, digits and special characters (e.g., #, %,$). Authorized user passwords must be changed periodically.
Security tokens shall not be stored with the corresponding microcomputer/pc (including transportable/laptop computers, PDAs, etc.).

Log off computer systems/resources if you leave your pc unattended or will not be accessing data for an extended time.

IV. Privacy

University computer systems/resources may record information about each user session. Information recorded includes the username/operator id associated with the session, the login and logout dates and times, and the amount and kind of computer resources used during the session. This information is used for legitimate University purposes including issues of law, abuse, security or system managements.

The University does not routinely monitor the content of computer systems/resources including files, programs and electronic communications/emails.

The University has the authority and reserves the right to examine material (e.g., email, files, images, etc.) stored on or transmitted through its resources if there is cause to believe that the standards for acceptable and ethical use are being violated by a member of the University community, a trespasser is on its systems or networks, or for other legitimate administrative reasons. Additionally, the University has the responsibility and authority to scan computers attached to the University's wired and wireless networks to ensure appropriate security, and support network operations and performance.

The University has the responsibility and authority to release data and information to outside authorities based on bona fide requests following due legal process. The University takes steps to protect employee privacy and to ensure that protected/privileged information is not disclosed, however this privacy can not be guaranteed because the court ultimately determines whether confidential information must be disclosed. The University takes reasonable steps to protect files stored on the university systems from unauthorized access, however, the University cannot guarantee the confidentiality of any of these files.

V. Unauthorized Activities

Individuals shall not:
- Attempt to compromise or tamper with user passwords. This includes, but is not limited to cracking, decoding, copying password files, “sniffing” packets to search for passwords or otherwise attempting to discover passwords belonging to other individuals.
- Attempt to intercept any network communication for purposes including, but not limited to: reading message/file content; rerouting packets; or packet “sniffing”.
- Remotely log into (or otherwise use) any microcomputer/PC not designated explicitly for public logons over the University and/or Campus networks, even if the configuration of the computer permits remote access, unless you have been given explicit permission from appropriate authorized personnel.
- Attempt to or obtain unauthorized access to University data, computer systems/resources, or another's computer or email account. This includes using computing systems/resources to access any other computer system (on or off-campus) without authorization.
- Access or copy files, regardless of media (e.g., paper, diskette, etc.), of another user without prior consent from the file owner/data custodian.

- Perform or assist in the performance of any act that will interfere with the normal operation of computer, terminals, peripherals, networks, or in any activity that interferes with the rights of others such as writing/releasing viruses.

- Disseminate any Confidential information unless such dissemination is required by the individual’s job at the University.

- Post, send or publicly display or print unsolicited mail or materials that violate existing laws or University policies/standards/codes of conduct.

- “Rebroadcast” information obtained from another individual that the individual reasonably expects to be confidential.

- Illegally use, solicit or distribute copyrighted software within or outside the University, including print, audio, and video.

- Use personally owned software on University computer systems/resources unless the software is properly licensed for such use and system administrator approval has been obtained.

VI. Impersonation, Misrepresentation and Anonymity

Individuals shall not provide false or misleading information to obtain access to University computing facilities or resources nor send any electronic messages with a forged sender identity.

VII. Commercial, Political and Illegal Activities

Individuals shall not use University computer systems/resources or networks for monetary gain, political purposes or illegal activities. This includes using University Internet resources to create web pages for personal business or financial gain, except as permitted by other University policies, or to endorse or otherwise support a specific political campaign, candidate, party or referendum.

VIII. Legal Responsibilities

Individuals shall not use University data or computing resources/systems to violate state or federal laws/regulations.

All University employees are under a legal duty to preserve all evidence, whether electronically stored information (i.e., ESI) or hardcopy, when notified to do so by the General Counsel’s office. Failure to do so may result in fines and may jeopardize the University’s position in a claim or lawsuit.

