Student Affairs Technology/Computer Labs Program Review

Summer/Fall 2009

Self Study Team

- Clayton Oyler – Director, Student Affairs Technology
- Chip Coleman - Programmer Analyst
- Dave Taylor - Systems Analyst
- Sarah Padilla - Testing Center Support Specialist
- Carey Anson - Coordinator, Student Computer Labs
- M. Omar Alam - Student Lab Technician/STAs

Site Review Team

- Jonathan Karras - Information Technology, Network Systems - Weber State University
- Geetha Sendhil - Executive Director, Student Affairs Technology - University of Nevada, Las Vegas
- Dr. Alden Talbot - Telecommunications and Business Ed, Dept. Chair - Weber State University

Weber State University Mission Statement

Weber State University offers associate, baccalaureate and master degree programs in a broad variety of liberal arts, sciences, technical and professional fields. The university provides excellent educational experiences for its students through extensive personal contact among faculty, staff and students in and out of the classroom. To accomplish its mission, the university, in partnership with the broader community, engages in research, artistic expression, public service, economic development, and community-based learning experiences in an environment that encourages freedom of expression while valuing diversity.

Student Affairs Mission Statement

The Division of Student Affairs promotes student learning, well-being and success through comprehensive services and programs provided in an inclusive environment. Student Affairs serves the needs of a diverse student population by offering educational experiences, leadership opportunities, and academic support which advances the social, intellectual, cultural, and civic development of students.

Student Affairs Technology Mission Statement

Student Affairs Technology (SAT) at Weber State University is committed to uphold the mission of Student Affairs by developing, enhancing and supporting technologies used by students, faculty and staff.

Table of Contents

1. Unit Mission, Goals, and Outcomes

Student Affairs Technology (SAT) has four main units providing service to the Division of Student Affairs. Each unit has a specific mission, but due to the nature and limits of our departmental resources, we have overlapping responsibilities. Our goal is to provide the technology support and services to the Division, be a liaison to the Information Technology Division, and support student technology needs.

Student Computer Labs

The Student Computer Labs and support staff strive to provide the latest in technology for students in a collaborative, stable learning environment while enhancing the work experience of student staff through professional development.

The open labs provide students access to technologies needed to succeed in their academic endeavors. These services are free to all students and include: managed printing, trained on-sight student lab technicians, and a full catalog of campus standard software

While the student computer labs focus on student learning outcomes, each of the following units offer dedicated support for all Student Affairs departments. These units provide the technology service needed for individual department pursuits to support the overarching goals and outcomes for the Division.

Student Technology Assistants (STA)

The Student Technology Assistants provide first level technical support to the Student Affairs division staff.

STAs provide first line technical support for the Division and are a primary liaison with the campus IT help desk to ensure that staff are help able to receive timely help with technical issues.

- Provide service no later than 48 hours after initial call
- Install and configure new technologies in departmental offices
- Corroborate equipment inventory within the division and campus Property Control

Testing Center Support

Testing Center Support provides timely technology support to faculty and the Student Affairs Testing staff and centers.

Testing Center Support is an integral component of the SAT department. This unit helps to maintain a partnership with the Testing Centers and allows for new and improved technologies to be deployed and maintained. Testing center support responsibilities include: immediate support for all Student Affairs testing centers, investigation into alternative test delivery systems, desktop support for testing

staff, and collaboration with other divisional services to ensure compatibility and integration with WSU Online, Information Systems and Technology testing and other testing needs.

Student Affairs Systems

Student Affairs Systems collaborate to meet the technology needs of the Division by providing necessary infrastructure, data management, development, education, and support.

Student Affairs Systems staff provide unique services to many departments within Student Affairs that require specialized equipment, programming, and support. Examples include: server management, database management and creation, data warehousing and support, website management and training, information systems security, and technology education.

2. Core Programs and Services

Student Computer Labs

The Student Computer Labs provide a wide range of services to students, faculty, and staff on campus. The primary function of the labs is to provide free access to technology to all current students in locations and with hours that will accommodate the largest majority of students possible. The student labs are funded primarily through student fees. WSU's Policies and Procedures Manual, section 2-12 (Appendix A), directly address the purpose of the open labs. Services and programs beyond the PPM are managed on a by need basis and handled by the Computer Lab Coordinator Committee. This committee is comprised of all the Academic Support Centers and Programs administrators. During monthly meetings, this group makes decisions concerning lab policies, student hours, and other outstanding issues.

Core programs and services associated with the labs include:

- ***Student access to technology in an open and inclusive setting***
  - Computer labs are accessible to all WSU students regardless of major or college. The labs have 220 dual boot iMacs and 250 Windows computers. Labs are conveniently located in the Davis Campus, Roy Campus, Shepherd Union, Lampros Hall, Social and Behavioral Sciences, Natural Sciences, Dumke College of Health Sciences, Goddard School of Business, and Elizabeth Hall.
- ***Managed print services for labs and other campus entities***
  - The labs provide students with equitable and managed printing services through the Pharos printing system. Each student is allotted 150 ($4.50) free prints per year on their Wildcat card. After these funds are exhausted, students can print at a cost of $0.06 per page (or $.03 per side). Color printing is available in the Shepherd Union, Lampros Hall, and Davis Information Commons for $0.15 per page. Students are provided access to wireless printing from their personal laptops. These services are supported in departmental labs that fall outside of the Student Affairs Division, such as the Library and the Visual Arts Lab.

- ***Professional development and growth for student staff***
  - The employment structure for student staff within SAT is designed to promote student growth and development by way of continuous professional development. Training and assessment of students' growth is conducted through collaboration with the Office of Workplace Learning and Student Affairs Assessment. The positions within student lab aide employment include: general lab aides, level I aides, level II aides, and team leaders. These levels reflect different responsibilities and wages.
- ***Collaboration with faculty for enhanced classroom learning***
  - The labs provide computer classrooms to faculty for teaching and curriculum. In faculty collaboration, these classrooms are designed to promote teaching and learning.
- ***Knowledgeable on-site support***
  - Each lab has an on-site student staff who provides students with customer service and support in the lab facility. Staff members are evaluated every semester on their technical knowledge and job performance.
- ***Configured computer systems***
  - The SAT department rotates an average of 120 computers each year. The purchasing schedule is based on a 3-4 year rotation plan for each individual lab. The computers are configured based on the technology available and the needs of the students and faculty. All of the computers we rotate from the open labs are put back into service on campus through formal request process and in cooperation with the Academic Resource and Computing Committee. (Appendix A [PPM2-12])
- ***Maintenance of, troubleshooting for, and repair of new computer lab equipment and software***
  - Lab software and hardware are maintained and supported by the computer lab support staff, which includes a professional computer technician and student technician. These technicians are trained to specifically service the open lab computers. In addition, the support staff is also responsible for researching technologies that improve the efficiency, support, and maintenance of equipment.
- ***Collaboration with other University IT areas and external system vendors***
  - The computer lab staff collaborate closely with University Information Technology departments including: network management, technology services, and multimedia services as well as WSU contracted external vendors.

The computer labs support the mission of the Division by providing professional growth and development opportunities for student staff in an environment that supports the academic curriculum and thusly contributes to their learning and success. New programs and services in the labs are initiated through research and by observing student behavior and learning styles. These behaviors are also studied through student surveys, suggestions, and dialogue with students and faculty.

Outreach, Campus Relations, and Collaborations

Students purposely seek the computer labs, so limited advertising is needed to support the service. We place information in Student Affairs Divisional publications dictating times and locations. We place a ¼ page ad in the student newspaper, the Signpost, for the Welcome Back addition in which we advertise job opportunities for students wishing to work in the labs. Tri-

fold handouts and flyers are prepared and placed in each lab. These publications provide students with detailed information concerning lab locations, hours of service, and other lab specific information.

Student and professional staff are provided with opportunities to take part in community service through donating time and services to various local and national organizations. One consistent service opportunity is in the form of annual conference technology support for the Prevent Child Abuse Utah Foundation. The student labs also collaborate with the Student Affairs Division Community Involvement Center to offer service opportunities to lab aides seeking advancement to the level II lab aide positions.

Core Changes in Computer Lab Program and Services
The program and services in the student computer labs have evolved over the past five years. These changes involve the management and support of equipment, which includes a change in the computer rotation from three to four years, integration of newer technologies such as utilization of Apple multi-boot computers with active directory. The labs have improved methods of imaging and updating computers by utilizing the latest in desktop imaging and control software (e.g., Ghost, Deploy Studio, Refit, Apple Remote Desktop). The labs have also designed and implemented physical learning spaces through providing students with additional desk space. The Apple iMac Labs allow student both a choice of operating systems and also provide substantially more desk space to students. This was a long time request by students on surveys given each semester, and this new system has allowed us to provide students with this requested space.

Anticipated Changes in Programs and Services
The success of the multi-boot Apple platform and the positive feedback we have received from students demonstrates that these changes are a successful solution for the labs in the future. As such, we will continue implementing these platforms until they are available in all labs.

Student Technology Assistants (STAs)
The Student Technology Assistants, introduced in 2006, provide first level technical support for the Student Affairs staff. Support includes desktop/mobile, audio/visual, software and networking support. This service was developed to meet the needs of the Division for first level support in technology by technicians familiar with the role and needs of Student Affairs. This service was designed in collaboration with the existing WSU Service Desk in order to relieve them of many of the requirements that different departments within Student Affairs were demanding.

Core programs and services associated with the Student Technology Assistants (STAs) include:

- ***First level technical support for the Division***
  - Student Technology Assistants provide support for all the technology needs of the Student Affairs Division. The areas of technical support include software, hardware, and networking. The STAs strive to provide service within 48 hours of the initial contact by a staff member. The STAs also manage the escalation of issues to the appropriate services within Student Affairs Technology or other Information

Technology support departments or the Information Technology Division support personnel.

- ***Collaboration with University entities and external vendors***
  - Having a detailed functional knowledge of the current hardware and software needs of the departments and individuals in the Student Affairs Division allows the STA to collaborate with external vendors in the event of technical problems, warranty replacement or necessary replacement of hardware or software.
- ***Deployment, configuration, and support for Division staff technologies***
  - The STAs are trained with the capability to image a variety of machines, migrate data, upgrade machines, and troubleshoot a variety of technology issues. The development of a STA Wiki (http://sat.weber.edu/wiki) allows STAs and staff alike to resolve known technical questions often reported by staff.
- ***Division inventory services***
  - The STAs are responsible for maintaining and updating the inventory of all department desktops. This is accomplished by installing custom software on all the staff machines across the Division that allows the retrieval of pertinent inventory information. This database enables SAT to track the age of the computers, provide an inventory list of all computers in a department if necessary for an inventory audit, and issue updated listing of system information for IT security reasons.

The Student Technology Assistants follow a training and employment structure that is designed to closely resemble that of the Student Labs. New services provided by the STAs are initiated through research and by observing staff needs. These needs are also studied through staff surveys and suggestions.

Marketing and Outreach

The STA service is advertised via flyers given during Divisional retreats and meetings in order to remind the staff of the STAs' contact number and the services provided.

The STAs have the same opportunities for outreach as the student computer lab aides. This provides the student staff the chance to collaborate with a wide variety of campus personnel, mainly in the Information Technology areas.

Core Changes in Programs and Services

The STA program has been continuously evolving within the Division since its conception in 2006. The first year of service was a struggle because of the need to learn the demands of the Division. Through thorough training of staff and expansion of service available, the STAs have seen positive feedback via assessment of the service.

Testing Center Support

The Testing Support Specialist's primary responsibility is to provide immediate support for the Academic Support Centers and Programs (ASCP) Testing Centers. Since computer based testing has expanded at a rapid rate, the specialist position was deemed an essential addition in order quickly and efficiently manage testing issues to allow for a seamless testing operation for students, staff, and faculty.

