Applications

Applications development in Student Affairs requires that the following conditions be met:

1. Applications must be SAIT approved and compatible with SAIT systems. Development must be done using the following: SQL, ASP, and ASP.net.
2. The submission of documentation from the requesting department detailing a clear and concise explanation of the application desired.
3. The establishment of a development, implementation, review, and approval timeline.
4. Significant application additions and/or changes after implementation must be SAIT approved and a new timeline established.
5. All non-SAIT student/staff involved in development are required to coordinate with SAIT applications personnel and receive approval from SAIT.
6. SAIT reserves the right to remove or block applications that conflict with other applications, interfere with server processes, have security risks, or fail to meet USC/Student Affairs standards.
7. SAIT and VP approval must be obtained for any Student Affairs site not located on a USC or SAIT server.
8. All websites must adhere to the USC and Student Affairs Graphics Identity policy.

Consultants & Non-SAIT Tech Staff

Consultants:

Consultants are permitted to help departments in the areas of applications development but are subject to the following limitations:

1. Consultants are required to coordinate with SAIT applications development personnel and all work must be approved before going live.
2. Applications constructed by Consultants that are deemed to be unstable or insecure will be disabled and/or removed until corrections are completed.
3. Consultants must adhere to both USC and SAIT development standards (font, identity, programming languages, etc.).
4. Consultants must maintain/adhere to the required USC established insurance limits as well as all USC policies governing non-USC employees.
6. Consultants must agree to keep all sensitive University data on USC servers. No data must leave USC or reside on non-SAIT approved equipment.

Non-SAIT Technical Staff:

Non-SAIT technical staff are not permitted in Student Affairs with the exception of existing positions or new positions that are subject to the following conditions:

1. New technical support positions outside of SAIT are not permitted without SAIT shared or total supervision of the technical personnel. Exceptions may be made based on the nature of the position and the specific duties involved as determined by the VP’s Office.
2. Existing technical support personnel outside of SAIT are required to adhere to all SAIT policies.
3. Existing technical support personnel outside of SAIT are not permitted to alter computer configurations, install software and/or hardware without prior approval from SAIT. All such alterations may be removed upon discovery. Special consideration and exceptions may be made based on specific conditions and justification.
4. Non-SAIT technical staff must provide SAIT with all administrator passwords.
5. Non-SAIT technical staff must keep detailed documentation regarding their systems and provide a copy of the documentation to SAIT.
6. Non-SAIT technical staff and the respective department agree to be held responsible for any security, performance, and stability related problems resulting from work done without SAIT’s knowledge or approval.

Computers and Equipment:

1. All departments are required to work with SAIT for specifications when considering purchasing new computer related equipment. This includes CPUs, monitors, printers, scanners, and other devices. Without compliance with SAIT specifications, SAIT does not guarantee a fully functional device or access to SAIT controlled resources.
2. All technical equipment purchases must be purchased by SAIT. Departments must contact SAIT to arrange for equipment purchases. SAIT will order all computer related equipment for departments and bill each department for equipment.
3. Computers must be processed (registered with SAIT and ITS) before setup on the USC network. Registration must be done by SAIT personnel.
4. A copy of all supporting peripheral software (printer drivers, etc.) must remain within SAIT for installation, support, and troubleshooting purposes.
5. The Division is PC based. New MACs for staff are not permitted in the Division without justification and SAIT approval. This policy does not include replacement for existing MACs. Technical support for MACs is limited; outsourcing support (at the department’s expense) may be required.
6. SAIT does NOT support or authorize departments to setup peer-to-peer networks or wireless networks and will remove such setups upon discovery.
7. Departments are not permitted to have servers of any kind. Discovery of servers outside of SAIT control will be removed from connection to both SAIT’s and USC’s network. The exceptions are servers that were established prior to SA Core Infrastructure implementation (September 2001) and such servers cannot be altered from their original function (ex. a web server turned into a file server, etc.). Other exceptions may be permitted based on the department’s specific need and ability to maintain and support the equipment.
8. Stand-alone (not connected to the SA Domain) computers must conform to SAIT’s software, licensing, and hardware requirements or network ports will be disabled. These units require justification and must be setup by SAIT techs. Non-SAIT registered equipment will be disabled from the USC network upon discovery.

9. Mobile devices such as Phones and PDAs must be of a make and model that is supported by SAIT in order to receive full connectivity and support. Contact SAIT for verification and ordering of Business phones and other mobile equipment.

10. Downloading or file sharing of copyrighted material without express permission of the legal owner is forbidden. Movies, music, etc. are not to be downloaded or stored on Student Affairs computers or other media. All users are required to review and adhere to all USC and ITS policies regarding the downloading of copyrighted material.

11. University policy requires that all laptops and external data devices such as USB Flash drives be password protected and use data encryption software. SAIT’s policy forbids storing any sensitive data on laptop computers, portable/removable media, or on internet storage (the Cloud). Laptop computers must not contain any confidential or “sensitive” data including student, faculty, or staff profile information, payroll or other University protected data. Exceptions require data protection using encryption software. For a list of password/encrypted capable and approved devices, help with data encryption, or for assistance and further details regarding data protection and University standards, please contact SAIT.