Violation of University data and computing standards/guidelines may result in the loss of your computer account; disconnection from networks; your being denied or given limited access to University data, applications and/or computer systems. Individuals may be subject to reprimand, suspension, dismissal/termination, or other disciplinary action based on the offence and may be charged with criminal offenses or have civil action taken for computer abuses or violation of law within the confines of law.
Appendix B – Sensitive/Confidential Data

Document: Sensitive Data Notice
Date: 9/30/2009

The purpose of this document is to provide information on what constitutes sensitive data and communicate responsibility regarding the use and retention of this data.

Sensitive data refers to:

**Personal information**: An individual’s name in combination with any of the following: Social Security Number, Driver’s License Number, State Identification Card Number, financial account number, credit or debit card number (including Campus UCard Run#).

![Chapter 93H Diagram]

(Based on Chapter 93H of the Massachusetts General Laws of 2007).

**Health information**: Individually identifiable information related to a person’s physical or mental health. This applies to any past, present, or future condition, treatment, or payment of health care service.

![HIPAA Diagram]

(Based on the Health Insurance Portability and Accountability Act of 1996, a.k.a. HIPAA).

**Education records**: Students’ academic, personal, and financial information as described in the most recent Academic Regulations Handbook.
Please keep in mind these important guidelines:

1. Know what constitutes sensitive data at UMass Amherst. Limit the amount of such information collected to that which is necessary for official business. Do not save such information beyond the time that it is needed in accordance with University Record Management, Retention and Disposition Standards.

   **SACL staff should not use, store, or display Social Security Numbers (i.e., SSNs) unless absolutely required to perform job responsibilities or required by law.**

2. Keep what’s necessary, purge what’s not.
   - For departments - Collect, distribute, and retain only the minimum amount of sensitive data necessary for your official needs.
   - For individuals - Collect and retain only that sensitive data which is necessary to the performance of your official functions.

3. Dispose of sensitive data in an appropriate and secure manner. Delete personal and protected information when there is no longer a business need for its retention, in accordance with University Record Management, Retention and Disposition Standards.

4. Choose the right storage option. Save sensitive data that you need on departmental/division server(s). Use caution when saving information on desktops, laptops or shared computers. If this is necessary, contact the SATS Help Desk (7-SAIT) for information about passwords and encryption. This would apply to not only common resources such as shared network storage and hard drives, but also to workstations, laptops, thumb/flash drives, CD’s, floppies, zip disks, portable hard drives, cell phones, handheld electronic devices, etc.

   You should not store sensitive data on USB drives or other portable devices that can be easily lost or misplaced.

5. Sensitive or personally identifiable data should not be stored on off-site or third party servers, websites or systems unless the University has ensured through a contract that they are appropriately protecting University data.
Appendix C – Campus and University IT Policies and Resources

UMass Amherst – OIT – Policies
UMass System – Data and Computing Policies
Dean of Students - FERPA
Ferpa Tutorial (PDF)
Ferpa Tutorial (PowerPoint)
OIT Services At A Glance
Appendix D – FERPA

Guidelines and Responsibilities for Data Confidentiality and Access to Student Data (FERPA)
Student directory data (see item B), as well as other student data, is provided to staff based on their job responsibilities and role. Student directory data may be provided as a part of the integration with in-house and third party database applications.

All staff that have access to systems with student data must be sure to read and understand the information included in this section.

Requests for direct access (individual logon) to SPIRE, EMPAC, or other University database require authorization of the data custodian and can be requested through your departments IT group.

Downloads and requests for data from SPIRE in an electronic form requires a formal request to the Registrar’s Office. Contact your IT group or the Registrars’ Office for more information.

Federal Family Educational Rights and Privacy Act (FERPA)
University policy and the Federal Family Educational Rights and Privacy Act (FERPA), commonly referred to as the Buckley Amendment, govern the access to student data. The following information is excerpted from the Family Educational Rights and Privacy Act concerning the Student Telephone Directory records of enrolled students.

A. The Family Educational Rights and Privacy Act (Part 99 of Title 34 of the Code of Federal Regulations), also known as the Buckley Amendment, was developed to allow present or former students at educational institutions access to certain records maintained by the institution containing information about them. It also established standards of access accorded others, to ensure students’ rights of privacy.