Core programs and services provided by the Testing Support Specialist are:

- ***On-site incident response for all online testing software.***
- ***Testing center workstation support***
  - Technical support is provided for academic and non-academic testing (e.g., military testing and other community based tests) for WSU, other universities, and the community at large. This includes all staff computers administering the tests as well as the testing center lab machines.
- ***Administrative system support***
  - Provide administrative support for the testing tools used by the testing centers.
    - Administrative support of the following testing tools, services and servers: ChiTester and PaperChi, Accuplacer, Compass, CLEP, Miller Analogy Test, Digital Desk paper testing management, Kryterion
- ***Research, test and implement new hardware and software***
  - Technical support is provided for changes, upgrades, and new hardware and software employed by the testing centers. The specialist ensures that special disability requests are met by testing center equipment.

Core Changes in Programs and Services

During the transition time for the new Testing Support Specialist, the SAT department has increased its crossover support for the testing centers. We have increased the community based testing offerings such as Bureau of Emergency Medical Services (BEMS) at the Davis Campus testing center, replaced Compass computer based testing placement software with Accuplacer. The paper testing system "Scout" was no longer supported by the vendor so a replacement was found with "Digital Desk." All computer stations have been replaced in every testing center as of Summer 2009 as they had not been changed out in over five years.

The Digital Desk paper testing management software is now in a transition to a new system developed by the Continuing Education Department at WSU. This will tie into our current online based testing software ChiTester and will offer local support for paper testing services. The testing centers are investigating the need to place computer based testing in the Natural Science testing center, which currently only provides paper testing.

Student Affair Systems (SAS)

Student Affairs Systems provides the development, support, and training for the Student Affairs Division in a myriad of services. Services provided focus around department specific needs for servers, programming web applications, security, data management and reporting, and Divisional technology training.

Core programs and services provided by the Student Affairs Systems unit are:

- ***Administration of Student Affairs database systems.***
  - Database systems provide an ability to collect sets of data that can then be shared by users in Student Affairs. The reliable persistent storage of information is crucial for record keeping, scheduling, and reporting. SAT databases store information for applications that include Tutor Scheduling, Goal/Initiative Tracking and Reporting, registration of clubs and organizations, student body elections, Nontraditional childcare registration, Wilderness Recreation equipment and transactions, Union

management, Computer Lab surplus acquisition information, Employee Recognition, and Division statistical records.

- ***Provide the information technology infrastructure for the Student Affairs division.***
  - To fulfill Divisional needs, Systems' Programs partners with University IT to provide firewall, network, hardware, and software access to Student Affairs departments and staff. Depending on need, they help to facilitate private networks, virtual private networks, servers, and specialized equipment and software for departments.
- ***Creating and managing Student Affairs websites throughout the division.***
- ***Supporting application production and project development.***
  - Student Affairs Systems designs and develops online and other server based technology that is required by any Student Affairs department using the current best practices of development.
- ***Ensuring information system security.***
  - SAS provides a layered defense for the protection and management of crucial data, systems, equipment and personal information. This requires coordination with the University IT security plan included in the PPM in sections 10-1 and 10-2 (See Appendix A). We also support the University IT Division's plan to follow the best practices and concepts laid out by the Information Technology Infrastructure Library (ITIL).
- ***Educating, advising, and supporting systems users.***
  - SAS provides system designs, price quotes, and implements a myriad of support applications for departments in the Division. SAS continually trains staff on using system programs and supports users in order to promote efficiency and effectiveness of their programs. This includes unique systems demanded by specialized departments including:
    - Counseling & Psychological Services Center
    - Student Health Center
    - Services for Students with Disabilities
- ***Data analysis emphasis on usage, forecasting outcomes, trending, and fiscal information***
  - SAS provides units with information upon which rational, objective, and useful decisions can be based. This information is recorded via student logins at the computer labs, student data provided by University data services, and budget reports.

Outreach, Campus Relations, and Collaborations

Close collaboration with the IT Division is a necessity for SAS to ensure compliance for best practices acknowledged by the University. SAT and IT have an established relationship and continue to strive to keep information continually flowing between each entity to enable services provided by the respected areas.

Core Changes in SAS Programs and Services

All web pages have been redesigned and moved to the University's "Site Management Tool" to better represent the new look of the main WSU web site. New image tools and event tools were introduced to allow individual departments to add graphics to their department pages. A Student Affairs portal channel was developed to allow personalized Student Affairs applications to be delivered to staff. This enables the development of the online tools such as the Division Skill

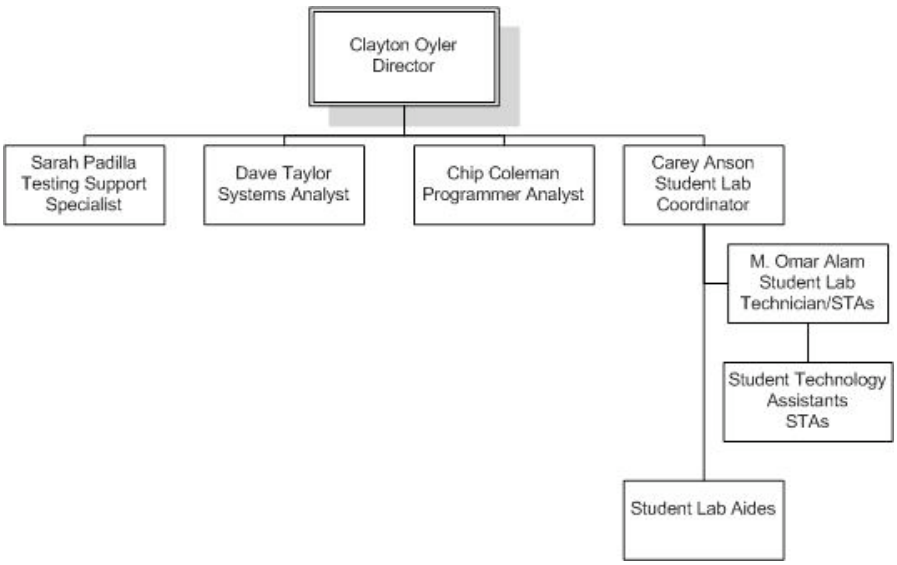
Sharing Index, Builders of Excellence recognition system, Kitten Kare (for hourly childcare), Wilderness Recreation's rental management, tutor management, 6 column model goal tool, and other departmental tools.

Anticipated Changes in Programs and Services

The main Division website is being redesigned to reflect updated information and to keep the sites looking fresh since being redesigned over three years ago. This change will offer updated tools and navigation to reflect student needs. New virtual servers to transition out physical servers are in progress to better service our division's need for security and availability of services. New implementation of other services and programs are usually dictated by departmental needs in the Division.

3. Leadership and Staffing

There are six professional staff and 55 student employees (i.e., 51 Lab Aides and 4 STAs) in SAT. (See Appendix B)



SAT schedules monthly department meetings and individual one-on-one meetings to disseminate information and to report on assignments. Decisions are generally discussed with the entire staff, and feedback is encouraged. If crucial issues are to be handled, the director will make the final decision on how to handle assignments. This is after a discussion has been held by all involved and key people understand the details of an assignment. The department relies on instant messaging for immediate communication and email/phone. Ad-hoc meetings are also scheduled on a need-to basis.

The Student Labs communicate within monthly team meetings held for student managers (Team leaders). This information is then is disseminated down to individual labs and student employees. The Student Lab Coordinator leads these Team leader meetings.

Staff & Responsibilities

Professional Staffing

SAT have had limited need to perform professional staff recruitment and searches as most of our staff have been at WSU for many years. During such time when we need to perform a candidate search, SAT have found that the technology industry is very volatile. Depending on the economy, we will have a candidate pool size adjusted by that measure. So far, SAT have been

very successful in professional staff recruitment by using the standard statewide newspaper advertising through Human Resources and the WSU job website.

Director, Student Affairs Technology
Responsible for managing department and providing leadership and program development for SAT. Meets with other units inside Student Affairs to collaborate and plan technology needs. Meets with areas outside Student Affairs to ensure that compliance standards are met and collaborations with external entities continued.
Qualifications:
Bachelor's degree in technology field or equivalent
6-10 years IT management experience

Systems Analyst
Liaison with other departments in meeting technology needs
Provide server, database and application support to department
Provide department specific support
Qualifications:
Bachelor's degree in CS, IT or equivalent
1-5 years IT industry experience

Systems Programmer
The Systems Programmer maintains SA Divisional computer software and hardware operating environments. The Systems Programmer is responsible for application development & maintenance, database management, intranet infrastructure, network security, hardware & software evaluation, client training, and University IT collaboration.
Qualifications:
Bachelor's degree in CS, IT or equivalent
1-5 years IT industry experience

Testing Support Specialist
Provides technology support to seven WSU testing centers. Support, troubleshoot, develop and maintain computerized testing system software and hardware. Research, design and implement technology to meet testing center needs. Train testing center staff on system upgrades and changes as needed.
Qualifications:
Bachelor's degree in CS, IT or equivalent
1-5 years IT industry experience

Student Computer Lab Coordinator
Provides leadership and program planning for the student computer labs. The position requires working in close coordination with other IT departments. Support, troubleshoot, develop and maintain computer systems for student use in computer labs. Research, design and implement technology to meet current lab needs and trends. Provide training and professional growth for student employees.
Qualifications:
Bachelor's degree in CS, IT or equivalent
1-5 years IT industry experience

Student Lab Technician
Primary responsibility is to provide desktop hardware and software support to all open student computer labs and departments. This includes setup and configuration of new computers, diagnosing and resolving hardware issues. The position requires working in close coordination with IT departments on campus. On a semester or yearly basis, the job entails some amount of physical labor in setting up computers, running cables and moving computers.
Qualifications:
Bachelor's degree in CS, IT or equivalent
1-5 years IT industry experience

Training and Professional Development
Newly hired full-time staff are oriented to the campus by the Human Resources. This orientation serves the purpose of providing new staff an overview of various campus offices and their functions. The two-day orientation includes tours of the Ogden, Davis, and Roy campuses and department sessions that highlight the role of various Student Affairs programs and services. Existing staff have the opportunity to attend professional trainings held by the Office of Workplace Learning. These trainings are held through out the semester and provide resources and skills in meeting the goals of the division. The Division also provides a four day "Student Affairs Academy" each May to provide insight into becoming a better Student Affairs professional.

Evaluation
Professional Staff are evaluated every 12 months using the University's Performance Review and Enrichment Program (PREP) that enables communication on job performance between the Director and staff in an open and formal manner. This process is standard for all evaluations given at the University.

The PREP process allows for the supervisor and supervisee to collectively set goals. Timelines will be set for the goals and agreed upon by both parties during the review process. These goals and timelines are then approved by the Executive Director of Academic Support Centers and Programs (ASCP), the overseeing management of the SAT department.

Departmental Rewards and Recognition
The Student Affairs Division accepts nominations biannually Division-level awards. SAT will nominate members of the department as appropriate. Within our department, we also take advantage of the "Builders of Excellence" Division program that allows staff members to

recognize and offer kind feedback to another when something was performed and appreciated by another.

Staffing Needs
The need for a full time web designer has been discussed with recent Division site updates. Typically, we rely heavily and incorporate the use of student designers to fill this need, but have had constant issues with design differences. Re-training students has caused timeline problems and disconnection with previously designed pages. Web design and training has often fallen to the duty of the web programmer, which creates a backlog of jobs needing development and coding.

Central support staff is non-existent within the department and we rely on student staff to fill this role and we lack continuity in the position. Being so decentralized with our office space, the ability to justify and place a full-time staff member would be a challenge.

