

Information Technology Department



IT Department Operational Procedures

Sisseton-Wahpeton College

3rd Edition – January, 2004

Table of Contents

Section	Page
IT Department Structure	3
Resources and Equipment	6
Systems Documentation	9
Network Structure	12
Network Access	14
Network Security	16
Internet Use	19
E-Mail Use	22
Requests for Service	25
Purchasing Procedure	27
Computer Science & Technology Instruction	28

THIS HANDBOOK IS NOT INTENDED TO CREATE, NOR IS IT TO BE INTERPRETED AS TO CREATE, A LEGALLY BINDING CONTRACT BETWEEN THE SISSETON-WAHPETON COLLEGE AND ANY OF ITS EMPLOYEES.

In the event that the terms of this handbook conflict with the written and approved personnel policies of the Sisseton-Wahpeton College, the policies of the College shall be controlling.

Nothing in this handbook shall mean or be interpreted to be a waiver of the sovereign immunity of the Sisseton-Wahpeton Oyate of the Lake Traverse Reservation, the Sisseton-Wahpeton Community College, its officers or any of its employees. Any waiver of sovereign immunity shall be unequivocally expressed only through a written resolution passed by the Tribal Council of the Sisseton-Wahpeton Oyate.

IT Operational Procedures

IT Department Structure

The IT Department at the Sisseton Wahpeton College has responsibilities in three major areas: infrastructure, telecommunications, and academics. The IT Department's involvement in each of these areas has a historical basis at SWC, and has allowed a greater level of integration and efficiency than what is present at similar institutions. The head of the department is the Director of Technology, whose position is described in the *IT Department Policies* (p. 4). A Technology Coordinator, an Academic Coordinator, and Telecommunications (Distant Education) Coordinator will assist the Director.

Infrastructure

This core responsibility of any IT department is the primary province of the **Technology Coordinator**. Functions of this position will include supervision of subordinate staff members along with the allocation and maintenance of resources required to maintain the college's LAN, servers, workstations, network devices, applications, and databases. The security and integrity of the information systems at SWC is a primary concern of the Technology Coordinator. This position will report to the Director of Technology. A written report will be submitted to the Director three days prior to the first Friday of each month. Communications between these two individuals should occur on a daily basis to ensure proper personnel and resources are available to perform the assigned tasks. Other key duties include:

- Assisting in the development of the *IT Department Strategic Plan*
- Review and propose revisions to the *IT Department Policies*
- Maintain a list of all administrative passwords for systems under the Department's jurisdiction in a secure location
- Archive and store critical data in a secure location
- Propose and implement modifications and/or expansions of SWC's IT infrastructure
- The enforcement all appropriate policies and procedures

Infrastructure is further divided into two major components: network and applications. The network component focuses on the LAN, from the media and network appliances to the addressing schemes, network services, and the hardware aspect of all nodes and equipment. The application component focuses on the software, data, and related support services requirements of SWC.

Network Administrator

Network Analyst

Network Specialist

Applications Administrator

Applications Manager

Applications Specialist

Systems Technician

Academics

The **Academic Coordinator** is primarily responsible for the CST programs, and community education and outreach programs in the area of technology. This position is comparable to

the chair of other academic programs with additional responsibilities assigned by the Director of Technology. These include supporting the general use of instructional technologies by all SWC faculty, providing appropriate professional development to all staff members, and being a liaison for the IT Department and faculty groups. This position will report to the Director of Technology. A written report will be submitted to the Director three days prior to the first Friday of each month. Other key duties include:

- Assisting in the development of the *IT Department Strategic Plan*
- Review and propose revisions to the *IT Department Policies*
- Conduct CST faculty meetings on a monthly basis
- Formally meeting with the Director of Technology a minimum of three times per semester
- The enforcement of appropriate policies and procedures, particularly those outlined in subheading *Computer Science & Technology*.

Telecommunication (Distance Education)

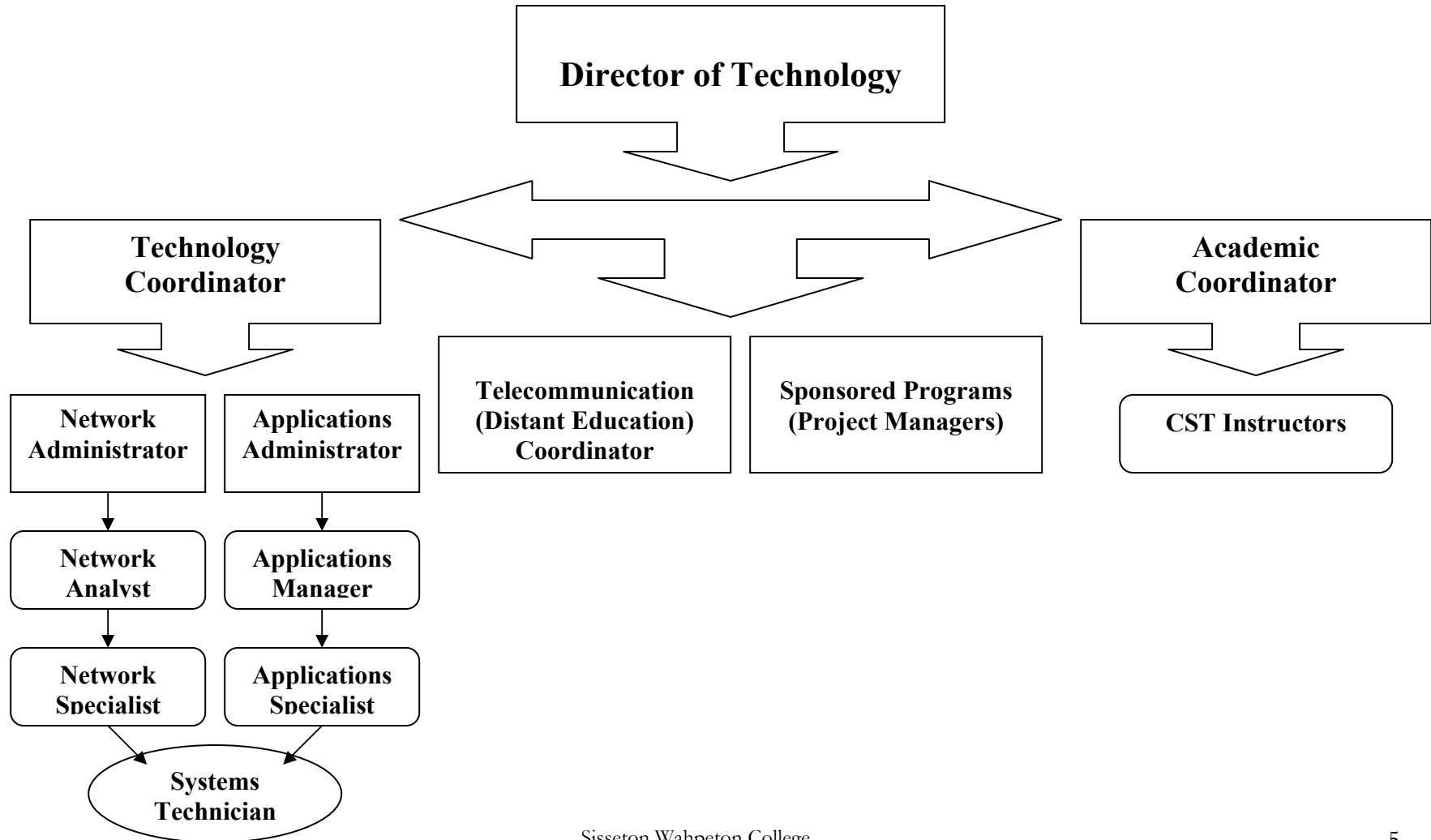
The systems for communicating with individuals or organizations outside of the SWC network, particularly platforms used for educational purposes, are the province of the **Telecommunications (Distance Education) Coordinator**. In addition to implementing, maintaining, and providing user support for the telecommunication systems the coordinator will provide assistance in the modification of curriculum by faculty to utilize distant education platforms. This position will report to the Director of Technology. A written report will be submitted to the Director three days prior to the first Friday of each month. A copy of this report will be forwarded to the Technology Coordinator and the Academic Coordinator as a high degree of interaction between these individuals is required by this position. Other key duties include:

- Assisting in the development of the *IT Department Strategic Plan*
- Review and propose revisions to the *IT Department Policies*
- Provide professional development programs for staff and faculty regarding the telecommunication systems and distant education platforms
- Develop best practice strategies for presenting courses through distant education platforms
- Scheduling the use of video conferencing or other synchronous delivery systems
- The enforcement all appropriate policies and procedures

Sponsored Programs (Technology)

The IT Department is responsible for programs that are primarily technological in nature, as assigned by the President. The project managers and/or assistant project managers of these programs will report to the Director of Technology or properly designated representative. A written report will be submitted to the Director three days prior to the first Friday of each month. The project regulations and the Director will specify other duties.

Sisseton Wahpeton College IT Department Organization Chart



IT Operational Procedures

Resources and Equipment

The IT Department has jurisdiction over all computer workstations, network devices, software, and all other computer/telephony components and accessories. Within the guidelines established through SWC policies, the Director of Technology has the discretionary power to allocate these resources as required, to establish proper-use procedures, and the ability to delegate these functions to other authorized staff members. The purchase, modification, or placement on the college's network or existing systems of any of the aforementioned items must be authorized by the Director of Technology, or by an officially designated proxy.

All software and hardware relating to computer/network/telephony systems will be inventoried and maintained according to the *IT Department Policies*, and within the appropriate subsections of the *IT Operational Procedures*. This subsection details the procedures established by the IT Department to ensure proper-use and the compliance to policies regarding IT resources and equipment.

Workstations: Most faculty and staff members will be given the use of a computer in their office with access to the college's network. Modifications to faculty and staff workstations including the addition or removal of hardware or software are not allowed without prior approval of the IT Department.

- Every workstation will be able to print on at least one network printer and one backup printer (one of which will be color).
- Individual desktop printers will not be available unless if the Director of Technology deems it necessary under special circumstances.
- Unless otherwise authorized by the Director or Technology Coordinator all workstations will use Windows 2000 or XP Pro as the operating system. The initial software install on the system will include Office XP (Standard or Professional), Internet Explorer, Acrobat Reader, and Norton Antivirus Corporate Edition.
- Access to the Internet will be through Internet Explorer and e-mail will be through the college's system.
- Additional hardware and software may be requested by filing the proper form with the Director.

Computer Labs, Smart Classrooms, and Student Workstations: Dedicated workstations for student use will be located at various locations on campus. Only enrolled students with a proper username and password may use these computers. All student workstations will be connected to the network and have access to a network printer. Students are not allowed to make any hardware or software modifications to any computer system. Students are not allowed to use any faculty or staff computer without prior approval of an authorized IT staff member.

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

- The Computer Lab and the CST Lab are under the supervision of the IT Department's Academic Coordinator. All modifications to the workstations located in these rooms need to have his or her approval or must be directly authorized by the Director.
- All modifications to the workstations in the various smart classrooms/labs and in the student computer centers must be authorized by the Director (or authorized representative) and will be performed by IT personnel.
- Internet access and email access can only be through authorized programs (Internet Explorer and the college's email server).
- No streaming media applications, instant messaging, or chat rooms are to be utilized for non-academic purposes on any workstations at SWC. Academic purposes are defined by activities assigned by a faculty member are an integral part of, or to enhance, a course.

Public Access Areas: Non-students are only allowed to access SWC workstations in pre-approved locations. The individual in charge of this area will maintain a login sheet that will record the name of the person, the station being used, and date and time (on and off) that this person was on the system. The user will then be provided with a visitor username and password.

- Currently the SWC/SWO Library, the Learning Lab, and the TANF Classroom are the only authorize public access locations.
- Visitors have only the basic student user rights and access.

Printers, Copiers, Faxes, Scanners, and Other Shared Devices: All shared devices, either on the network or stand-alone equipment, are under the province of the IT Department, and will be located by the Director. Only IT personnel or specifically authorized staff will service these items.

- All equipment of this nature that is placed on the college's network is under the direct supervision of the Technology Coordinator.

IT Resource Center: SWC owns a number of items that are of a portable nature that are available for use by faculty and staff members with the approval of the Director. When not in use these items will be stored in IT cabinets/closets, which will be locked at all times when not under the direct supervision of an authorized IT staff member.