The law generally grants the following rights of access to students regarding their own records:

1. The right to be provided a list of the types of educational records maintained by the institution which directly relate to them.
2. The right to inspect and review the contents of their own records.
3. The right to obtain copies of those records when:
   a) Failure to provide such copies would effectively prevent the student from exercising the right to inspect and review his/her educational records;
   b) When the student has submitted his/her written consent to allow the University to disclose certain personally identifiable information from the student's educational record, and the student requests a copy of the information to be disclosed; and
c) When the University transfers the student's educational records to another educational institution, and a copy of those records is requested by the student.

4. The right to a response to a reasonable request for an explanation and/or interpretation of their record.
5. The right to an opportunity for a hearing to challenge the contents of their records.

The law generally exempts personal records kept by instructional, supervisory, and administrative staff, as long as those records are not accessible or revealed to any other person except a substitute; records of law enforcement unit; records of employees of an educational institution; and records which are created or maintained by a physician, psychiatrist, or other recognized professional or paraprofessional, and which are created or maintained or used only in connection with the treatment of the student.

B. The law permits the University to release and/or publish, without students' permission, directory information. This is defined as student's:
   • Name
   • Local address
   • Home address
   • E-mail address
   • Major
   • Local telephone number
   • Date and place of birth
   • Acknowledgment of a student's participation in officially recognized activities and sports,
   • Weight and height of athletic team members
   • Date(s) of attendance
   • Degree
   • Certificates
   • Awards received
   • Most recent previous educational agency or institution attended by the student
   • Dollar amount of money earned on the state or trust payroll.

(Additional Note - If a student specifically requests suppression of this data then the information is not to be released.)

C. The University recognizes its obligation and responsibilities concerning rights of access to education records. Policies concerning transcripts, access of records to advisors, academic departments, counselors, and others with a need to know are available from either the office of the Undergraduate Registrar, 213 Whitmore, 545-0555, or the Graduate Registrar, 519 Goodell, 545-5296.

D. Copies of the full text of federal regulations in the Federal Register are available at the office of the Associate University Counsel, 374 Whitmore, 545-2204.

REQUESTS TO SUPPRESS DIRECTORY INFORMATION MUST BE INITIATED IN THE DEAN OF STUDENTS OFFICE BY THE STUDENT CONCERNED NOT LATER THAN THE DEADLINE PUBLISHED IN REGISTRATION NOTES, AND MUST BE RENEWED EACH SEMESTER OF ENROLLMENT.
Appendix E - Property Transfer Form

Student Affairs and Campus Life

Documentation of Movement of University Property to Off-Campus Location
(For University Business Use at Off-Campus Locations Only)

AGREEMENT

The purpose of this agreement is (1) to aid SACL and the Property and Inventory Control Office in accounting for the property of the University of Massachusetts/Amherst and (2) protection for the University and the Department lending property against damage (actual and collateral), loss or misuse of the property and (3) document University of Massachusetts/Amherst property in off-campus locations. Equipment can only be signed out when it’s required for specific University business purposes. Equipment that is no longer being used off-site for its intended business purpose needs to be returned to campus. The computer and the data stored on it must be maintained in a secure environment. Confidential University data and/or PII (Personally Identifiable Information) can not be put at risk by being taken off-site.