Student Staffing

The goals of the computer labs are to provide knowledgeable and friendly customer service. To this end, new student employees are hired based on their experience in customer service, technical skills, community involvement and strong academic background. The team leaders select potential interview candidates by reviewing applications and resumes. During the interview, candidates are evaluated on their responses to typical lab scenarios. The candidates are also required to take a competency test in which the technical knowledge of the candidate is evaluated. The topics in the competency test include using Microsoft Word, Excel, and PowerPoint.

These requirements have served the lab well in hiring quality and knowledgeable student staff who typically work in the labs through their schooling career until their graduation or transfer to other universities. The labs recruit new student staff before the start of fall and spring semester. The labs have been successful in recruiting new employees before the start of each semester; however, the challenge is recruiting student employees to fill certain shifts two or three weeks into the semester.

As per campus standards, all jobs are posted and processed through the Human Resources office. Fliers and word of mouth have served successful to recruit students (See Appendix C)

Lab Aides
The primary responsibility of the lab aides is to provide customer service and support to students using the computer labs.
Responsibilities include, but are not limited to the following tasks:

- Assist students
- Perform basic computer operations
- Provide software and minor hardware support
- Maintain a clean and efficient lab environment
- Assist team leader and supervisor as needed

Qualifications:

- The applicant must have completed TBE 1700 (or equivalent) with a grade of "B" or higher
- Comprehend written and oral instructions
- Demonstrate working as teams
- Have good communication and customer service skills
- Leadership skills and experience are preferred and beneficial for advancement.

Level I
Lab aides have the opportunity to advance to the level I position after working in the labs for a full semester. The level I training entails an understanding of the labs' policies and procedures, resources and referrals, ethics and safety. The training is conducted through WSU online and is intended to assess the knowledge of the lab aides. In order to pass this training, student employees must score eighty percent.

Level II
Candidates for the level II aide position must complete three out of five learning projects with mandatory participation in service learning. The categories are customer service, technology, leadership, student involvement and service learning projects (See Appendix D). Participation in level II can begin in the first semester of working in the lab.

Team Leaders
The job responsibilities of the team leader are:
- Hire and train new workers
- Schedule lab shifts and resolve scheduling needs or conflicts
- Enforce lab policies
- Post and update lab information
- Ensure cleanliness and working condition of equipment
- Report technical problems to lab technician
- Attend monthly team leader meetings

Qualifications: (team leaders are chosen by the lab supervisor)
- The candidate would have worked at least one full semester in the labs
- Demonstrated strong work ethics
- Have strong communication and customer service skills
- Aptitude for leadership role and supervisory skills
- Good managerial skills

Head Team Leader
In addition to the responsibilities of a team leader, the head team leader is also responsible for:
- Updating information on computer lab web page
- Updating information on lab manuals, fliers and posters
- Updating and post level I trainings online
- Scheduling monthly team leader meetings
- Report on technical or other concerns in the lab on a weekly basis
- Inform team leaders and lab aides informed of pertinent trainings available
- Plan and organize lab events such as semester-end get-togethers, lab aide retreats and block parties

- Scheduling and sending out surveys

Qualifications: (head team leader is chosen by Student Lab Coordinator)

- Candidates for the position of head team leader will have worked in the labs for at least one year
- Demonstrated leadership and supervisory skills
- Thorough understanding for the functions of the lab
- Demonstrated good written and oral communication
- Have good organizational skills

Student Technology Assistants (STAs)

The STAs' primary responsibility is to provide hardware and software support to all Student Affairs Division. This includes setup and configuration of new computers, installation of office printers, diagnosing and resolving software issues and troubleshooting some common computer problems. On a semester basis, the job entails some amount of physical labor in setting up computers, running cables and moving computers.

Qualifications:

- Must be majoring in Computer Science, Information Systems & Technology or Telecommunications Administration
- Should be able to install, maintain, troubleshoot and repair various types of computer equipments (PC or MAC desktops, and laptops, scanners and printers)
- Previous knowledge and experience with technical support
- Excellent customer service skills
- Hands on experience with Novel Client, Faronics Deep Freeze, and Symantec Ghost.

Training and Professional Development

Student staff are required to attend an annual lab aide retreat. During this retreat, lab aides are oriented to the purpose and goals of the department as well as facility and lab responsibilities. New lab aides are also scheduled for a week with another lab aide to allow for job shadowing. We will also sponsor student employees to attend the Student Affairs Academy of Leadership provided by Student Involvement and Leadership.

Feedback from students regarding lab operation and management are reviewed every semester. Student employee evaluations are reviewed together with the staff and employee on a semester basis.

Evaluation

Student employees are evaluated on their job performance by student staff and supervisors. These evaluations are based on their attendance, participation in lab activities, communication, helpfulness and approachability.

For 2009-2010, four learning outcomes have been identified for the student employees. They are responsibility and accountability, communication, self-management, and problem solving. These learning outcomes will be measured before the employee training (August 17th & 18th) and throughout the academic year through student self-assessment and supervisor evaluations.

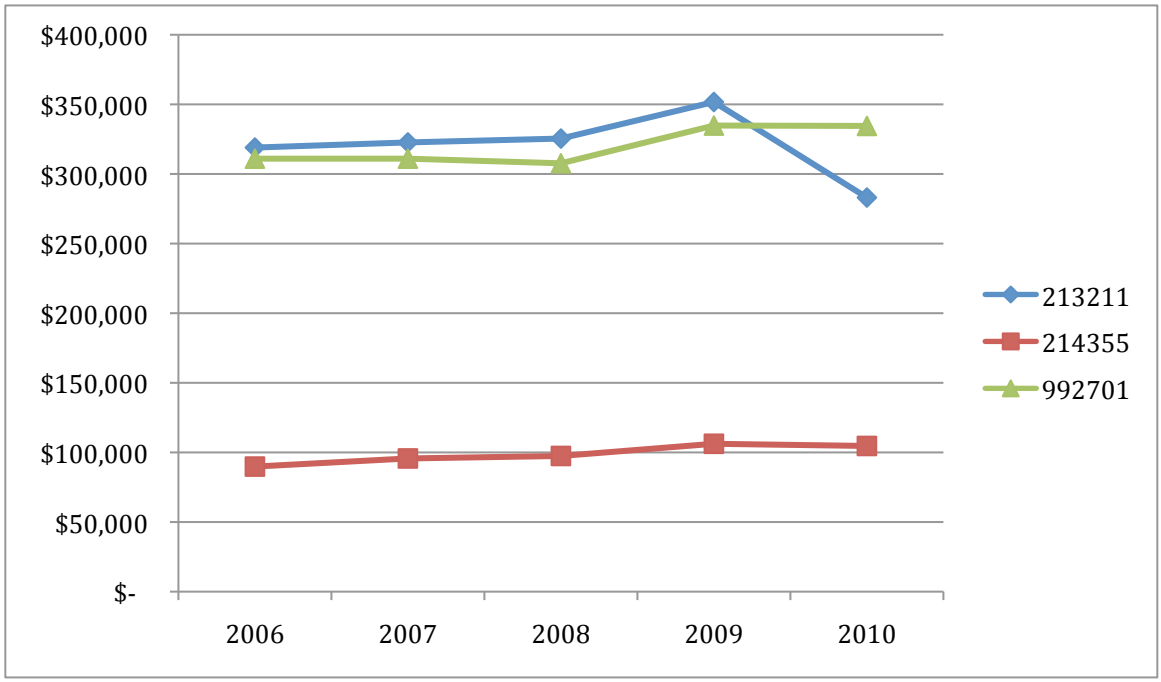
Departmental Rewards and Recognition
Student employees are given rewards and recognition during various periods of the academic year. These include:

- Lab aide of the month: Is chosen by the team leader based on the lab aides' performance
- Lab aide of the semester: Chosen by the team leader committee
- Lab aide appreciation party: Every semester an appreciation party is organized by lab leadership. This party is typically held at the ice-sheet, bowling alley and other campus venues
- Farewell/Graduation: Farewell/Graduation card signed by all lab aides

Staffing needs
Staffing for labs is on a needs basis and beyond individual hiring; all other needs are evaluated by Student Lab Coordinator and acted upon if required.

4. Financial Resources and Budget

Student Affairs Technology is provided with three budgets to manage services. These budgets include one student fee budget (992701) dedicated to the student labs and two E&G (State Economic & Growth) budgets (213211 & 214355) providing both student lab financial support and overall departmental support.



In 2008-09, the breakdown per student served (including salary) was $50.79 and $2.37 per session. This is based on a $722,232 total budget with 14,219 students served in over 304,950 sessions. Excluding salaries, the cost per student was $16.00 and cost per session was $0.75.

Priorities for funding are based primarily on the student lab three-four rotation of technology schedule. The majority of budget is dedicated to this function along with student wages. The Director manages the budget. Funding is needed by staff members beyond the areas described above, it is distributed appropriately. The Executive Director of ASCP also oversees this budget and has management rights to offer suggestions for funding services.

In 2008-09 SAT was required to take a $70,187 base budget cut. This has caused the SAT department to be creative in how services are managed.

In response to budget cuts, the computer rotation schedule for the computer labs from a 3-year to a 4-year plan. The concern with this change is the computer labs will have 1-year of usage and upkeep outside of the standard 3-year warranty given by computer vendors. In addition to the change in the rotation schedule, the computer lab in the Mathematics building was closed. This dropped our overall computer count and the ability to serve math majoring students with a convenient lab for schoolwork.

5. Facilities, Equipment, and Technology

Computer Labs
Our computer labs are located in academic buildings across campus including Davis Campus and Roy campus. The variety of locations helps us serve the student body by providing easy access to technology for students. Certain challenges arise with typical programming space and the lack of room to provide ergonomic seating for students. Many of our locations are located in older buildings not designed for large computer lab needs. This causes issues when trying to troubleshoot issues and remotely managing services, causing the lab technicians challenges supporting all the locations in a timely manner.

In 2009-10, SAT will be losing a popular open lab in Lampros Hall due to academic needs for the Development Math Department. Since we do not own our locations and are essentially guest in academic buildings, SAT is at the discretion of the Deans and other Administrators.

Professional Staff
Professional staff within SAT is distributed broadly. This is due to the merging of SAIT and SAT, and the acquisition of other new staff. Because new staff has been hired intermittently, they have been placed in whatever space is available as opposed to a central locations.

Geographically decentralized staff locations create an inconvenience to collaboration and communication at times, but it does not detract from meeting the departmental missions. Due to the nature of technology support, many of the professional offices do not provide the correct workspace required to offer repairs, maintenance and storage of technology systems.

Expansion of staff is currently impossible because of space restrictions. Student employees are currently sharing space, working in professional staff offices, which sometimes causes

inconveniences when staff members are required to have meetings "in confidence" with other staff or conducting general departmental business.

Technology Usage
Due to the nature of our department, we use, support and manage technology on a daily basis. Rotation of technology for professional staff is based on a first in/first out schedule or if needs require.

Projected Needs in Regards to Facilities, Equipment, and Technology
We are always in communication with Facilities Management concerning new lab locations. Whenever a new building project is considered, we consult with the project managers on providing space for a new computer lab. An example is in the Elizabeth Hall Humanities Building finished in January 2009. In this building, SAT was able to provide a new computer lab for students because of communication with Facilities Management.

6. Ethics and Legal Responsibilities

Student Affairs Technology understands the value of accurate information that is readily available to parties that require it. SAT ensures that measures are in place to protect the security, integrity and reliability of data, both digitally and physically. These measures include the housing of servers in a secure area, as well as creating databases, firewalls and password policies that protect against accidental or unauthorized access of student/staff directory information, educational records, and personally identifiable information as per federal (FERPA, HIPAA, GRAMA, or the Data Protection Act) and state laws and Section 10 of the WSU PPM. (See Appendix A)

SAT also recognizes that websites can be valuable support tools for Divisional and University initiatives and encourages staff to utilize this technology. Websites should be designed to convey constituency appropriate information for each service and program while adhering to University communication, template, and graphic standards.