- The Director, the Technology Coordinator, and specifically designated IT staff members will be assigned the key(s) for the storage area(s). Only these individuals have the authorization to access the IT Resource Center area(s).
- The IT Resource Center will maintain a list of items available for loan. This list will be located on the college's intranet. These items will be inventoried according to subheading *Systems Documentation*.
- Only faculty and staff members can check out items from the IT Resource Center. To checkout an item the individual must contact one of the authorized IT staff members, then sign and date the checkout sheet.
- Certain items maybe reserved by contacting an authorized IT staff member who will place the information on a calendar kept for that purpose.
- First priority for use is by the grant program that purchased the item, if applicable. Second priority is given to any reservations on the item.

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

- Once an individual signs-out an item he or she assumes full responsibility (including financial compensation) for it until properly returned.
- No item can be checked for more than **three** working days, unless it is by the grant program that purchased it, or by prior approval from the Director or Technology Coordinator.
- All items must be returned to the Resource Center on a monthly basis for the purpose of periodic maintenance, updating systems, virus scans, and for maintaining inventory records.
- The individual that signed for the item must return it on or prior to, the due date/time to an authorized IT staff member, and report any known problems with the item. The IT member is required to at least spot check the item for any obvious damage or missing components. He or she will then record its return and initial the checkout sheet, and will report any irregularities to the Director or Technology Coordinator.

IT Operational Procedures

Systems Documentation

The subheading *Systems Documentation* contains the procedures for recording the acquisition of new resources and maintaining the inventory of existing equipment and materials.

All new acquisitions will be classified as either consumable or durable. Supplies are items classified as consumable such as recordable media, toner, ink cartridges, paper, RJ47, and CAT5 cable. Durable items are divided into hardware (equipment) or software and licenses. When a shipment is received the items will be examined for damage and marked off the packing list, which will be initialed and dated. The packing list will be attached to the corresponding *purchase order* and *Form IT-G*. Any damaged, missing, backordered, or extra items are to be noted and the vendor is to be contacted promptly.

Supplies

- Ink cartridges: are the responsibility of the individual user
- Toner: 1 set will be in stock for every four printers of that model
- Drums, Imaging Units, etc: 1 will be in stock if there are four or more printers of that model on campus
- Recordable Media: will be reordered when the following minimum levels in stock are reached
 - CD-R: 25
 - CD-RW: 5
 - DVD-/+R: 5
 - Data Tapes: 2/drive
 - Zip: 5
 - 3 ½ inch: 10
- Cabling Supplies: will be reordered when the following minimum levels in stock are reached
 - RJ45: 30
 - Jacks: 5
 - GBIC Module: 1/type used
 - Fiber Jumper: 1/type used
 - CAT5 Patch Cable: 10
 - CAT5e: 300' (should be plenum)
- Other Supplies: minimum levels will be established by the Director of Technology
- SWC staff members may request supplies from the IT Resource Center.

Hardware

All hardware/equipment will be given a SWC ID Tag with a unique number. Unauthorized removal or modification of a tag is strictly forbidden. All hardware will be recorded into the

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

IT Inventory Database. Certain component items will be listed together as a single unit, such as a PC. A PC includes the hard drive, RAM, other internal components, along with a keyboard and mouse. The IT Inventory Database will utilize the following field (if applicable) for each record:

- SWC ID #
- Description
- Purchase Order #
- Manufacturer
- Model #
- Serial #
- IP address (if static)
- MAC Address
- Network Name
- Physical Location
- User's Name
- Processor/CPU speed and type
- RAM
- Hard Drive
- Internal Drives (CD, DVD, etc)
- Graphics Card
- Sound Card
- Modem
- Keyboard and Mouse
- Screen size and type
- Available ports or outlets
- Available slots
- Available bays
- Date salvaged

Software

All software and licenses will be inventoried using the database; in addition a hard copy record will be maintained in a fireproof cabinet or offsite. Software will not be tagged or assigned a SWC ID number. Software will be categorized as a box license; site licensed, or network versions (including CAL) along with whether the seats are concurrent or static. The following fields will be used in the IT Inventory Database for each record (if applicable):

- Description/Title
- Version
- Publisher
- Serial #
- Product ID #
- Purchase Order #
- License Type
- Number of Licenses/Classification
- License #

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

- Key Code
- SWC ID # (where it is installed)

IT Inventory Database

Any new acquisitions classified as hardware or software will be entered into the database prior to its allocation. Any modification to a PC, network appliance or device, or any supported system must be documented in the IT Inventory Database. The staff member making the alterations, including the installation of software or relocating the device must complete **Form IT-C** and submit it to the Director of Technology, or properly designated representative, within two working days. Items designated as salvage by the Director of Technology will be noted on the database, listing the date the item is removed from the inventory.

IT Operational Procedures

Network Structure

The subheading **Network Structure** elaborates on the basic information supplied in the **IT Department Policies** (p. 8-9) concerning the design, implementation, maintenance, and utilization of the information networks at SWC. The basic structure of the computer network at SWC will be a client/server domain controller on a Fast Ethernet network running TCP/IP. The primary network at the college will be based on an extended star topology.

Physical Structure/Layers 1-2

The primary media used for vertical drops will be CAT5e or higher cable with RJ45 or Keystone Jacks for terminations. Patch panels and keystone jacks will be wired using the T568B standard. 802.11(x) will be used for wireless networking when and where appropriate. Additional information on wireless network structure will be located under subheading **Wireless Network** of the **IT Operational Procedures**. Horizontal runs between the MDF and the primary IDF locations will utilize fiber optic cable with a minimum rating 1 gigabit. Horizontal runs from a primary IDF to a local switch will utilize CAT5e or higher cable. All switches will be rated at 100 megabit or higher, with new acquisitions being VLAN capable.

Protocols

SWC's computer network will use TCP/IP as the primary protocol. TCP/IP addresses will be assigned to servers, network appliances (switches, etc.), network printers, and other devices designated by the Director of Technology. The TCP/IP addresses used will be one of the private sets reserved for private networks. The Technology Coordinator will assign internal addresses utilizing the following scheme:

- Servers and Network Devices: 172.16.1.xxx
- IP Telephony Devices: 172.16.2-4.xxx
- Workstations: 172.16.5-10.xxx (generally set by DHCP)

The Technology Coordinator will assign all public TCP/IP addresses to the appropriate devices (such as the Web and E-mail servers) using those numbers assigned to SWC by the Internet Service Provider (ISP).