In consideration of permission granted to me by University of Massachusetts/Amherst Student Affairs and Campus Life, to move the following University property to the off-campus location indicated below and use of said property for University business, I agree to exercise reasonable care for said property while in my possession. In the event that said property is damaged, including but not necessarily limited to the total destruction of said property, by vandalism, theft, or negligence, I understand that it is at the discretion of the SACL Department Head, whose name appears below, or his/her designee, as to whether the Employee must reimburse the University for any or all necessary costs incurred for repair, or replacement with equipment of same model and manufacturer or in like kind. In the event that said property is no longer needed, I am no longer employed by SACL or the property is requested to be returned by an SACL representative, I agree to remove the property from the off campus location and return same to Student Affairs and Campus Life IT staff (SATS). I agree to abide by current SACL division, department and/or University standards and guidelines regarding the installation, operation and use of said property. In addition, I understand that I have received this property by choice and, as such, SACL is not responsible or liable for any off campus installations, configurations, trouble-shooting, personal equipment usage reimbursements, maintenance, repair, or collateral damage, etc. incurred from the use or misuse of said property.
I. Property Description:

Model No.: ______________________ Serial/License No.: ______________________
Manufacturer: ________________________________
University Tag No.: __________________ PO #: __________________

II. Location at which property is to be used: ________________________________

III. Period beginning ______________ and ending ________________

IV. Signed by me on (date) ____________________________________________

Print name of Borrower ______________________________ Signature of Borrower/Title

Dept. Head Approval: ______________________________ Date: ______________

V. Comments:

____________________________________________________________________

____________________________________________________________________

____________________________________________________________________

____________________________________________________________________
Appendix F – Procedure for IT review of purchases

University of Massachusetts Amherst
Student Affairs and Campus Life

University of Massachusetts/Amherst – Procedure for IT review of purchases

September 2010

Pursuant to the Board of Trustee policy T08-086, Information Technology Acquisition Policy, and the preliminary University Internal Audit review findings, this is a draft procedure to enable review of IT purchases at the University of Massachusetts/Amherst.

Due to the large volume of such purchases on the Amherst Campus, the recommendation is to have an individual at each Executive Area designated as the IT Procurement Approver for that area. The individual in this position will receive training from the Amherst campus Office of Information Technologies (OIT) on the campus and University IT policy and requirements, sensitive data policy, and Procurement Card Industry (PCI) requirements. Ideally the individual reviewing such purchases should have some level of IT background or knowledge. OIT will remain a resource to assist each IT Procurement Approver in the case of questions, concerns or need for further information on a particular order.

Beginning in September 2010, Student Affairs and Campus Life, Administration and Finance and Office of Information Technologies will pilot the IT Review process for purchases $1,000 and over. The purpose of the pilot group is to work with the review process to develop and document the changes and issues in anticipation of a final policy and full rollout to the entire campus.

Affected purchases predominantly fall under “UU” Information Technology account codes which contain, for example, telecommunications purchases, computer equipment, or software. Noted below are the typical Information Technology expense codes that will need review. However purchases related to information technology could also include items and services as defined below but purchased under other expense codes such as video system under facility equipment 763400 or security software under initial facility purchases 772180. The intent of this policy is to have review of the categories noted below regardless of the expense code used on the requisition.

All requests for bids or requests for proposals that involve any IT will be reviewed by the appropriate IT Procurement reviewer and are not subject to any of the exceptions noted in the list below. Once the bid is awarded and the vendor accepts all language and terms/conditions, the purchase does not need to be re-reviewed.
Information Technology expense categories and exceptions to the review process. Departments may have stricter review policies in place but must review these types of purchases at a minimum. Procurement Buyers will review for these types of purchases; if a department has stricter policies, enforcement must be handled at the department level.

All requisitions that require review should be saved but not submitted to workflow by using the “save and preview” button. An email should be sent to the appropriate IT Procurement reviewer containing the following information along with all appropriate attachments and documentation:

- **Requisition ID**
- **Requesting Department**
- **Contact name, phone and email**
- If unclear by the description on the requisition, a short description

- **Telecommunications related purchases**
  - **Typical Expense Codes to be reviewed include**
    - 734610 Video Conference Service
    - 734791 Telecom Services Voice
    - 734792 Telecom Services Data Lines
    - 757037 Telecom Consultants
    - 761450 Telecom Cabling
    - 763140 Telecom Equipment
    - 766150 Telecom Equip Lease/Purchase
    - 767150 Telecom Equip Rent/Lease
    - 768150 Telecom Equip Maintenance
  - **With the exception of the following:**
    - Purchased by the University’s Telcom Office
    - Cell phone and cell phone plans
    - Offsite offices phone charges