Due to the sensitive nature of content in the testing centers, Testing Support must abide by FERPA regulations as well as testing regulations regarding the confidentiality of tests that they may encounter in the course of their work. Testing data must be kept confidential in order to protect students, faculty and staff as well as the University. Testing Support must protect the confidentiality and rights of privacy of examinees and staff as well as adhere to program requirements of testing companies in administration of specific tests.

The Computer Labs have distinct guidelines identified in the WSU Policies and Procedures section 10-1 (Information Security Policy) and 10-2 (Acceptable Use Policy) (See Appendix A) that dictate how computer systems are protected and used on campus. In addition, the labs collaborate closely with IT to ensure software licensing is up to date and correct for all the areas supported.

Professional staff are required to attend the WSU Office of Workplace Learning's ethics training to establish and reinforce the need for awareness in this important area to ensure the all those associated are protected.

7. Assessment and Evaluation

SAT follows the 6-Column Model of Assessment, as laid out by the Student Affairs Division and defined as:

1. Unit Goals
2. Means to Achieving Goal
3. Student Learning Outcome
4. Methods of Assessment
5. Results of Assessment
6. Use of Results.

The Student Computer labs, being our outreach to the student population, are the main focus upon which educational goals and learning outcomes are sighted. The remainder of our department strives for more of a program goal approach, which fits into our service related mission.

Student Computer Labs

Learning outcomes based assessment:

As part of the WSU Student Affairs Student Employee Project, we are gathering information on students' achievement of learning outcomes through the student employment program related to four learning outcome categories: responsibility and accountability, communication, self-management, and problem solving and critical thinking. A supervisor evaluation will supplement the students' self-report of learning outcome achievement and will be filled out one month after the beginning of the each semester and during the last month of classes (See Appendix E).

In addition to the supervisor evaluation, there is also a performance evaluation given to student employees once a semester to measure working skills (See Appendix F). At the end of each semester, the employee and supervisor review the performance evaluation and offer feedback.

The student employment program in the labs is informed by Nevitt Sanford's (1966) theory of student development as a function of person-environment interaction. The Computer Labs evaluate student staff on their readiness in taking on additional responsibilities. On accepting those responsibilities, the student staff are provided with the resources and training to meet those responsibilities. The employment structure is also informed by Astin (1993) theory of involvement. Astin's theory is based on the idea that students learn better when they are more involved, Student Affairs Technology Computer labs engage students in ways that provide them with skills that are learned and practiced outside the classroom environment.

Goals and initiatives are determined on current trends often reflected in industry standards as well as student surveys. These also continue the support of the overarching goals the Division and University initiatives. Goals are discussed, planned, and activated during department meetings. During the course of the year, goals are revisited and discussed to ensure that programs are on track for achieving the end results.

Cohort Information
Student lab staff comparisons were established during Fall 2008 demonstrating the following information:

	Computer Lab Aide	All SA student staff	WSU Student Body
Total # of Unique Students	43	495	23978
Average Cumulative GPA	3.2	3.14	3.0
Retention Rate (Return/Grad)	95%	94%	71%
Avg. # Total Credit Hours	90	78	64

(See Appendix G)

Since we are open to all students regardless of major, we do not define programming to a specific group. When examining lab users compared to the overall student body, we had a difficult time differentiating whether we impact student learning. We provide service on average to over 14,000 students each year, which is close to 64% of the entire student body. There is no data on what a typical user's session involves as far as software usage, so this limits our ability to qualify data in regards to learning outcomes. We can only assume trends based on who uses the labs and who do not and compare GPA. We are currently in the process of evaluating methods on how to gather the necessary data to provide us with the cohort information.

Student Needs & Satisfaction
Student needs are assessed by periodic surveys administered electronically via a desktop icon to a StudentVoice survey. This survey inquires about needs and desires of student users and provides us with a basis of information to manage new and current services. This same survey also measures student satisfaction with each lab's service. We provide the desktop link once a semester for a two-week period. This method has allowed us to consider usage strategies by students and pattern our lab hours after them. For example, we have also been able to establish which labs would best benefit from a color printing service through these surveys.

In addition to electronic surveys, our student lab aides are available to document student feedback and deliver it to the coordinator for consideration. This is done by observation and through direct communication with the students.

Basic student information
Student usage is tracked by user log in. We use identity management through the Novell client, in which all current students have active through IT's network services. Each time a student enters their WSU username and password to log into the computer, we capture:

- Username
- IP address (allowing us to identify lab and station number)
- Date
- Time In and Out

Through our print management software, we are able to report on print usage in every lab. Based on usage reports, there is a direct correlate between lab size and lab usage (Appendix H). We plan our labs to incorporate as much space for technology as possible while still allowing personal workspace.

Dissemination
The primary stakeholders for our services are the students as the majority of our funding is provided through student fees. Currently, other than sharing detailed data to the Student Fee Recommendation Committee for funding, we do not share information. It is not out of unwillingness, but out of indecisiveness of what and how to share the information.

In the future, we plan to create marketing and other informational flyers to distribute to students, faculty, and staff containing usage and survey data.

8. Summary

Over the past five years, the Student Affairs Technology department has seen growth with the addition of the Student Technology Assistants, Testing Support Specialist and the merge of the Student Affairs Information Technology Department. These additions have allowed all of the Student Affairs Division technology needs to be held within one department, which has allowed for technology related programs and services to be streamlined for the Division.

During this process, we have found that our primary strength as a department is the ability to work closely with each other and share the workload for tasks assigned. We have well defined roles within the department, but we all understand and have the ability to work together as a team to achieve common goals. We provide essential technological services to the Division, which allows those departments to provide their essential services to the campus. We will also continue to build upon our student employee professional development program by collaborating with other departments within the Division.

This preparation of this self-study has allowed us to understand that, due to our manpower to work ratio, we need to strategize a plan to prioritize our workload. We must change our theory of taking on everything and anything with strict, sometimes unmanageable timelines. We feel that we are near our threshold with current demands for our services and anticipate that this may impact the quality and quantity of our services in the future due to high demand and low manpower. We recognize that we are one of the few departments in the Division without a dedicated full-time support staff. During this process, we have realized the amount of time that must be reallocated from our individual daily activities to conduct office support work. As such, this has impacted the way in which we are able to achieve our overall mission.

Overall, this process has allowed us time to look inwards at our core duties and how we perform. We realize the strength of our department is in the people that are at its core. Due to this strength, we have the ability to adapt to perceived challenges and carry on with our overarching goals.

Appendix A

WEBER STATE UNIVERSITY	**Open Student Computer Labs**	No. 2-12	Rev.
		Date: 12-14-99	

I. OVERVIEW Weber State University maintains open and discipline-specific computer labs. Open labs are funded with student fee monies and are managed by Academic Computing and Learning Support. They are open to all students and all departments. Discipline specific labs are managed by departments and colleges and do not receive student fee monies. A list of all open computer labs is available at the Computing Support web site. Academic Computing is responsible for the maintenance of computers, printers, servers and network connections within the labs and installs and debugs software. Learning Support maintains facilities, provides printing and other expendable supplies and provides on-site lab personnel, including staff coordinators and student aides. The two departments work together in the education of staff, in the development of new services and in the general execution of lab policy. Open lab policy is set by the Faculty Senate through the Academic Resources and Computing Committee.

II. Purpose A. For Faculty. Open labs provide an environment in which faculty can offer computer programs, lessons or experiences necessary or valuable to Weber State educational programs. Faculty from all disciplines are welcome and many approaches to learning, from individual student exploration to instructor led groups, can be supported. B. For Students. Open labs support academic development and learning by providing an environment in which students can

1. Use computer tools, such as word processors, to accomplish class projects; 2. Learn to use computer programs both general value, such as spreadsheets, and of value to particular academic fields, such as statistics packages; 3. Use information technology, such as electronic mail and Internet browsers, to learn about the world and to communicate with others; 4. Learn independently about computers and information technology; 5. Enhance computer and information literacy.

III. GENERAL POLICY

A. Access. All labs are available to all members of the Weber State community. Curricular work has priority over other uses. Students engaging in scheduled curricular work have priority over other students. Students have priority over staff and faculty. All lab usage must conform to state and federal law, general University policy and lab rules. B. Generality of Service. As much as technically and legally possible all labs will provide all services, so that any student can work in any lab. C. Scheduling. Part or all of lab can be scheduled for the exclusive use of a class or a group of students working on class related projects under constraints established for each particular lab. Reservations must be made in advance with lab personnel. D. Open hours. Labs will remain open during periods of reasonable student demand, including nights, weekends and holidays as necessary. E. Closed hours. Faculty and contract staff employees, with the approval of the Director of Learning Support or Academic computing, may use a lab during regularly closed hours. Academic Computing or Learning Support personnel must be informed of all such off-hour usage. The person using the lab during such periods has complete responsibility for the security and safety of all lab hardware and software. No student may use a lab

Appendix A

during a closed period, except under the direct supervision of a faculty or staff member with approval from the Director of Academic Computing or the Director of Learning Support. Lab personnel must be informed of all such off-hour usage. The faculty or staff person is responsible for that student, and for the security and safety of all lab hardware and software while that student is in the lab. F. Staffing. As much as is practicable, labs will be staffed during all open hours by employees who can start and stop all hardware and can initiate and terminate all application software maintained by the lab. These employees are expected to teach lab patrons how to carry out routine operations with the hardware and software and to help patrons when unusual problems arise. G. Staff education. Lab personnel will be taught how to perform their basic functions of system maintenance, patron support and general management. They will be informed of new services and procedures regularly. H. Printing Service. A moderate amount of printed output related to curricular work will be available in the labs free of charge. Users will be expected to show restraint, requesting no more printing then necessary, so that this service remains economically feasible. Lab personnel may establish printing schedules or limit printing as necessary to maximize printing service for all lab patrons. I. Equipment maintenance. Computers and peripherals will be maintained in good working order. J. New equipment acquisition. No regular acquisition of equipment is budgeted. Lab personnel will assist outside departments in specifying and selecting new equipment and in preparing requests for funding equipment acquisitions. Academic Computing will install all new equipment. All new hardware must be approved by Academic Computing before it can be installed in the labs. K. Software maintenance. Software requested by faculty will be maintained in working order on as many computers as is technically possible, within license constraints. A periodic review will be made of software holdings and applications which are out of date will be removed, with faculty approval. L. New software acquisition. An academic department or individual faculty member may request the installation and support of new software by providing to Academic Computing staff:

> A. A legally usable copy of the software; B. A written description of the copyright status of the software, including any copy restriction, and the number of users who can simultaneously access the software; C. A brief description of intended usage; and D. All necessary technical and user documentation;

When installation of new software is requested, Academic Computing personnel will assess its impact on disk space, printer capacity, workstation time, and other lab facilities. If the expected impact is not deleterious, the software will be made available to users in a timely fashion. If it is deleterious Academic Computing staff will consult with interested faculty and users before a determination is made to proceed with the installation. M. Educating patrons. Education and assistance in the use of software outside the basic core (word processor, electronic mail and web browser) is provided by faculty or personnel provided by academic departments. Lab personnel are not software tutors. N. Scheduling system changes. Whenever possible, upgrades and enhancements of lab hardware and software will be scheduled between terms or at other times when they will cause the least disruption of service. Users will be given prior notice as early as possible before any planned service outages or changes in service.