Primary Domain Controller Server

The Primary Domain Controller will be the server that administers and controls the **swc.tc** domain. This server will control the permissions for the network and network devices, allowing access according to the rights assigned to each user. All users must log onto this server to obtain access to SWC's network. All passwords will be stored on this server, eliminating the security risks of keeping passwords on individual workstations. The Primary Domain Controller will be located in a physically secure area and password protected. Electronic access to this server will be limited to the Technology Coordinator and the Director. Under special circumstances the Director may give temporary authorization to another IT staff member.

Main and Intermediate Distribution Facilities

The Main Distribution Facility (MDF) will be located in a secure area with restricted access. The Director will allocate keys for the MDF to the Technology Coordinator and other authorized IT personnel. The MDF will house the POP for the telecommunication and Internet connections, in addition to the primary server bank. The MDF is the center hub of the extended star network topology; all fiber optic horizontal runs terminate on the central switch.

Intermediate Distribution Facilities (IDF) will be located throughout the campus where needed, and preferably in secure wiring closets with limited access. The Director will authorize certain IT personnel to have access to the IDF locations (keys will be located in the MDF). Primary IDF locations will be connected to the MDF by a minimum of 1-gigabit fiber optic cable to the central switch located in the MDF. Secondary IDF locations, such as individual classrooms or program offices (as designated by the Director) will be connected to a primary IDF with a minimum of CAT5e copper cable.

Servers

The primary domain controller and most other servers will be located in the MDF. The Director or Technology Coordinator may locate other servers in an IDF location if it does not compromise security and if it primarily supports only the computers connected to that IDF switch. SWC will maintain the following servers (minimum), additional servers will be added based on the recommendations of the Technology, Distance Education, or Academic coordinators with the authorization of the Director.

- Authentication
- DHCP
- Proxy/Firewall
- IP Telephony
- E-mail
- Web
- Student File
- Staff File
- Business Applications
- Academic Applications
- Security/Fire System

The Administrator passwords for the network and servers will be set and maintained by the Technology Coordinator. The list of four (4) passwords will be documented and stored in a file in the IT Department's lockable fireproof cabinet. The same procedure will be followed in regards to the administrative password for all workstations and devices at SWC.

Telephone and Internet Connections

SWC will maintain at least one POT line for each of the following: fax machine, security system, and elevator phone. For basic telephone service 1 outside line per 10 employees will be maintained as the minimum ratio. For Internet connectivity a minimum of 1 frame relay (1024 Kbps rating) per 100 networked office stations (2 student stations = 1 office).

IT Operational Procedures

Network Access

The subheading *Network Access* contains the procedures for new employees or students to obtain access to the college's network resources. New users (or existing users who need to make changes) must follow these procedures to be issued a(n): user name, initial password, roaming profile, home directory, and their college email account. Access to specific components or programs on the college's network, in addition to security levels will be assigned through the procedures established herein. SWC maintains the ownership of all user accounts along with rights to monitor and access the information therein.

As stated in the *IT Department Policies* (p. 9), the employee/student must complete, sign, and submit *Form IT-D*, to the Director of Technology. Upon approval by the Director the Technology Coordinator (or authorized personnel) will, within three working days, create a unique user name, initial network password, roaming profile, and home directory for the employee/student. The employee/student will also be given access to a college email account with the same user name as for accessing the network, with an address of user-name@swc.tc (in the case of a student it would be student-id-#@dakotavillage.org) the institution does retain ownership of the account. For more information on email see subheading *E-Mail Use*. In certain instances the employee may also be given to a positional email account such as: president@swc.tc acctpayable@swc.tc or swrsi@swc.tc

If a new employee (or existing employee needs to modify) needs additional network access for restricted resources, he or she needs to complete *Form IT-E*. Restricted resources include any software platforms, databases, or other resources that have security levels, additional password requirements, or information that contains sensitive materials (as proscribed by the administration of SWC). Once the employee completes *Form IT-E* it must be submitted to the department head or area supervisor for approval. After the supervisor reviews the application and signs the form it is then forwarded to the Director of Technology to receive final approval. The Director of Technology has three working days to approve or deny the request. If denied he/she will notify, with an explanation, the applicant. If approved the following process will occur:

- The Director will contact the Technology Coordinator to establish the proper access, passwords, user name, etc. for the employee making the request. This will be completed in three working days.
- An IT staff member will contact the employee to provide an orientation/training on the network resources that are being made available. This will include information on the appropriate policies and procedures that govern use of the college's resources. During this orientation the employee will be given the access and security level that were approved.

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

In the case of new employees the department head or area supervisor may initiate the request process. However, the user name, passwords, or other security codes will not be given to the employee before the employee signs, dates, and submits Form IT-D and Form IT-E to the Director of Technology.

Internet access for workshops can be handled through the normal processes stated above or in special instances where this procedure is deemed unnecessarily cumbersome the following procedure maybe substituted. This would be in the case of a single day workshop whose participants are primarily not college students, staff, or faculty, and are unlikely to need access to the SWC network again in the foreseeable future. Under these or similar circumstances the organizer of the workshop or event may request an exemption from the Director of Technology by completing and submitting **Form IT-I**, at least three (preferably five) working days prior to the event. If approved, the Technology Coordinator will create a special user name and password, along with the appropriate network access and resources to be used by the organizer of the event. These will be removed from the system within five working days after the end of the event. The organizer will be responsible for ensuring that the participants of the event follow the appropriate policies and procedures governing use of the network and Internet at SWC.

Issues involving the access and use of a wireless network will be located under subheading ***Wireless Network*** of the ***IT Operational Procedures***.

IT Operational Procedures

Network Security

The subheading *Network Security* contains the procedures for providing the highest level of security for the SWC network while maintaining a high degree of usability. All network users, staff and students, must complete, sign, and submit *Form IT-D*, to the Director of Technology (see subheading *Network Access*). Upon approval by the Director the Technology Coordinator (or authorized personnel) will, within three working days, create a unique user name, initial network password, roaming profile, and home directory for the employee/student. The employee/student will also be given access to a college email account. If access to restricted applications or specific components of such programs is required the user must complete and submit *Form IT-E* as outlined in subheading *Network Access*. Issues pertaining to the security of the operation of a wireless network will be located under subheading *Wireless Network* of the *IT Operational Procedures*.