Data-Local, Network files, and Backups:

1. All users are responsible for the files and folders on both their local and network directories. Photos, movies, music, and other non-mission critical or non-business related files are not permitted on the SAIT File Server and will be removed when discovered.

2. Running applications directly from the SAIT File Server is not permitted and these applications will be removed when discovered.

3. All users are responsible for abiding by their assigned SAIT File Server space quota limits. If you need more than the standard allocation, please contact SAIT. SAIT will require justification for the increase.

4. All users are responsible for maintaining the security of their workstations and passwords. This includes not divulging passwords or posting passwords on monitors, desks, walls, etc., not leaving logged in workstations unattended, and logging off the network at the end of the day.

5. Network directories and files of individuals no longer affiliated with USC are transferred to another staff provided that the department makes such a request. Directories and files of prior employees not transferred to another staff are permanently deleted.

6. SAIT highly recommends that employees who save data to their local drives backup such data. Data not on SAIT servers are not backed up by SAIT.

7. Student Affairs policy forbids storing non-encrypted data on internet cloud storage sites. While cloud services may be used, SAIT does not support cloud services.

E-mail:

1. Student Affairs e-mail system utilizes ITS provided Unix and Web e-mail accounts. All staff and students are provided with a Unix e-mail account by ITS when first hired or first registered by USC. The setup process usually takes 1-2 weeks.

2. All users are responsible for maintaining their e-mail accounts. Maintenance of e-mail accounts includes all of the ITS guidelines and regulations listed on ITS’s website, [http://www.usc.edu/ITS](http://www.usc.edu/ITS).

3. Users of both USC and SA mail systems are required to stay within mailbox quota limits, i.e., users need to periodically achieve or delete messages.

4. Mobile devices - Please contact SAIT for a list of supported mobile devices.
Relationships:

1. AIS and SIS are USC services outside of SAIT control. Users requesting services from these organizations should contact their appropriate department business coordinator.
2. SAIT and all Student Affairs users are required to adhere to all of the policies set forth by AIS and SIS. AIS and SIS policies can be viewed on USC’s website or information can be obtained from department coordinators.
3. SAIT and all Student Affairs users will abide by all of the rules and regulations of ITS. ITS policies can be found on USC’s website or via links on SAIT’s website.
4. ITS provides the networking backbone (ports, ethernet lines, routers, switches, internet access, and e-mail services) to the Division of Student Affairs. SAIT will arrange, assess, and coordinate installation and maintenance of backbone services for all users.
5. Departments are required to submit written requests to SAIT via memo or e-mail for installation and termination of backbone services. Departments are not permitted to contact ITS for backbone services. These services will be managed by SAIT.
6. Departments are not permitted to arrange for ITS to install, purchase, or maintain servers or other equipment.
7. SAIT is not responsible for failure or maintenance of AIS, SIS, Backbone, or other University controlled services, but does support the software needed to access these services.
8. The Student Health Center maintains its own fully functional and independent technology department. Thus, SAIT is not responsible for supporting this organization.
9. SAIT will track and coordinate billing and other information for ITS backbone services for all departments; however, departments are also required to keep track of the number of network ports, locations, and other ITS services/resources. This includes telephone and phone jack installation and maintenance.
10. SAIT is not responsible for supporting the ITS controlled Library or other computer labs and/or equipment.
11. All USC Telecom requests and services are coordinated through SAIT. Departments are required to contact SAIT Administrative staff for matters concerning USC Telcom (phones, phone jacks, etc.).

Resource Access:

SAIT does NOT currently provide and/or permit the following services:

1. Access to network resources from outside of the USC Domain. Exceptions may be granted based on job function and/or collaboration with non-SA personnel with proper justification.
2. Training on OS or software packages (both approved and non-approved).
3. Technical support outside of the normal USC business day (8:30am - 5:00pm, M-F).
4. Support for outside agencies, consultants, developers, or internet service providers.
5. Support for non-approved and/or non-MS compliant hardware such as PalmPilots, Jaz Drives, Blackberry devices, and SCSI devices.
6. Support for non-approved and legacy operating systems (Windows 95, 98, ME, etc.).
7. Support for non-approved and legacy software applications.
8. Website development on ITS's CWIS server.
9. Support for remote control software, such as Timbuktu, PcAnywhere, Laplink, etc.
10. Setup or support of Virtual Private Networks for home users; however, we will provide installation information in conjunction with ITS.
11. Support for Student Organizations, which includes network, website, and email services.
12. SAIT does not support the use of external email systems such as hotmail and gmail.
Security:

1. All Student Affairs Staff and Students are responsible for maintaining the confidentiality of passwords, local data, and network data. Failure to appropriately maintain confidentiality may result in the removal or alteration of network access.
2. Users are not permitted to alter the security settings of workstations which include local and network account creation, deletion, or alteration.
3. Altering security settings may result in the removal of access.
4. Users are not permitted to install software or alter existing software configurations without SAIT approval. Such software or altered configurations will either be reconfigured or removed.
5. Users are not permitted to install, add, or alter workstation hardware.
6. Users are not permitted to open (remove the CPU cover panel) any computer.
7. Users are not permitted to disable or remove security software.
8. Users are not permitted to install remote control software without justification and SAIT approval.
9. Users are not permitted to use “hubs” or other networking devices that may interfere with the overall operation of SAIT’s or USC’s network including wireless.
10. Users are not permitted to "experiment" with workstations using scripts, trojan horses, port scanners, or other potentially harmful software.
11. Users are not permitted to access or alter a workstation’s BIOS.
12. Departments are required to physically secure computers and other equipment via locked offices, alarms, or lockdown mechanisms. SAIT is not responsible for equipment that has been stolen.
13. Departments are required to inform SAIT of Staff or Students that are no longer employed by Student Affairs so that proper account and access removal can be performed.
14. Departments must not setup wireless routers or other Wireless connections without SAIT approval. Wireless access is controlled and maintained by ITS. Contact SAIT for help with wireless connectivity.

Security Password Policy:

1. All users must have 8 characters, upper and lowercase letters, and numbers.
2. Passwords must be changed every 180 days.
3. Account lockout is enforced after 7 bad attempts.
4. Accounts are locked for 30 minutes.
5. Passwords cannot contain the username.
6. Passwords cannot be reused for the last 24 passwords used.
7. Users are automatically prompted for password changes.
8. Users must type a password after 30 minutes of inactivity due to required screen saver.

Data Security:

1. Users are required to encrypt or password protect any files that contain confidential/sensitive data. This includes files that are on the network shared directories.
2. Users are not permitted to create, copy, delete, modify, or transfer any files that contain confidential/sensitive data to non-Student Affairs equipment. This is includes USB Flash Drives, External Drives, CDs/DVDs, and Home or Internet locations (Cloud Services).
3. Users must use AES 256 Bit encryption on laptops, USB Flash Drives, and External Hard Drives.
4. Users are not permitted to share or otherwise distribute files that contain confidential/sensitive data with unauthorized personnel.
5. Users are not permitted to use personal USB Flash Drives and/or External Hard Drives without prior approval from the Department’s Director and verification from SAIT that the devices are enabled for AES 256 Bit data encryption.
6. Users will adhere to the Student Affairs Credit card processing policy http://sait.usc.edu/crdpolicy.pdf
Software:

1. Departments are not permitted to purchase their own software, including upgrades to existing packages, without SAIT approval. SAIT reserves the right to refuse installation of software not purchased through SAIT, purchased without SAIT approval, or software that does not have the appropriate licensing.
2. While SAIT makes several software packages available, the only software packages currently supported is the Microsoft Office Suite and the Adobe Creative Suite. Other packages are available but support will be limited.
3. Departments with existing software packages not supported by SAIT are required to upgrade to the version that SAIT deems necessary for compatibility, functionality, and security with Student Affairs’ current environment.
4. SAIT will install, configure and troubleshoot software; however, SAIT is not responsible for Staff training on any software package.
5. Users will not copy or distribute software without SAIT approval and appropriate licenses.
6. Software not approved or provided by SAIT, including downloaded utilities, video programs, chatting programs, etc. are not permitted on any computer in Student Affairs.
7. Downloading of applications and other files (movies, etc.) from the internet to either local or network drives is not permitted unless such media is business related (seminars, demos, tutorials, etc.) and does not involve copyright infringement.

Software Billing:

1. SAIT will purchase and provide the standard software packages (MS Office Suite and Adobe Creative Suite).
2. Software not included in the standard packages will require SAIT approval and be purchased by SAIT with the understanding that SAIT will be reimbursed by the ordering department.
3. Approved operating system software and licensing will be distributed, maintained and purchased by SAIT only.

Websites:

1. SAIT does not support student websites.
2. Departments are required to locate their websites on either ITS’s CWIS server or the SAIT web server, not on the ITS student servers. Locations on non-USC servers require SAIT and VP approval.
3. SAIT does not update or maintain departmental websites. It is the responsibility of the individual departments to ensure current data and to comply with all ITS website regulations and the USC/Student Affairs Graphics Identity policies.
4. As authorized signers for the Division, SAIT personnel will request account creation and rights for departmental webmasters (either student workers or staff) but only at the explicit written request of the department’s director.
5. Website accuracy and content is the responsibility of individual departments, SAIT takes no responsibility, but does make periodic scans and may require departments to make site changes or disable a site that fails to meet SAIT, ITS, and USC policies.
6. Student Affairs University Publications is responsible for USC Graphics Identity compliance of Student Affairs websites.

*Legal Notice:*

All computers and other technology related resources are the property of Student Affairs and the University of Southern California. By logging on to any Student Affairs computer, users are agreeing to abide by University, ITS, and SAIT policies and agree to periodic auditing of technology resources.
SAIT reserves the right to change or amend policies. Users should periodically check the SAIT website for the latest version of this document.
For questions or clarification please contact SAIT at 213-740-5244.