Appendix A

O. Policy for Distribution of Surplus Equipment from Open Computing Labs

After ARCC has made final allocation decisions (approximately April 15th) the campus will be notified by Academic Computing if surplus equipment from open student labs is available. A list of this equipment will accompany the notice. Requests will be collected for two weeks after notification. These requests will be categorized into three groups: 1.) computers that will be used primarily by students for academic work 2.) computers that will be used primarily by students for other University activities 3.) computers for faculty and staff. Requests from group 1 will be randomly selected until all equipment has been distributed. If the equipment outnumbers the requests from group 1, the random selection will continue with group 2 and, if necessary, with group 3.

IV. Rules for Lab Patrons Users of the lab must conform to all applicable state and federal laws. They must conform to Weber State University policy, and they must obey specific rules of the open labs.

A. Laws. Lab personnel are neither lawyers nor policemen. If they feel that illegal activity may be occurring they notify their supervisor, or, in an emergency, campus security. B. General University Policies. Several sections of the University Policy and Procedure Manual govern lab operation. These are listed below.

1. Computing Services PPM 2-11 2. Personal Computers PPM 2-13 3. Discrimination and Harassment PPM 3-32 4. Student Code PPM 6-22

C. Infractions and offenses. Problems are resolved at the lowest level possible. Patrons who violate rules are asked to desist. If a patron's work offends another, an attempt is made to separate the tow parties. Only if direct resolution fails are problems reported to authorities.

Appendix A

WEBER STATE UNIVERSITY	INFORMATION SECURITY POLICY	No. 10-1	Rev. 06-10-08
		Date: 04-13-04	

The *Information Security Policy* ("Policy") applies to all organizations within the University even though not all organizations are the same and the data needed and used by those organizations are different. The principles of academic freedom and free exchange of ideas apply to this Policy, which is not intended to limit or restrict those principles. This Policy is in accordance with federal and state laws and regulations regarding information security**.**

Each organization within the University must appropriately apply this Policy to make certain they are meeting the requirements regarding information security. It is recognized that the technology at some organizations may limit immediate compliance with the Policy; such instances of non-compliance must be reviewed and approved by the Information Security Office (ISO) and the Information Security Task Force (ISTF).

University Information Technology Resources are a valuable University asset and must be managed accordingly to ensure their integrity, security and availability for lawful educational purposes. This document describes policy for use by all University staff, students and users of the University's Information Technology Resources.

Note: Throughout the Policy the terms *data* and *information* are used interchangeably.

I. PURPOSE

The purpose of the Information Security Policy is to:

- Provide policy to secure High-Risk, Restricted and/or Confidential information of faculty, staff, students, and others affiliated with the University, and to prevent the loss of information that is critical to the operation of the University.
- Provide reasonable and appropriate procedures to ensure the confidentiality, integrity and availability of the University's Information Technology Resources.
- Prescribe mechanisms which help identify and prevent the compromise of information security and the misuse of University data, applications, networks and computer systems.
- Define mechanisms which protect the reputation of the University and allow the University to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to networks outside the University.
- Provide written guidelines and procedures to manage and control information considered to be High-Risk, Restricted and/or Confidential whether in electronic, paper or other forms.
- Protect the integrity and validity of University data.
- Ensure the Security and protection of High-Risk, Restricted and Confidential information in the University's custody, whether in electronic, paper, or other forms.

II. SCOPE

This Policy covers electronic and paper-based data defined to include, but not limited to, all information

maintained, processed, or distributed by the University on primary computer systems or any subsidiary systems that contain data defined by law or policy as High-Risk, Restricted or Confidential. This Policy also applies, but is not limited to, all faculty, staff, administrators, students, consultants, and any person or agency employed or contracted by the University or any of its auxiliary organizations who have a legitimate need to have access to University High-Risk, Restricted or Confidential information.

The unauthorized addition, modification, deletion, or disclosure of High-Risk, Restricted or Confidential information included in University data files and data systems is expressly forbidden. In certain limited circumstances, as specified in federal and state legislation, the University may disclose High-Risk, Restricted or Confidential information.

III. DEFINITIONS

It is the Data Security Steward's responsibility to implement the necessary Security requirements should such data be considered High-Risk, Restricted or Confidential.

Data Classifications

High-Risk – Data that could be used to steal an individual's identity or cause harm to the individual, and which there are legal requirements or industry standards prohibiting or imposing financial penalties for unauthorized disclosure. Data covered by Gramm Liech Blyey (GLBA)and Payment Card Industry Data Security Standards (PCI DSS) are in this class.

This Policy recognizes that other data may need to be treated as High-Risk because it would cause severe damage to the University if disclosed or modified.

Restricted – Information assets for which there are legal requirements prohibiting or imposing financial penalties for unauthorized disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA, GRAMA, or the Data Protection Act, are in this class.

Confidential – Data that the University has determined should be protected because it may expose the University to loss if disclosed, but is not protected by federal or state legislation.

Public – Although there are no restrictions on disclosure to protect public data (because the data is provided for broad viewing access), sufficient protection must be applied to prevent unauthorized modification of such data.

If uncertain whether or not an IT Resource contains High-Risk, Restricted or Confidential information or is a Critical IT Resource, a User must seek direction from the appropriate Data Security Steward, Legal Counsel or Information Security Office.

General Definitions

Centralized Computer Systems - Computer hardware (including but not limited to Servers, Routers, Switches and Access Points) and software systems (including but not limited to Web hosts, Customized databases, University databases, and Faculty developed software for educational purposes) maintained by the IT Division and located in the University's data centers.

Critical IT Resource - An IT Resource which is required for the continuing operation of the institution and/or its colleges and departments, including any IT Resource which, if it fails to function correctly and/or on schedule, could result in a major failure of mission-critical business functions, a significant loss of funds, or a significant liability or other legal exposure.

Appendix A

Decentralized Computer Systems - Computer hardware (including but not limited to Servers, Routers, Switches and Access Points) and software systems (including but not limited to Web hosts, Customized databases, University databases, and Faculty developed software for educational purposes) maintained by any non- IT Division department.

Electronic Media - Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, or CD (optical disk).

Frequently – At least every 120 days.

Information Technology Resource (IT Resource) - A resource used for electronic storage, processing or transmitting of any data or information, as well as the data or information itself. This definition includes but is not limited to electronic mail, voice mail, local databases, externally accessed databases, CD-ROM, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

Portable Equipment – Laptops, PDAs, and other removable storage devices such as Flash Drives (Thumb Drive).

Security - Measures taken to reduce the risk of (a) Unauthorized Access to IT Resources, via logical, physical, managerial, or social engineering means; and/or (b) damage to or loss of IT Resources through any type of disaster, including cases where a violation of Security or a disaster occurs despite preventative measures.

Strong Password – A password that is at least 8 characters long and is a combination of upper and lower case letters, numbers and characters. Strong passwords do not include phrases, names, or other types of dictionary words.

Unauthorized Access to IT Resources - Access to High-Risk, Restricted or Confidential Information or Critical IT Resources by a User(s) that does not need access to perform his/her job duties.

User – All faculty, staff, administrators, students, consultants, and any person or agency employed or contracted by the University or any of its auxiliary organizations who have a legitimate need to have access to University High-Risk, Restricted and Confidential information.

-

-

IV. ROLES AND RESPONSIBILITIES

The persons responsible for implementing this Policy and their respective duties and/or responsibilities with respect to this Policy are described in Appendix A.

V. POLICY

A. CENTRALIZED / DECENTRALIZED COMPUTING SYSTEMS

- All University computing systems will comply with this Policy and the University Security standards or guidelines identified by the ISTF regardless of whether they are centralized or decentralized. These standards and guidelines are available upon request from the University's ISO.
- If Decentralized Computing Systems are unable to adhere to this Policy and the University Security standards or guidelines, decentralized systems must be relocated to a Centralized

Computing System. Division Heads and/or Deans may also chose to have a Decentralized Computing System relocated to the Centralized Computing System if desired.

B. COLLECTION OF DATA

- The collection of High-Risk, Restricted and Confidential information, not supported by applicable law or policy or otherwise justified by legitimate University purposes, is not permitted except with notification and permission of the individual to whom the data applies.
- The collection of High-Risk, Restricted and Confidential information must, to the extent practicable, be collected from the individual directly and not from other individuals or data sources outside the University.
- When information is obtained from data sources outside the University or other individuals, documentation or a log must be maintained of these sources.
- If providing High-Risk, Restricted or Confidential information is purely voluntary, this fact must be communicated to the individual providing the information.

C. ACCESS CONTROL

- Access to High-Risk, Restricted and Confidential information via the University's computer system is limited to those employees who have a legitimate business reason to access and/or use such information.
- Data access control must have sufficient documentation to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized.
- High-Risk, Restricted and Confidential information, electronic or paper, should not be left in plain sight to prevent unauthorized viewing and must be secured when unattended.
- All Users of systems that contain High-Risk, Restricted or Confidential data must have their own user name and use a Strong Password. The sharing of user names and passwords is not allowed.
- The password of empowered accounts, such as administrator, root or supervisor, must be changed frequently.
- Passwords used for University access must not be the same as passwords used for personal accounts (banks, g-mail, and credit cards).
- Passwords must not be placed in emails unless they have been encrypted.
- First-time passwords for new Users must be set to a unique value for each User and changed after first use.
- Human Resources and the IT Division will work with other departments to ensure that terminated employees have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in User responsibilities, periodic User access reviews should be conducted by the organization’s Data Security Steward.
- Personnel who have administrative system access must use other non-administrative accounts when performing non-administrative tasks.
- Accessing or attempting to access other computer systems through the University network, including those external to the University, without authorization of the owner of that system, as documented in the Acceptable Use Policy (PPM 10-2) is strictly prohibited.

D. REMOTE ACCESS

- Only authorized Users will be permitted to remotely connect to University computer systems, networks and data repositories to conduct University related business. Such connections must be done through University approved, secure, authenticated and centrally managed methods of

remote access.

- Individuals who work from remote locations are required to abide by the Standard for Secure Remote Access.

E. PHYSICAL SECURITY

- The party responsible for ensuring physical protection of all Centralized Computing Systems is the IT Division.
- The party responsible for ensuring physical Security of Decentralized Computing Systems is the appropriate IT Specialist.
- At a minimum, the appropriate responsible party shall comply with University guidelines and procedures to protect physical areas with shared electronic information resources that contain High-Risk, Restricted and Confidential information.
- Individual Organizations/Departments within the University are responsible for physical Security for personal computers and other local electronic information resources, including portable equipment, housed within their immediate work area or under their control.
- Permanent copies of High-Risk, Restricted or Confidential data must not be stored on portable equipment.
- High-Risk, Restricted or Confidential data must only be used temporarily on portable equipment and then only for the duration of the necessary use and only if protective measures, such as encryption are implemented that will safeguard the confidentiality and integrity of the data in the event of theft or loss of the portable equipment.
- All University owned computing equipment that has access to University information should be documented and managed (e.g. configuration management database).

F. DATA SECURITY

- Users must not knowingly retain on personal computers, servers, or other computing devices, High-Risk, Restricted or Confidential information, such as social security numbers, financial information including credit card numbers and bank information, or protected health information, including health records and medical information except under the following conditions:
    1. The User requires such High-Risk, Restricted or Confidential information to perform duties that are necessary to conduct the business of the University, or
    2. The appropriate Dean, Department Chair, Vice President or Director grants documented permission to the User.

    In the event that High-Risk, Restricted or Confidential information is retained on personal computers, server or other computing devices, the User must take reasonable precautions to secure the High-Risk, Restricted or Confidential information, e.g., implement password protection for documents that contain High-Risk, Restricted or Confidential information.