User Names and Passwords

The following procedure will be adhered to in regards to the creation/issuing of user names and passwords unless specifically altered by the Director. Employee user names will be the first initial of the person's first name along with the last name. Student user names will be the student ID number assigned by the Registrar. The Technology Coordinator (or designated representative) will assign the default passwords and the user will be required to change the password on the initial login.

- Passwords are case sensitive and must be a *minimum of 4* characters
- Student and most staff member passwords must be changed at a minimum of once/semester
- IT personnel and other users with administrative rights must change their password a minimum of once/month
- The same password may not be used twice in a row
- The person assigned to a particular user name is responsible for its use, therefore it *can not be shared* with other individuals or groups
 - Violations must be reported to the Director
- The Administrator password for a workstation or device will be designated by the Director
 - This password will be recorded in a secure cabinet in the IT Office
 - Only the Director, Technology Coordinator, and those staff members authorized by the Director will have access to the password(s)
- The Administrator password for the SWC network will be designated by the Technology Coordinator
 - This password will be recorded in a secure cabinet in the IT Office
 - Only the Director, Technology Coordinator, and those staff members authorized by the Director will have access to the password(s)

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

- All staff and student user names will be given restricted privileges on the network and individual workstations by default
 - The Director may authorize higher levels of access for IT staff members and other users under special circumstances
 - Users may request high access levels by following the procedure outlined in subheading *Network Access*

Firewalls and Virus Protection

The IT Department will maintain a proxy server and/or a network firewall protecting the college's LAN from outside intrusion. No server, workstation, or other network device will be assigned a public IP address without the prior approval of the Director or Technology Coordinator. The Technology Coordinator will assign public IP addresses from those assigned to SWC by the ISP. Any device with a public IP address must have a firewall protecting it from outside intrusions. Any successful or even a persistent attempt to breach the SWC systems must be reported to the Director promptly. Any attempt by a SWC network user to intentionally breach or bypass a secure/restricted system without authorization will result in loss of network privileges. The Director will report such occurrences to the President of SWC, or designate representative, for additional actions (such as suspension or termination, or even possible legal action).

The IT Department will maintain virus protection on the email server, to scan incoming messages, and on all other servers, workstations, and appropriate network devices. To limit possible routes of infection the preferred method of data transfer from the outside to systems on our network will be through email attachments. Staff members are allowed to use removable disk media or other portable storage devices such as USB key drives. Before transferring data onto the SWC system data must be scanned using an up-to-date virus protection program. Students are not allowed to use portable storage devices or recordable disks on SWC equipment without having a staff member scan the data for viruses. In the case of CD-R or similar DVD format the staff member may initial the disk after the scan thus bypassing this step in the future. Under certain circumstances a student may be authorized to perform his or her own virus scans by the Director.

Suspicious email/attachments/files should not be opened and must be reported to an IT staff member. Any computer/network problems that may be due to virus or other outside intrusion likewise need to be reported promptly to an IT staff member. These reports will be forwarded onto both the Director and Technology Coordinator for further investigation and action. Affected devices maybe removed from the network by any IT staff member to halt the transmission of the infection or intrusion until the Director, or a designated representative gives authorization to reconnect the device. Infecting, or transmitting a virus, worm, other malicious code or "spam" on or from SWC equipment is strictly prohibited, and must be reported to the Director. In cases of gross negligence or intentional violations of this policy the Director will report the occurrence(s) to the President of SWC, or designate representative, for additional actions (such as suspension or termination, or even possible legal action).

Internal Security of the SWC LAN

To protect the overall security of the LAN individual user will only have restricted rights on the workstation they use, unless authorized by the Director (see *Network Access*). The purpose for this is to limit the ability to download and install harmful programs or code. It also limits the capabilities to inadvertently change settings that could adversely affect the performance of an application, workstation, or the overall network. Incorrectly setting an IP address for example could halt the operation of the telephony system. No user, other than IT personnel designated by the Director, will have administrative rights on any computer other than the station assigned (i.e. their office computer). The Director may authorize special access for academic purposes in classrooms where a particular application's use requires a higher level of rights.

All downloads (see **Form IT-F**) or the installation of programs onto any system at SWC requires the adherence to the proper policies and procedures as outlined in this manual. The Director, or properly designated representative, will approve or deny authorization on a case-to-case basis depended on issues of resources, licensing agreements, and security.

The security of servers, along with the data stored upon them, is the primary responsibility of the Technology Coordinator. Servers (excluding those used exclusively in academic labs) must be maintained in a secure lockable area with access limited to the Technology Coordinator and others specifically authorized by the Director. Data will be backed up on a regular basis to a hard drive located on a separate chassis at a minimum of once per week. Systems or files designated as critical by the Director or the President will be backed up using the same procedure a minimum of every other working day. Archiving of data to a removable storage media will depend on its nature. However, for critical systems/files a weekly schedule for archiving will be the minimum. Archived media will be stored in a lockable fireproof storage unit. Access will be limited to the Technology Coordinator and others specifically authorized by the Director.

Security of individual workstations and the data stored upon them is the primary responsibility of the assigned user. When the area is open to public the individual user should lock their computer and/or use a password protected screensaver when logged on to the system. When a user will be absent from their station for an extended period of time it is recommended that they shut down the system or log off. If using a common area computer a user must log off the system before leaving.

IT Operational Procedures

Internet Use

The subheading *Internet Use* contains the procedures governing student and staff access and use of the Internet. This procedure also establishes guidelines on how SWC connects to the Internet.