- **IT Equipment – capital and noncapital equipment purchases**
  - **Typical Expense Codes to be reviewed include**
    - 741980 Non-Capital IT Equip
    - 761080 IT Cabling
    - 763100 IT Equipment
    - 763120 IT Equipment/Enhancement
    - 765916 Non-Cap Grant IT Equip
  - **With the exception of**
    - Laptops – PC or Mac
    - Desktops - PC or Mac
    - Desktop or laptop parts – ex: monitor
    - Internal parts such as Ethernet cards or memory
    (Student Affairs and Campus Life requires coordination of all desktop, laptop and related purchase with appropriate IT area (SATS, UHS IT or HRL Tech Services)

- **Software and IT licenses – all software and license purchases and renewals including ‘off the shelf’ software**
Typical Expense Codes to be reviewed include:

- 734800  Software & IT Licenses
- 734810  Software & Support Renewal Fee
- 763180  Computer Software over 100K

With the exception of:
- Software purchased from OIT
- Microsoft Office Suite
- Adobe Acrobat
- SPSS (statistical software)

The following IT areas will be covered by required data protection language in the appropriate maintenance contract, contracts for service, or lease/rental agreements.

- IT equipment maintenance
  - 768100  IT Equip Maintenance

- IT Professionals/Consultants
  - 757030  IT Professionals/Consultants

- IT Rental or Lease/Purchase
  - 766100  IT Equipment Lease/Purch
  - 767100  IT Equipment Rental/Lease

A post-audit review of IT purchases will be performed periodically to look at purchases that did not fall under the formal IT review such as purchases under $1000 or exempted account codes.
Appendix G – Web Site Guidelines/Standards

This document provides guidelines and requirements for Student Affairs and Campus Life (SACL) department and agency (co-curricular organization) web sites. All SACL web sites reflect the professionalism and credibility of the division. We have vast information to share and stories to tell.

The Players

Each web site must identify a sponsor who is a full-time permanent staff member. In larger departments, this can be accomplished with a work group. The responsibility of this staff member/group is to ensure accuracy, currency, content and adherence to guidelines of the web page. The Sponsor must insure that the web site is managed via an organizational account and not an individual or personal account and that the account is kept active.

Each web site/organization must also designate primary and secondary information providers. Information providers are responsible for the development and maintenance of the web page. In small departments the sponsor may fill both roles. This function may also be under contract with a third party.

The sponsor and information providers must agree to abide by any and all related University, Division and/or departmental policies and procedures concerning web sites and IT.

A summary of SACL’s current web sites is attached as Appendix A.

University Requirements

University Relations develops and supports University-approved standards for visual and graphic identity and provides guidelines and tools for consistent branding of the University. As a member of the University community, Student Affairs and Campus Life web sites must adhere to these guidelines. Additional information is available at - http://www.umass.edu/universityrelations/guidelines.html.

The University’s Web Identity Guidelines must be incorporated into all SACL department and agency web sites. They can be found at - http://umass.edu/umhome/identity/web/. These standards apply to all sites representing UMass Amherst schools, colleges departments, programs, units, research centers, and administrative offices. The Web identity guidelines serve several purposes. They brand your site as part of UMass Amherst without diminishing the uniqueness of each area. They make your site easy to find on the Web both within the larger UMass Amherst site and on the larger World Wide Web, and they make it easy to navigate to and from your site and other sites at UMass Amherst.

As published on the University Relations web site as of summer 2010, the University guidelines are -
The Web identity guidelines consist of the following mandatory elements that must be included on each page of your site and updated as necessary. The elements are:

- **Top Banner**: The banner strip across the top of the page brands the site as part of UMass Amherst, links back to the home page and provides a site search.

- **Footer**: The page footer shows site ownership, both as part of UMass Amherst and within the specific department or group with the university.