    The User must also take reasonable precautions to reduce the risk of loss of High-Risk, Restricted or Confidential data that resides on a User's personal computer or other computing device, i.e., encryption, backup critical documents on CDs or other media, or back up documents to a storage device or system, at regular intervals.
- All desktop systems and servers that connect to the network must be protected with an approved licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- Headers of all incoming data, including electronic mail, must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should also be scanned where such capabilities exist.
- Any employee, agent, or affiliate of the University who handles High-Risk, Restricted or

Confidential data for the purpose of performing their job duties or other functions directly related to their contractual affiliation with the University, is responsible for the proper handling of this data while under their control.

- The University will take reasonable and appropriate steps consistent with current technological developments to make sure that all High-Risk, Restricted and Confidential information is secure, and to safeguard the integrity of records in storage and transmission.

- The IT Division requires that all servers must be registered before being allowed to transmit data through Weber State University's firewall.

- Encryption technology will be utilized for local or central storage and transmission when required by law, policy, business standards, and University standards or guidelines.

- High-Risk, Restricted or Confidential information stored on portable devices must be protected via encryption, where feasible, to reduce the risk of unauthorized access or disclosure.

- All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the transmitted data is classified High-Risk, Restricted or Confidential.
- All systems connected to the Internet should have a vendor supported version of the operating system installed including the most recent security patches.

G. BACKUP AND RECOVERY

- Data backup and copies of data and software associated with any essential electronic information stored on Centralized Computer Systems must be sufficient to satisfy disaster recovery requirements and must be stored at a secure, commercial site that provides standard protection. (see IT Division Continuity of Service Plan)
- Backup and recovery procedures are required for essential data and software stored on Decentralized Computer Systems, including desktop systems.
- Electronic Media used for backup purposes must be stored in a secured physical location (not an employee’s residence).
- Users must take reasonable precautions to reduce the risk of loss of Critical IT Resources that reside on their personal computers or other computing devices, i.e., at regular intervals backup critical documents.

H. SECURITY INCIDENT RESPONSE AND HANDLING

- All suspected or actual Security breaches of University, college or departmental systems must immediately be reported to the Data Security Steward for their respective organization.
- If any High-Risk, Restricted or Confidential information (e.g. credit card information, social security numbers, etc.) has been accessed or compromised by unauthorized persons or organizations, the Data Security Steward for the respective organization must consult with the Information Security Office to assess the level of threat and/or liability posed to the University and to those whose High-Risk, Restricted or Confidential information was accessed.
- The Incident Response guidelines outline procedures for responding to an actual or attempted unauthorized access to High-Risk, Restricted and Confidential information. This guideline is available upon request from the University's Information Security Office.
- The University will report and/or publicize unauthorized information disclosures, as required by law or specific industry requirements.

I. SERVICE PROVIDERS

Appendix A

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be required to provide resources that the University determines not to provide on its own. The service provider must provide contractual assurance that they will protect the University's high-risk, restricted and confidential information it receives according to commercially reasonable standards.

Such contracts should be sent to Legal Counsel for review and should include appropriate terminology regarding use and protection of High-Risk, Restricted and Confidential information in accordance with the following guidelines:

- Explicit acknowledgment that the contract allows the contract partner access to High-Risk, Restricted and/or Confidential information.
- A specific definition or description of the High-Risk, Restricted and/or Confidential information being provided.
- A stipulation that the High-Risk, Restricted and/or Confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract.
- Assurance from the contract partner that the partner will protect the High-Risk, Restricted and/or Confidential information it receives according to commercially reasonable standards.
- A provision providing for the return or destruction of all High-Risk, Restricted and/or Confidential information received by the contract provider upon completion or termination of the contract.
- An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles the University to terminate the contract without penalty.
- A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.
- An agreement that an audit can be performed by a University employee, for any or no reason, with the intent of ensuring the integrity and confidentiality of High-Risk, Restricted and/or Confidential information that has been provided to a service provider.
- A provision requiring compliance certificates as proof of a service provider's compliance with federal, state, or other industry regulations that include but are not limited to GLB and PCI.

J. TRAINING AND AWARENESS

Each new University employee will be trained on the Acceptable Use Policy and University Information Security Policy as they relate to individual job responsibilities. Such training will include information regarding controls and procedures to prevent employees from providing High-Risk, Restricted and Confidential information to an unauthorized individual.

K. EMPLOYEE MANAGEMENT

References must be checked and criminal background checks obtained for all new employees in

compliance with University's Employment of Persons with Criminal Records policy (PPM 3-5a).

L. MONITORING AND TESTING OF NETWORKS

- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must also be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious Security intrusion is detected.
- Intruder detection tools must be installed where appropriate and checked on a regular basis.
- System integrity checks must be performed on all host and server systems housing High-Risk, Restricted or Confidential University data should be performed.
- Internal and external network vulnerability scans and penetration testing will be performed on the network infrastructure on a regular basis and after any significant change in the infrastructure, application upgrade or modification (e.g., new system component installations, changes in network topology, firewall rule modifications or product upgrades).

M. PENALITIES AND ENFORCEMENT

Penalties and enforcement of this policy will be in accordance with University policies and appropriate disciplinary and/or legal action will be taken when warranted in any area involving information security.

N. POLICY COORDINATION

- The University has identified the Information Security Office to act as the coordinator of this Policy.
- The Information Security Office will be responsible for assessing the risks associated with High-Risk, Restricted and Confidential information and developing procedures to minimize those risks to the University.
- Internal Audit personnel will conduct reviews of areas that have access to High-Risk, Restricted and Confidential information to verify that University departments comply with the requirements of this Policy.

O. REVIEW AND REVISION OF POLICY

- This Policy will be subject to periodic review and revision.
- Continued administration of the development, implementation and maintenance of the Information Security Policy will be the responsibility of the Information Security Task Force.
- The Information Security Office, in consultation with the Office of University Legal Counsel, will review the standards set forth in this Policy and recommend updates and revisions as necessary.

APPENDIX A

Division Heads/College Deans - These individuals, including managers of campus auxiliary organizations, shall be responsible for oversight of their employees' authorized use and access to High-Risk, Restricted and Confidential information in their areas of supervision. They will:

- Ensure that the management and control of risks outlined in the Policy are adhered to by employees in their unit.
- Ensure employees' access to High-Risk, Restricted and Confidential data is appropriate.
- Identify the necessary Data Security Steward and ensure they receive adequate training to perform this

Appendix A

role.

- Provide employees with resources and methods to properly secure equipment where High-Risk, Restricted and Confidential information is processed, stored, or handled.
- Provide employees with approved resources and methods for external data storage where High-Risk, Restricted and Confidential information is processed, stored, or handled.

IT Specialist - One or more individuals who are responsible for being the computer or technical support within a business unit, college/school, or department.

Data Security Steward – These individuals who are responsible for business processes within their areas of supervision will:

- Implement and administer the Policy in order to protect the privacy rights of University faculty, staff, and students, and to comply with legal and policy requirements.
- Protect confidentiality and Security of electronic and paper data maintained in their area.
- Define the functions for staff authorized to access Confidential data and approve authorization.
- Regularly review and document employee access to High-Risk, Restricted and Confidential data.
- Ensure that all employees receive employee/student confidentiality training as directed by the Information Security Task Force.
- Develop and implement appropriate processes to ensure employees comply with the required training.
- Provide an additional level of training for employees with access to High-Risk, Restricted and Confidential data.
- Communicate the expectations and means for the safeguarding of High-Risk, Restricted and Confidential information to appropriate persons and organizations.
- Provide recommendations for revisions to this Policy as appropriate.

Employees, including department chairs, faculty, staff, and student workers – These individuals:

- Shall not disclose High-Risk, Restricted and Confidential information to unauthorized individuals.
- Shall not modify or delete High-Risk, Restricted and Confidential information unless authorized to do so.
- Shall maintain High-Risk, Restricted and Confidential data in a secure manner.
- Shall complete the employee/student confidentiality training.
- Shall be required to sign a University confidentiality/FERPA agreement before access is granted to High-Risk, Restricted and Confidential data.
- Shall complete specific confidentiality training if they have job related responsibilities that require access to High-Risk, Restricted and Confidential information.

Network Security Administrator - This individual, within the IT Division will:

- Implement adequate Security measures for computing systems containing High-Risk, Restricted and Confidential data within his/her jurisdiction.
- Implement appropriate Security strategies for both the transmission and the storage of High-Risk, Restricted and Confidential data.
- Notify appropriate units of possible Security infringements.
- Report any Security breach as outlined in section H "**SECURITY INCIDENT RESPONSE AND HANDLING**" of this policy.
- Disseminate technical guidelines related to Security to the appropriate IT Specialists.

Information Security Task Force – A group of individuals appointed by the President to review and evaluate University Security issues such as:

- Current practices and the associated risks to the institution.
- Actions needed to address those risks through appropriate policy and associated guidelines.

Appendix A

- Identify new processes that are needed (for example security incident management).
- Implement new Security standards as needed.
- Disseminate general guidelines related to Security to the appropriate IT Specialists.
- Function as the Incident Response Team
  - Responsible for immediate response to any breach of Security.
  - Responsible for determining and disseminating remedies and preventative measures that are developed as a result of responding to and resolving security breaches.

Information Security Office – This office, within Administrative Services will:

- Assist the campus in identifying internal and external risks to the Security and confidentiality of information.
- Provide guidance for handling High-Risk, Restricted and Confidential information in the custody of the University.
- Provide guidance for the Security of the equipment or data storage devices where the information is processed and/or maintained.
- Promote and encourage good Security procedures and practices.
- Develop and maintain Security policy, plans, procedures, strategies, best practices.
- Provide standards and guidelines consistent with University policies.

Internal Audit – Internal Audit will:

- Evaluate the effectiveness of the current safeguards for controlling these risks.
- Provide recommendations for revisions to this Policy as appropriate.
- Develop and perform random audits of departments and individuals as deemed necessary.

Appendix A

WEBER STATE UNIVERSITY	ACCEPTABLE USE POLICY	No. 10-2	Rev.
		Date: 10-11-05	

I. Preamble. Weber State University provides students, faculty and staff with access to both an internal campus network and to the Internet. Such access, used appropriately, legitimately advances the mission of the university. But there is always the possibility for misuse. This Acceptable Use Policy provides guidelines for the use of network and computing resources that reflect the mission statement of the university, protects WSU community members and others from harm, and helps to preserve the availability of network resources for all WSU community members.

II. Scope of Policy. While this policy deals specifically with issues involving the use of university computing resources and networks, it does not stand alone. All users of university resources are expected to abide by the rules and regulations contained in applicable university handbooks, the Student Code, guidelines and policy and procedure manuals, as well as the laws of the State of Utah and of the United States of America. We remind users that state and federal laws apply to the use of campus networks and the Internet, including but not limited to those dealing with:

- copyright infringement
- defamation
- discrimination
- fraud
- harassment
- identity theft
- obscene materials

This Acceptable Use Policy applies to all individual users of Weber State University's computing and data network facilities. By using these systems, the user agrees to comply with and be subject to this policy. Users accessing Weber State University computing and data network facilities are responsible for maintaining a current understanding of the terms of this policy, which the university reserves the right to change without prior notice. The current version of this policy is available in the university's Policy and Procedures Manual. This policy also covers the use of all devices connected to the university computing and data network facilities whether owned by the university or private individuals.

III. State of Purpose. Weber State University computing facilities and data networks (including the university's Internet connection) are provided for university-related use by Weber State students, faculty, administration and staff in support of the teaching, research, public service and administrative activities of the university. Weber State expects its users to exercise responsible and ethical behavior when using the university's computing and data network facilities.

IV. Implementation and Enforcement.

A. General Guidelines.

Appendix A

1. Use of university computing facilities and data networks must be in keeping with the mission of the university.

2. Use of university computing facilities and data networks is limited to authorized users.

3. University computing facilities and data networks must be used in compliance with applicable state and federal laws and university policies, and may not be used for any illegal purpose.