As stated in the *IT Department Policies* (p. 9), the employee or student must complete, sign, and submit *Form IT-D*, to the Director of Technology. Upon approval, the Technology Coordinator (or authorized personnel) will create a unique user name, initial network password, roaming profile, and home directory for the employee (see *Network Access*). No one is allowed access to the Internet using SWC equipment without completing this form. Exceptions will be made for special workshops or events with the approval of the Director of Technology, and in the public section of the SWC Library

If a new employee needs additional Internet access (or existing employee needs to modify) he or she needs to complete *Form IT-E*. Additional Internet access would include any ability to download files of the Internet using FTP or related protocols or plug-ins not normally provided to employees, or passwords to restricted web sites (as proscribed by the administration of SWC). Once the employee completes *Form IT-E* it must be submitted to the department head or area supervisor for approval. After the supervisor reviews the application and signs the form it will be forwarded to the Director of Technology to receive final approval. The Director of Technology has three working days to approve or deny the request. If denied he/she will notify, with an explanation, the applicant. If approved, the following process will occur:

- The Director will contact the Technology Coordinator to establish the proper access, passwords, user name, etc. for the employee making the request. This will be completed in three working days.
- An IT staff member will contact the employee to provide an orientation/training on the Internet resources that are being made available. This will include information on the appropriate policies and procedures that govern their use. During this orientation the employee will be given the access and security level that were approved.

In the case of new employees, the department head or area supervisor may initiate the request process. However, the user name, passwords, or other security codes will not be given to the employee before the employee signs, dates, and submits *Form IT-D* and *Form IT-E* to the Director of Technology.

Internet access for workshops and for the public library computers can be handled in a separate manner. In the case of the library, the Director of Technology or Technology Coordinator will work with the librarian to designate certain computer stations for open access. These stations will log into the network using a special user name with restricted access levels. Software or other blocking devices maybe used on these stations that restrict

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

web surfing beyond the normal levels proscribed at SWC, as determined by the librarian. Monitoring the use of the public stations in the library will be governed by policies and procedures established by the librarian and the SWC administration. Other aspects of these workstations will still be under the governance of the IT Department.

Internet access for workshops can be handled through the normal processes stated above, or in special instances where this procedure is deemed unnecessarily cumbersome; the following procedure may be substituted. This would be in the case of a single day workshop whose participants are primarily not college students, staff, or faculty, and are unlikely to need access to the SWC network again in the foreseeable future. Under these or similar circumstances the organizer of the workshop or event may request an exemption from the Director of Technology by completing and submitting **Form IT-I**, at least three (preferably five) working days prior to the event. If approved, the Technology Coordinator will create a special user name and password, along with the appropriate network access and resources to be used by the organizer of the event. These will be removed from the system within five working days after the end of the event. The organizer will be responsible for ensuring that the participants of the event follow the appropriate policies and procedures governing use of the network and Internet at SWC.

The Technology Coordinator has the primary responsibility for the establishment, maintenance, and regulation of the Internet at SWC. He or she may delegate these roles, in part, by designating an IT staff member as the web master (etc.), with the consent of the Director of Technology. The following are general guidelines regarding the Internet at SWC:

- The Proxy Server will control Internet traffic between the LAN and the WAN, unless specially approved by the Director.
- A log of Internet traffic will be maintained by the Technology Coordinator, and will be periodically reviewed for inappropriate use. The log will be archived for a minimum of 14 days before being deleted.
- Known or suspected use of the Internet that is inappropriate is to be reported promptly to the Technology Coordinator. Inappropriate use includes, but not necessarily limited to:
 1. Downloading, storing, or printing files or messages that are profane, obscene, or that use language or images that offends or tends to degrade others.
 2. Violating copyright laws
 3. Using SWC resources for commercial or financial gain without administration approval.
 4. Vandalizing data of others, damaging equipment or gaining unauthorized access to resource or invasion of privacy
 5. Using other people's accounts, posting personal communications without the original author's consent
 6. Wastefully using finite resources, including the unsanctioned use of Internet radio or streaming video (permission must be granted by Technology Coordinator, Director of Technology, or an officially designated representative).

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

- Inappropriate use of the Internet at SWC could result in the termination or restriction of the user's accounts, in addition to other penalties established by the administration of the college.
- To maintain acceptable bandwidth, the Technology Coordinator will establish a point system to calculate typical and high traffic usage rates.
- The Technology Coordinator or designated representative will maintain a reasonable level of security, including proxy settings and/or firewalls, against outside intrusions. Virus, spam, and other appropriate protections will be maintained at reasonable levels. The Director of Technology will be notified of breaches, and be given periodic assessments on the security status along with any suggested or required upgrades.
- The Technology Coordinator or designated representative will establish, maintain, and upgrade the SWC web site. He or she will establish guidelines for the format and content of all web sites hosted on any domain owned or controlled by the college. Documentation and regular briefings will be provided to the Director of Technology.
- The Technology Coordinator or designated representative is responsible for the establishment, maintenance, removal, and allocation of all domains, IP addresses, bandwidth, and related items owned or controlled by SWC. Documentation and regular briefings will be provided to the Director of Technology.

IT Operational Procedures

E-Mail Use

The subheading *E-Mail Use* contains the procedures governing establishment and use of student and staff e-mail accounts provided by SWC. This procedure also establishes guidelines for accounts provided to individuals and groups not part of the college.

As stated in the *IT Department Policies*, the employee or student must complete, sign, and submit *Form IT-D*, to the Director of Technology. Upon approval, the Technology Coordinator (or authorized personnel) will, within three working days, create a unique user name, initial network password, roaming profile, and home directory for the employee/student (see *Network Access*). At this time the user will also be assigned an email account by the Technology Coordinator.

The status of the person requesting the account will determine what domain will be used, the format of the user name, the default password, and storage space allotted. The Director of Technology under special circumstances will consider exceptions.

SWC Faculty and Staff

- The account will be created on the **swc.tc** domain
- User name will be the initial of the first name and the full last name, for example John Doe would be jdoe@swc.tc
- The default password will be **swcc**
- Storage space will be limited to 60MB

SWC Administrative Offices

- The account will be created on the **swc.tc** domain
- User name will be the office title or program name, such as president@swc.tc or studentservices@swc.tc or swrsi@swc.tc
- The default password will be **swcc**
- Storage space will be limited to 100MB
- The department head will determine who has access to the account
- If requested an alias could be established for these accounts

SWC Students

- The account will be created on the **dakotavillage.org** domain
- User name will be either the student ID# or first name (dot) last name, such as d1111@dakotavillage.org or john.doe@dakotavillage.org
- The default password will be the **Student ID#**
- Storage will be limited to 20MB