- **Page Title**: The page title displays in the border of each Web page and is an additional way to identity your site. It also helps to make the site identifiable in Google and other search engine results.

For more information on banners, footers and page titles, visit http://umass.edu/umhome/identity/web/.

- **Colors and Fonts**
  The color palette of each site should include UMass Amherst maroon and the campus seal and/or approved wordmark should be prominently displayed on each page.

  The official colors of UMass Amherst are maroon, gray, black and white. When designing for the Web, use hexcode #881c1c for maroon. You may use other colors as accents only.

  Verdana is the recommended font for body text. Georgia is recommended for headings. Graphic elements such as headers and buttons can be designed using Sabon, Centaur or Frutiger. These are not Web-safe fonts and should be used only in graphics.

- **Seals, Logos and Wordmarks**
  When displaying UMass Amherst logos and seals, display them only in the official colors provided. Do not change the colors.

  The UMass Amherst Seal, Wordmark, and the Wordmark/Seal combination are available for download below. Each archive (ZIP or SIT) contains a selection of image sizes, in the specified color, in GIF format.

  These marks may be rendered in black, white, gray or maroon only. Please note that the interior portion of the UMass Amherst Seal is transparent to the background, not white.

  Approved logos and wordmarks can be found at http://www.umass.edu/universityrelations/seals.html.

**SACL Standards/Requirements**

1) Both the U and M should be capitalized in reference to UMass.

2) All department web sites must provide a link to the Student Affairs and Campus Life web site (www.umass.edu/stuaf) from the main departmental page.
3) All department and agency web sites should have a Contact Us page or link.

4) All department web sites must include a Site Map or Site Index link.

5) SACL department web sites must be developed in the University's Content Management System (CMS) unless a waiver is requested and approved.

6) SACL agency web sites must be developed in a non-proprietary HTML editor like Dreamweaver.

7) Back up copies of web content must be saved in the appropriate network environment not on an individual's workstation.

8) Procedures must be in place to periodically review web content.

9) Procedures must also be in place to review updates to avoid typos, awkward language, mis-alignment, inconsistent tense and style, and broken links.

10) Do not use copyrighted materials without the express written permission of the copyright holder. Information about copyright can be found at the U.S. Copyright Office at [www.copyright.gov/circs](http://www.copyright.gov/circs).

11) When using photographs of individuals where the person is recognizable a written release is required. Releases are not required from people who are identifiable in a photograph of a public place, provided the photograph is related to the subject matter on the page and the individuals are not the focus of the photograph ie. Move in activity around residence halls; activity on campus center concourse.

12) Sponsors and information providers must understand the importance of providing accurate and up to date information to an extended community. It is suggested that effective writing be structured as an inverted pyramid. The most important information should be communicated first. Additional information should be presented in descending order of importance. You never know when someone is going to stop reading!

13) Use of Flash must be pre-approved and necessary for the page. The use of Flash must provide the option to communicate your information better to your intended audience than standard html. Send requests to Anne Bourbeau at abourbea@admin.umass.edu from the University Relations Web team.

14) For sites that are not maintained over the summer and/or breaks, a 'Extended Absence' page must be designed to provide information about when the page will be active again.
SACL Acceptable Use Policy User Agreement

I hereby acknowledge that I have read and understand the Data and Computing Policies, Standards and Procedures for the University and SACL. I agree to abide by these policies and ensure that persons working under my supervision abide by these policies. I understand that if I violate such rules, I may face legal or disciplinary action according to applicable law or departmental policy.

I hereby agree to indemnify and hold the University of Massachusetts and its officers, trustees, employees, and agents harmless for any loss, damage, expense or liability resulting from any claim, action or demand arising out of or related to the user’s use of University-owned computer resources and the network, including reasonable attorney fees. Such claims shall include, without limitation, those based on trademark or service mark infringement, trade name infringement, copyright infringement, unfair competition, defamation, unlawful discrimination or harassment, and invasion of privacy.

Name (printed): ____________________________________________

Signature: ____________________________________________

Date: ____________________________________________