4. Incidental and occasional personal use of computing resources is permitted as long as the use does not:

   a. violate applicable law, rules or policies,

   b. disrupt, distract from, or interfere with the conduct of university business (for example, due to nature, volume or frequency), and

   c. constitute a regular private business activity.

5. Users are responsible for all actions performed from their network, Internet, eMail and other accounts, as well as from personally owned computers connected to university data networks.

6. The privacy and rights of others must be respected.

7. The ability of legitimate users to utilize the computing facilities and data networks of the university in an efficient and secure manner must be respected.

8. Intellectual property rights, particularly those involving copyrighted material, must be respected.

9. The university reserves the right to take any and all actions necessary to protect the integrity and security of university computing facilities and data networks, including those necessary for law enforcement or other purposes.

10. The use of the university's computing facilities and data networks is a privilege that may be revoked at any time.

11. Disciplinary action in accordance with Weber State University policies and/or appropriate legal action will be taken when warranted.

B. The following are examples of actions which are specifically prohibited under this policy:

1. Use of university computing facilities or data networks for private financial gain in violation of university conflict of interest policies.

2. Sending unsolicited bulk eMail (spam) unrelated to the mission of the university or related bulk eMail without appropriate approval.

3. Sending eMail messages or creating web pages with fraudulent address or header information or containing misrepresentations in authorship or content in an attempt

Appendix A

to deceive others.

4. Use of university computing facilities and data networks by unauthorized users.

5. Unauthorized use of another user's account.

6. Providing false or misleading information for the purpose of obtaining access to computing or network facilities.

7. Attempts to access restricted portions of university systems and /or networks without authorization or the unauthorized possession of tools, including software, for such a purpose.

8. Use of university computing facilities and data networks for any illegal purpose or activity.

9. Placing of unlawful information on university systems.

10. Sending or storing public or private eMail message and attachments that violate state or federal law or university policy.

11. Monitoring (or attempting to monitor) another user's communications outside the scope of one's duties.

12. Obtaining (or attempting to obtain) another user's password without their consent.

13. Reading, copying, changing, or deleting (or attempting to read, copy, change or delete) another user's files or software without the prior permission of the owner.

14. Accessing or attempting to access computer systems through the university network, including those external to the university, without authorization of the owner of that system. (This includes port scanning, system exploits, or other techniques designed to gain unauthorized access to a system.)

15. Use of any device or software that interferes with the ability of others to access university networks or systems. (This includes unauthorized networking devices such as routers, and implementations of DHCP, DNS, NNTP, POP, IMAP, SMTP, and WINS servers or implementations of servers that provide uncontrolled access to copyrighted media such as music, video and computer software.)

16. Use of unauthorized wireless networking devices.

17. Damaging (or attempting to damage) any portion of university computing or data network facilities.

18. Use of university facilities for non-university related eMail, browsing the Internet or games or other such activities when computing facilities are crowded thereby depriving other authorized users of access to computing.

19. Use of peer-to-peer networking, or other file-sharing technology in such a manner as to place an undue burden on university resources, or to download or share copyrighted materials in violation of university policy or in violation of local, state,

Appendix A

or federal law.

20. Deliberate introduction of computer viruses/worms into university facilities, as well as attempts to create or disseminate such programs.

21. Deliberate misuse of software or other techniques to degrade system or network performance or otherwise deprive authorized personnel of resources or access to university systems or networks, including techniques to disguise or obscure the source of data network traffic.

22. Dissemination of copyrighted materials, outside of the provisions of "fair use," without permission of the copyright holder, including music, movies, games, software, etc.

23. Copying computer software protected by copyright into or by university computing facilities, except as permitted by law. (The use of illegally copied software is a violation of copyright law and will be treated as such.)

24. Use of the university's official web site or eMail for partisan political purposes (with the exception of announcements of general public interest by university political clubs).

25. Public release of confidential or proprietary information.

26. Misuse of trademarks in web pages and eMail, including university-owned marks such as the official logo or seal and trademarks owned by other entities.

27. Other activities of a similar nature not mentioned specifically herein but which violate the general guidelines above.

C. University Actions. The university reserves the right to take appropriate actions reasonably necessary to protect the integrity and security of university computing facilities and data networks. This includes the right to log and monitor network traffic and immediately disconnect any computer disrupting the university's data network, or being used for any activity in violation of this policy. Electronic information on university networks or equipment, including but not limited to electronic mail, is subject to copy and examination by the university where:

- It is necessary to maintain or improve the functioning of university computing resources
- Where there is reasonable cause for suspicion of misconduct under university policies or violation of state or federal laws
- It is necessary to comply with or verify compliance with federal or state law, including but not limited to software licensing agreements
- The requirements of maintaining a safe and secure network dictate the deployment of automatic security systems such as host and network intrusion detection systems, and active protection firewall systems designed to intercept, examine and block data that threatens the university or external networks

The system administrator will keep confidential the contents of files copied and read, unless misconduct is suspected, in which case a copy of the file(s) will be given to the appropriate

Appendix A

authorities.

The system administrator has the right to delete any file(s) belonging to faculty or staff who are no longer employed by the organization.

The university makes no warranties of any kind, whether express or implied, with respect to the information technology services it provides; this includes but is not limited to the accuracy or quality of information obtained through its electronic communication facilities and services except material specifically represented as official university records.

The university will not be responsible for damages resulting from the use or misuse of university computing and data network facilities and services, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, hacking, or service interruptions caused by the negligence of an organization employee, or by the user's error or omissions.

D. Enforcement. The university may suspend without notice, the network access privileges of any user who is believed to be in violation of this policy, pending investigation and review. Violation of this policy may result in denial of access to university computing resources, as well as appropriate disciplinary actions authorized by university policies up to and including termination or expulsion.

Appendix B

Department Staff Profile

STANDARD THREE-STUDENTS TABLE 2 STUDENT AFFAIRS STAFF PROFILE
Form used in NWCUU Accreditation

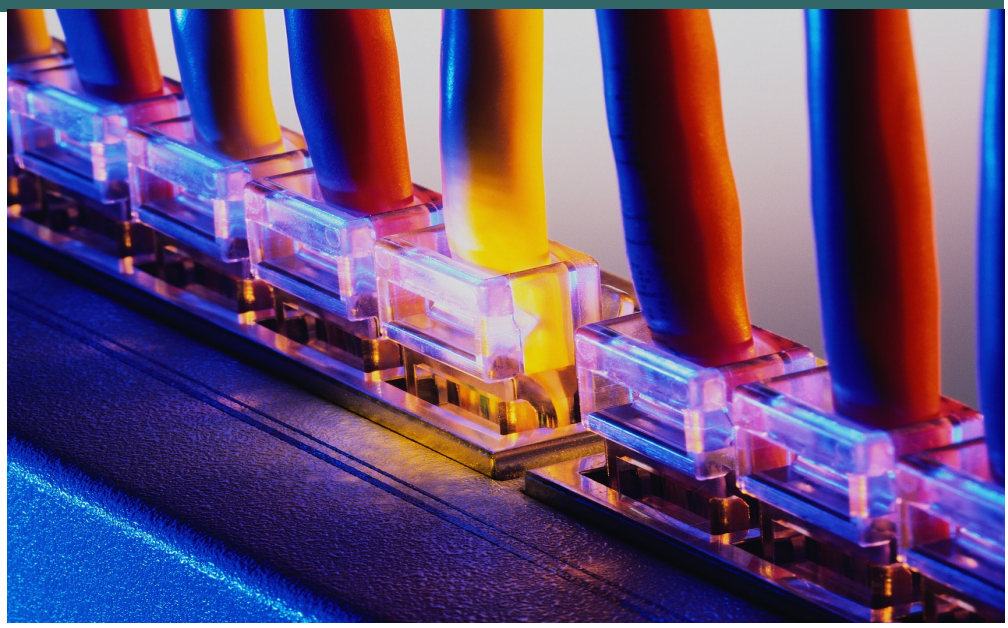
	Professional	Support	Student	Other
Female	1	1	21	
Male	5		30	
Degrees: PhD, EdD				
MD, JD, MSW				
MA, MS	1			
BA, BS	5	1	3	
AA, AAS, Certificate, etc.				
Years Experience in field: None				
Less than 5	3	1	55	
5 - 10	1			
11 – 15	2			
16 - 20				
More than 20				
Full-time: 9/10 months				
12 months	6			
Part-time: 9/10 months				
12 months				

SAT COMPUTER LABS

Benefits of Being a Lab Aide

"You are part of a team that strives to bring cutting-edge computer technology and superior customer service to WSU students."

-Lab Aide Manual



The Computer Lab Aide Position offers many benefits to its student workers.

- Becoming a lab aide will offer professional growth and experience.
- While working in the labs you will develop communication, presentation, customer service, trouble shooting, and leadership skills.
- You will have access to the state-of-the-art computer equipment and programs which will increase your development of computer and technical skills.
- Opportunities for advancement
- Opportunities for learning and training
- Social atmosphere—retreats, trainings, and interactions with students and other lab aides
- Flexible scheduling—work schedule arranged around your classes
- **Opportunity to do homework**
- Most holidays and semester breaks off
- Visibility on campus—increases opportunities to meet and network with campus faculty and staff
- Best campus pay available

WEBER STATE UNIVERSITY

Appendix D

Requirements

Level I lab aides interested in further job growth and challenges may now benefit from the opportunities offered by Level II.

Level II is now based on the overall performance review of the lab aide by the immediate supervisor, coordinator and team leader. Evaluations are focused on the performance and involvement of the lab aide in the labs and in the community.

To qualify for Level II, the lab aide needs to have worked one full semester as a Level I and complete the Service Learning Project and one goal in two of the following categories within one semester. If the lab aide is advancing within Level II during two consecutive semesters, he or she must complete one goal not previously chosen from two of the categories:

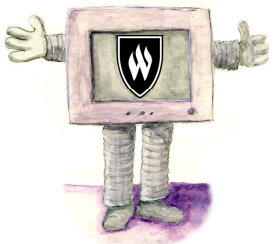
- Service Learning Project (Required)
- Technology
- Customer Service
- Leadership
- Student Involvement

When your goal(s) are complete, sign and date in the Goal Completion column. Also, have your team leader initial and date the form.

Upon completion of all the categories, fill out a Performance Review form and submit both the Review Form and the 'Goals Form' to your team leader.

The team leader with the SAT Coordinator will then schedule a performance review.

Pay rate for Level II lab aide ranges from $7.35 to $8.35.



ASCP/SAT
Fall 2007

Level II

An opportunity for professional growth.

Customer Service

Give a customer service training during a group meeting.

Attend a customer service training provided from Training Tracker. Present what you have learned in the next group meeting.

Take SST 3203, Customer Service Techniques, and complete the course with a "C" or higher.

Identify and demonstrate principles of good customer service throughout the semester.

Leadership

Schedule and chair all group meetings for one semester.

Participate in an interview. Give your comments and feedback to your coordinator and team leader.

Take a management class and complete with a "C" or higher.

Attend a student leadership training conference. Present what you have learned during the next group meeting.

Technology

Mac proficiency: Complete the online training module. Give a presentation to your team at the next group meeting.

SPSS proficiency: Complete a class requiring the use of SPSS with a "C" or higher.

Learn a new software program either on your own or from taking a class. Complete an assigned project from your coordinator.

Job shadow the computer lab technician for 10 hours. Have the technician sign the Advisor Form when your 10 hours are complete and you have proven

Student Involvement

Join a departmental club on campus. Attend 75% of the meetings and activities. Have the club advisor sign the appropriate form to verify your attendance.

Attend at least 5 sports events on campus during one semester. Keep a log of which games you attended, when they were held, and where they took place.

Attend 3 student government meetings. Report what you learn in a group meeting.