Sisseton Wahpeton Oyate Office Holders and Staff

- The account will be created on the **swtc.us** domain
- User name is based on the title of the office. For offices at the district level the title will be preceded by a two letter code: BC (Big Coulee), BL (Buffalo Lake), ES (Enemy Swim), HV (Heipa/Veblen), LH (Long Hollow), LT (Lake Traverse), and OA (Old Agency). For example: chair@swtc.us or ESrep@swtc.us
- The default password will be **swtc**
- Storage space will be limited to 60MB
- Requests for new accounts or modifications are to be forwarded from the Tribal MIS Manager to the SWC Director of Technology
- If requested an alias could be established for these accounts

Sisseton Wahpeton Oyate Employees

- The account will be created on the **swst.us** domain
- User name will be first name (dot) last name, such as john.doe@swst.us
- The default password will be **swst**
- Storage space will be limited to 40MB
- Requests for new accounts or modifications are to be forwarded from the Tribal MIS Manager to the SWC Director of Technology

Public Individual or Group Addresses

- The account will be created on the **dakotavillage.org** domain
- User name will be first name (dot) last name, such as john.doe@dakotavillage.org, or created by an automated system
- The default password will be **dakota**
- Storage space will be limited to 20MB
- Other guidelines will be established by the Technology Coordinator or by the designated Postmaster

The Technology Coordinator, or a person officially designated as Postmaster, will establish and maintain at least one email server capable of hosting the domains listed above along with reserving the required number of public IP addresses. The Postmaster will perform the required system maintenance, including software updates, required upgrades to the hardware, virus protection, and other configurations as needed. Disk storage and reasonable bandwidth will be maintained at a minimum level for twice the total number of SWC faculty, staff, and students. Any required acquisitions will be forwarded to the Director of Technology by submitting **Form IT-G**. In addition to ensuring adequate virus protection to the email server the Postmaster will make all reasonable efforts to eliminate spam from entering the system or originating from it.

The Policies and Procedures of the college and the SWC IT Department govern all email accounts provided by SWC. By accessing the account, the user is consenting to the provisions established in **Form IT-D** of the **SWC IT Department Policies**. Additionally, all faculty, staff, and administrative office accounts at SWC can be considered work product

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

dependent upon the policies established by the SWC Board of Trustees. Accounts for the Sisseton Wahpeton Oyate Office Holders and Employees may be deemed work product dependent on the policies established by the Tribal Council. Student and Public Individual/Group accounts are not subject to any work product rule, but are still liable to the appropriate use provisions. Inappropriate use includes, but is not limited to, the following:

- Using account provided by SWC for commercial or financial gain without administration approval.
- Using account provided by SWC for the creation or transmission of spam
- Using other people's accounts, posting personal communications without the original author's consent
- The willful transmission of viruses or another harmful programs

The allocation of accounts and other email related resources are in the following order:

1. SWC Faculty, Staff, and Students
2. SWC Administrative Offices
3. Sisseton Wahpeton Oyate Office Holders and Employees
4. Public Individuals and Groups

IT Operational Procedures

Requests for Service

The subheading *Requests for Service* details the procedures for differentiating between basic troubleshooting, emergency services, and regular service requests. Each of these different services has its own related procedures in regards to scheduling priorities, how service is rendered, and the reporting processes. In many circumstances, the decision of which procedure to use is left to the discretion of the IT staff member on the scene.

Regular Service Requests: The preferred method of handling any service request is to have the individual asking for support to complete *Form IT-B* and submit it to the Director of Technology. The Director will then review the application and either approve or disapprove the request. This decision will be rendered in one or two working days under most circumstances.

- If disapproved the Director will contact the individual making the request and explain why it was rejected, and suggest a possible solution to the problem.
- If approved the Director will assign a priority level and service number to the application and will forward it to the appropriate IT personnel.
- The IT staff member will then complete the request, or assign it to the Help Desk.
 - Upon completion of the service request, the proper form must be dated and initialed by the IT staff member and returned to the Director.
 - The IT staff member completing the service request must also complete (if applicable) *Form IT-C* and submit it to the Director.
- Priority levels will range from 1 (the highest) to 3 (the lowest). All the requests with a ranking of 1 must be completed before work can be start on those with a ranking of 2, and so on.
 - The Director can reassign a ranking based on changing circumstances.
 - IT personnel may complete several related work requests of various priorities if it is more efficient, such as fulfilling all open requests on a particular workstation.
- Service numbers will be assigned using the following formula: xx (month) – x (service requests approved that month) – xx (last two digits of the year).
 - For example the 21 approved service request in June of 2002 would be listed as: 06-21-02
- Requests that involve changing or resetting user-names or passwords, or for creating a roaming profile/network drive require the completion and submission of *Form IT-H*. Upon the receipt of the application the Director will proceed as if it was a regular service request.
- A request for Internet downloads or software installation requires the completion and submission of *Form IT-F*. Upon the receipt of the application the Director will proceed as if it was a regular service request.

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

- Requests for changing access level/rights on the network or an individual workstation requires the completion and submission of **Form IT-E**. Upon the receipt of the application the Director will proceed as if it was a regular service request.
- **Form IT-G** must accompany requests that require the purchase of hardware, software, or services not already available at the college.

Basic Troubleshooting Service Requests: These requests deal with basic service of equipment or common application problems such as: not being able to access the network or related services, reconnecting a network drive path, a printer/copier being out of toner or staples, or a problem with a software application. Proper procedure in these cases is to contact the Director of Technology or the Student Help Desk.

- The Director or the Student Help Desk member will note the occurrence on the weekly troubleshooting log, and at their earliest convenience the person on call will investigate the situation.
- If possible the IT member will fix the problem and will then initial the entry on the weekly troubleshooting log.
- The IT member will then complete and submit (if applicable) **Form IT-C** to the Director. Notes should be filed for reference in future troubleshooting cases.
 - There are certain cases that do not require the completion and submission of work notes. If it is a basic and routine procedure such as someone had the caps lock on will typing in their password, or if the computer had been moved and the patch cable came out.
 - **Form IT-C** must always be completed if a hardware component was replaced or if software needed to be installed.
- If new hardware or software needs to be purchased to remedy the problem **Form IT-G** must be completed and submitted to the Director.

Emergency Service Requests: These are the highest priority service requests. Work will commence as soon as possible, even prior to the completion and submittal of the proper forms to the Director. The IT staff member(s) completing the service must submit work notes and/or **Form IT-C** to the Director as in the case of a **basic troubleshooting service**.

Emergency services will be regulated to those systems designated as mission critical to the Sisseton Wahpeton College.

- The following have currently been designated **Mission Critical Systems**
 - Network accounting applications
 - *FX Scholar* or *Empower* software
 - Telephone communications
 - Internet communications to *Fastlane* and online transactions
 - Instructional technology services
 - File and application servers

IT Operational Procedures

Purchasing Procedure

All procurement of hardware, software, or technology services that will be part of or impact the Sisseton Wahpeton College's data or communications networks must be purchased through the IT Department. The purpose of this process is to ensure compatibility of new components with the existing infrastructure and to maximize the efficiency of our resources. The IT Department will only maintain and service equipment and software that was procured, allotted, and implemented in a manner consistent with the appropriate policies and procedures.

- The individual wishing to make a purchase must complete *Form IT-G* and submit it to the Director of Technology.
 - The form must have the signature of the appropriate departmental supervisor or grant officer.
 - The form must have the appropriate fund number and be an allowable expense.
 - The exact item does not have to be listed, although a detail of features or capabilities that are required should be included. For example, one would not have to list a HP 4550DN, but rather just ask for a colored laser printer with a duplexer.
- The Director will evaluate the request and determine if the product or service is already available, or needs to be acquired from outside sources. The Director will either approve or deny the request in 3 working days (if feasible) with an explanation of why it was denied, if applicable.
 - If approved the request will be processed by the IT Department.
 - At least two approved vendors will be contacted for quotes.
 - After choosing a vendor the Director (or authorized representative) will complete a SWC Purchase/Check Request according to the appropriate procedures of the college.
 - Upon receiving approval from the Business Office the Director (or authorized representative) will place the order with the vendor.
 - Once the order is received it will be inventoried according to the IT Department's policies and procedures. Then the individual/program officer requesting the product/service will be notified.
 - The IT Department will keep one copy of all documents for their files.

IT Operational Procedures

Computer Science & Technology Instruction

The subheading *Computer Science & Technology Instruction* contains the procedures for the academic sector of the IT Department, and in particular the operation of the CST programs. Academic programs, courses, and workshops in the field of technology are the direct province of the Academic Coordinator. Since this position serves as a liaison between the IT Department and academic sector of the college, the Academic Coordinator will report directly to the Director of Technology and to either the Academic Dean or the Vocational Education Director. He or she will also, whenever possible, serve as the IT Department's primary representative on any of the intitutional committees at the Sisseton Wahpeton College that are focused on education.

The Academic Coordinator will supervise all other CST faculty/trainers, implement and ensure curriculum standards, and will maintain the CST resources and facilities in compliance to certification requirements. The CST programs were established to train high quality IT personnel to staff small to mid-size departments that are common on or near the Lake Traverse Reservation. The procedures outlined in this document are to maintain the focus and quality of the CST programs and related academic/training functions.

Curriculum

- All CST instructors will submit a list of courses they propose to teach to the Academic Coordinator for approval. The Director of Technology will be forwarded the list with the Academic Coordinator's recommendations prior to its submittal to Curriculum Committee.
- All instructors teaching a CST or related course must submit a copy of the syllabus to the Academic Coordinator 2 weeks prior to the beginning of class. Upon his/her approval the syllabus will be forward to the proper college staff as per SWC policies, and also to the Director of Technology. The Academic Coordinator will maintain a record (preferably in an electronic format) of all course syllabi for the CST and related programs.
- At a minimum of once per year the Academic Coordinator will form a committee to review the CST curriculum. The committee may suggest any changes to the existing curriculum that would enhance the program, along with the addition or removal of courses. The Academic Coordinator will then report the committee's finding and recommendations, including an implementation or action plan, to the Director of Technology for approval.
- The Academic Coordinator through the proper channels will process any changes to the CST curriculum that requires approval from an individual or committee outside of the IT Department. Strict adherence to the proper SWC policies and procedures is required.

Adopted by the Sisseton Wahpeton College
Effective February 27th 2004

- The Academic Coordinator has the right to review, reject, and/or mandate curriculum material, activity, or pedagogy for use in any CST course, consistent with SWC and IT policies and procedures.

Instruction

- The Academic Coordinator is the direct supervisor of CST instructors and oversees the instruction of any faculty teaching a CST or related course. The Academic Coordinator will make the assignment of CST courses.
- In regards to hiring additional CST faculty, whether full-time or adjunct, the Academic Coordinator will submit a request to the Director of Technology for approval. In the case of an adjunct position the Academic Coordinator may fill the position (using standard SWC policies and procedures which govern this process) with an instructor that has previously taught at SWC and is in good standing. In the case of full or part time positions, or even new adjunct faculty the Academic Coordinator will form a committee to create a job description, advertise the position, interview the candidates, and make their recommendations to the Director of Technology, in addition to following standard SWC policies and procedures.
- The Academic Coordinator will create the CST course schedule for each semester and submit it to the college's Curriculum Committee.
- Instructors teaching a CST course will be evaluated at the end of each semester. The evaluation process will be the same as the one used for other IT staff with addition of an academic component. The use of inquiry-based and hands-on teaching methods is strongly encouraged.
 - The Academic Coordinator will be evaluated by one or more of the following individuals: Director of Technology, the Academic Dean, or the Vocational Education Director
 - The Academic Coordinator will evaluate other CST faculty
- Every instructor teaching a CST course is expected to attend both the mandatory SWC faculty meetings and CST meetings. CST meetings will occur at a minimum of twice per semester and will be scheduled by the Academic Coordinator.

CST Resources and Facilities

- The Academic Coordinator will maintain an inventory of all curriculum materials, equipment, software, and other durable materials for the CST program in a manner consistent with IT procedures. Consumable materials will be recorded and periodically checked by the Academic Coordinator for replenishment, and to check for waste.
- The Academic Coordinator will maintain the CST facilities and equipment in compliance with the certification requirements. The Director of Technology will be notified promptly in case of any and all deficiencies.
- Any purchases of hardware, software, or other materials besides curriculum materials need to follow the appropriate IT procedure.
- With permission of the Director of Technology the CST or other program under the direction of the Academic Coordinator may maintain a LAN that is not connected to the college's systems. The operation of this LAN does not have to adhere to the policies and procedures of the SWC IT Department outlined in this manual.