Become a student government representative. Have your advisor sign the appropriate form to verify your involvement.

Goal Completion

Goal 1:

Category: _____
Goal: _____
Date: _____
Signature: _____
Team Leader Initials: _____

Goal 2:

Category: _____
Goal: _____
Date: _____
Signature: _____
Team Leader Initials: _____

Service Learning Project

Coordinate with the Volunteer Involvement Program (VIP) and complete 6 hours of community service with an organization such as Saint Anne's or the YCC. Have VIP verify your participation via the Advisor Form. Give a presentation about your experiences during the next group meeting.

Phone number: 626-6349

Date(s) Completed: _____
Description: _____
Date Presented: _____

Other

Create your own goal. Get team leader and coordinator approval before beginning.

Goal: _____

Approval

Team Leader: _____
Coordinator: _____

Appendix E

Weber State University Student Affairs
Student Employee Learning Outcome Supervisor Evaluation

As part of the WSU Student Affairs Student Employee Project, we are gathering information on students' achievement of learning outcomes through the student employment program related to four learning outcome categories: responsibility and accountability, communication, self-management, and problem solving and critical thinking. This supervisor evaluation will supplement the students' self-report of learning outcome achievement and will be filled out one month after the beginning of the fall semester and during the last month of classes. Please choose only one option for each learning outcome.

	1	2	3	4
Effectively uses time to complete tasks	None of the Time	Some of the Time	Most of the Time	All of the Time
Consistently completing tasks	None of the Time	Some of the Time	Most of the Time	All of the Time
On time for shift and required to provide replacement if cannot work assigned shift	None of the Time	Some of the Time	Most of the Time	All of the Time
Understands staff roles	None of the Time	Some of the Time	Most of the Time	All of the Time
Presents her/himself in a friendly and professional manner	None of the Time	Some of the Time	Most of the Time	All of the Time
Takes responsibility for errors	None of the Time	Some of the Time	Most of the Time	All of the Time
Treats others with respect even when they are different from myself	None of the Time	Some of the Time	Most of the Time	All of the Time
Provides friendly service	None of the Time	Some of the Time	Most of the Time	All of the Time
Provides accurate service	None of the Time	Some of the Time	Most of the Time	All of the Time
Works with others to achieve a common goal	None of the Time	Some of the Time	Most of the Time	All of the Time
Able to express oneself clearly	None of the Time	Some of the Time	Most of the Time	All of the Time
Able to write clearly, understandably	None of the Time	Some of the Time	Most of the Time	All of the Time
Balances work, school, and home responsibilities	None of the Time	Some of the Time	Most of the Time	All of the Time
Articulates connection between current employment position and future goals	None of the Time	Some of the Time	Most of the Time	All of the Time
Understands personal health and wellness	None of the Time	Some of the Time	Most of the Time	All of the Time
Articulates one's strengths and weaknesses	None of the Time	Some of the Time	Most of the Time	All of the Time
Sets and achieves goals	None of the Time	Some of the Time	Most of the Time	All of the Time
Manages conflict with colleagues and others	None of the Time	Some of the Time	Most of the Time	All of the Time
Makes decisions appropriate to the situation	None of the Time	Some of the Time	Most of the Time	All of the Time
Applies effective reasoning processes	None of the Time	Some of the Time	Most of the Time	All of the Time
Solves complex problems	None of the Time	Some of the Time	Most of the Time	All of the Time
Seeks input from supervisor or colleagues where appropriate	None of the Time	Some of the Time	Most of the Time	All of the Time

Appendix F

Name: Observed by:

Date:

	1 Needs Improvement	2 Meets Expectations	3 Exceeds Expectations	Points
Communication Skills	Lab aide/ team leader does not appear to listen to student. The lab aide/ team leader is not easily understood and does not attempt to relate to the student and their needs.	Lab aide/team leader is sometimes able to relate to the student. They listen attentively the majority of the time and usually conveys messages with ease.	Lab aide/ team leader always listens attentively, is easy to understand, conveys messages with ease, and can relate to the student seeking assistance (including the ability to relate to the student's concerns).	
Accessibility/ Approachability	Lab aide/ team leader is wearing headphones or looking down at work and students frequently must wait for the lab aide/ team leader to notice them. The lab aide/ team leader appears unhappy or apathetic and is not attentive to the students.	Lab aide/ team leader is generally friendly and/or polite. They usually notice students immediately and are eager to help. Lab aide/ team leader had open posture and good nonverbal cues most of the time.	Lab aide/ team leader is always friendly and polite, has open posture and good nonverbal cues, and is attentive.	
Helpfulness	Lab aide/ team leader directs the student from their station as opposed to going to the student. The do not offer referrals or provide information/direction if they do not know the or question. They do not share information in a way that students understand it.	Lab aide/ team leader sometimes will go to the student lab station to help them. They generally provide accurate information and will sometimes refer the student to outside resources.	Lab aide/ team leader provides accurate information, assesses what the issue is and goes to the student (e.g., their lab station) if necessary. The lab aide/ team leader will also refer the student to someone or somewhere else for assistance, if necessary.	

Additional Comments:

Appendix G

2008 Student Affairs Computer Lab Aide Cohort

	Fall 2008	Spring 2009	Fall 2009	Spring 2010	Fall 2010	Spring 2011	Fall 2011	Spring 2012	Fall 2012	Spring 2013	Fall 2013	Spring 2014
Computer Lab Aide Cohort Information												
Total Number of Unique Students	43											
Cohort Average Term G.P.A.	3.31											
Change in G.P.A. from Last Term	N/A											
Cohort Average Cumulative G.P.A	3.2											
# Students who Graduated/ Degree Earned	2 Associates 2 Bachelor's											
# Students Continuing in Cohort	37											
Retention Rate (Returned/Grad)	95%											
Avg. # Total Credit Hours	90											
SA Cohort Information												
Total Number of Unique Students	495											
Cohort Average Term G.P.A.	3.03											
Change in G.P.A. from Last Term	N/A											
Cohort Average Cumulative G.P.A	3.14											
# Students who Graduated/ Degree Earned	20 Associate's 21 Bachelor's											
# Students Continuing in Cohort	464											
Retention Rate (Returned/Grad)	94%											
Avg. # Total Credit Hours	78											

WSU Student Body Information												
Total Number of Students	23978											
Cohort Average Term G.P.A.	2.84											
Change in G.P.A. from Last Term	N/A											

Appendix G

Average Cumulative G.P.A.	3											
# Students who Graduated/ Degree Earned	466 Associates 547 Bachelors											
# Students Continuing in Cohort	16765											
Retention Rate (Returned/Grad)	71%											
Avg. # Total Credit Hours	64											

Computer Lab Aide Cohort Characteristics:

Female:	37%	**Demographic Information**			
Male:	63%	African American:	2%	Hispanic:	7%
Avg. ACT Score:	22	Asian/Pacific Islander:	14%	Native American:	0%
Average Age:	25	Caucasian:	72%	Other:	5%

SA Cohort Characteristics:

Female:	52%	**Demographic Information**			
Male:	48%	African American:	3%	Hispanic:	6%
Avg. ACT Score:	23	Asian/Pacific Islander:	5%	Native American:	1%
Average Age:	24	Caucasian:	79%	Other:	6%

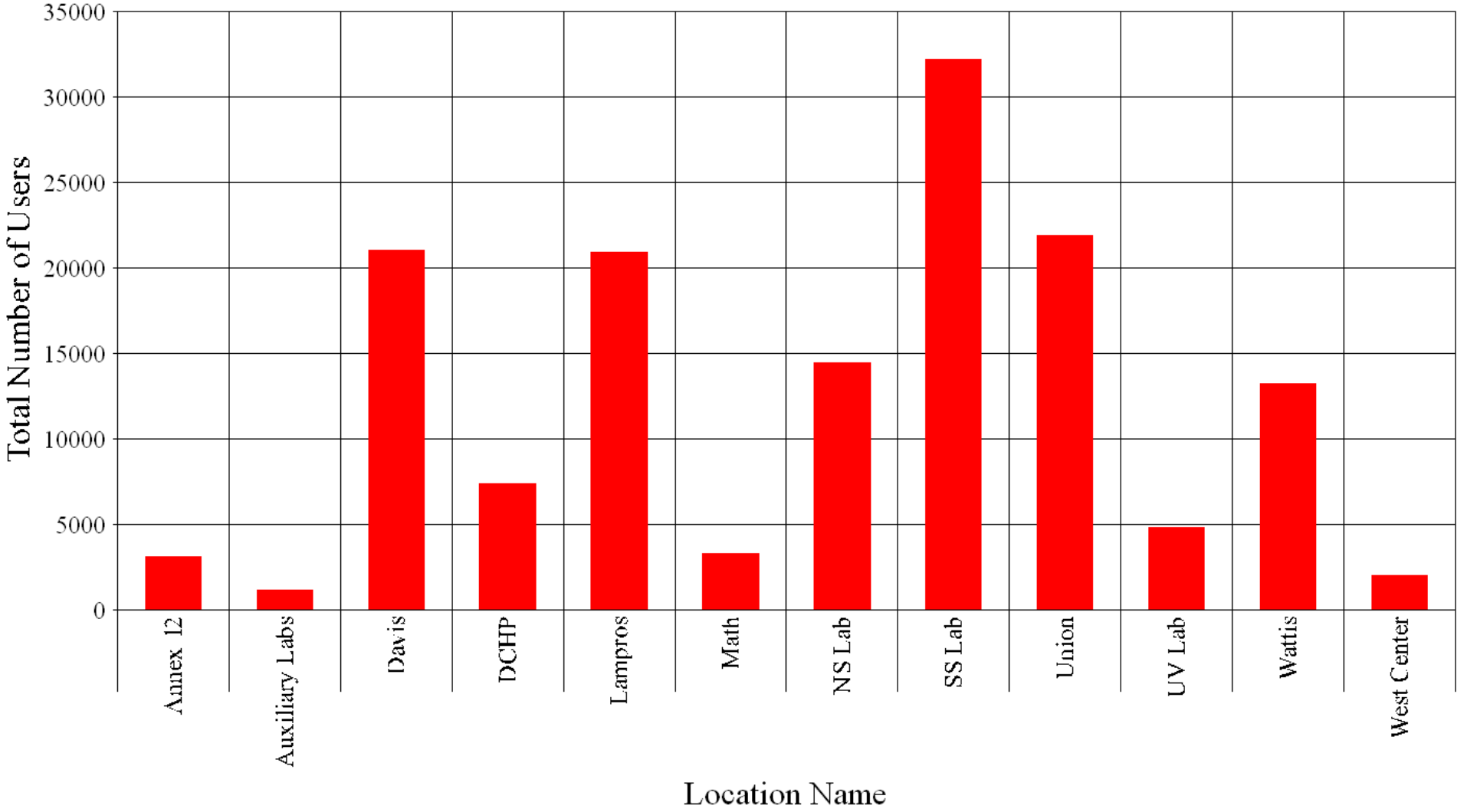
WSU Cohort Characteristics:

	Female: 51%	**Demographic Information**			
Avg. ACT Score: 22	**Male:** 49%	African American:	1%	Hispanic:	5%
		Asian/Pacific Islander:	2%	Native American:	1%
	Average Age: 26	Caucasian:	64%	Other:	26%

Appendix H

8/23/2008 - 12/12/2008: Overall Lab's Computer Usage on Windows XP (Fall 08)

All Labs



Location Name	Annex 12	Auxiliary Labs	Davis	DCHP	Lampros	Math	NS Lab	SS Lab	Union	UV Lab	Wattis	West Center	Total
Total Number of Users	3101	1196	21032	7380	20954	3320	14495	32253	21908	4817	13231	2057	145744

Note: A user is counted each time he/she uses a computer. Data only represents PC computers.