SWC

Sisseton Wahpeton College

Policy No	700	Effective Date	
Policy Title		Revisions Date(s)	
Policy Owner		Classification	

PURPOSE

The purpose of the Sisseton Wahpeton College Information Technology Department's Policies and Procedures is to provide the operational guidelines for the development, implementation, maintenance, and use of the information systems at this institution. The implementation of these policies and procedures is to provide for the overall security of the information systems at the college, while still allowing an acceptable level of usability and flexibility. It is important to understand that the purpose is not to arbitrarily set rules to limit the privileges of individual users, but is rather to promote the general efficiency of the college as a whole. The need to maximize limited resources and to protect the confidentiality and integrity of the information systems from a variety of threats requires certain sacrifices to be made. An integrated network provides many advantages to an individual user, greatly enhancing their capabilities and productivity. However, by its very nature such a network is also vulnerable to viruses, security threats, and debilitating consequences caused by the irresponsible actions of one user, which can affect everyone utilizing the system.

The structure of the Information Technology (IT) Department, and the basic roles and responsibilities of the IT staff are also outlined in this document. Further information is located in the Sisseton Wahpeton College's ***Strategic Technology Plan***. This is a living document and will be revised as necessary, with the approval of Administration, and available for review by the Sisseton Wahpeton College Board of Trustees. ***See form IT-A.***

DEPARTMENT STRUCTURE

The Information Technology (IT) Department of the Sisseton Wahpeton College (SWC) is under the jurisdiction of the Director of Technology. All other members of the IT Department are under the authority of the Director. All network media, devices, appliances, nodes, and other workstations along with all other information or instructional technology systems, including software, are under the authority of the Director. The Director of Technology is under the direct supervision of the CFO.

Responsibilities and Duties of the IT Department

The IT department is responsible for implementing, maintaining, and archiving all network systems, computer workstations, servers, and other related devices and software applications. The IT department is responsible for the procurement, allocation, and the repair or replacement of any of the aforementioned components of the information systems network, as determined by established protocols and procedures. The IT department will be responsible for creating and implementing operational procedures and protocols for the information systems network at SWC. Other responsibilities of the IT department include:

- Technical support to faculty and staff as needed, limited to reasonable requests as determined by established protocols and procedures
- Basic training in computer concepts and troubleshooting to faculty and staff, as requested and need is determined
- Support to faculty in the implementation of instructional technologies in their curricula
- Provision and maintenance of digital media hardware for use in classrooms, and other areas outside of the SWC Library
- Administer projects (grants) in the area of technology as assigned by the President

Duties of the Director of Technology (Chief Information Officer)

The Director will review and present all IT policies, procedures, and protocols to the President. The Director is responsible for analyzing the status of all Information Technology components and the overall capabilities of the system, and will report his or her findings to the President. The Director will periodically carryout evaluations to determine the future requirements of the technological infrastructure and the personnel requirements of the IT department, and will present his or her recommendations to the President for review and approval. Other responsibilities of the Director include:

- Supervise and coordinate the activities of the IT staff and the Student Help Desk
- The procurement, allocation, and use of IT equipment and software
- Development and supervision of IT outreach programs
- Coordinating with and supporting other departments at SWC, and the use of the instructional/information technology systems
- Develop, manage, and oversee the IT Department's budget
- Develop, review, and modify IT policies and procedures, and the IT Department's Strategic Plan
- Evaluate, or review the evaluations of IT personnel (at least annually)

Duties of IT Staff

The IT staff will compile data from the information systems components and report this data to the Director. The IT staff will maintain and repair the information systems components. The IT staff will be responsible for the installation of all new information systems components, and software. The IT staff will provide technical support to the faculty and staff of SWC, limited to reasonable requests, as needed.

In addition to specific duties outlined in the ***IT Operational Procedures*** all departmental employees will:

- Comply with all SWC, Tribal, and Federal policies, regulations and laws that govern the college
- Maintain high levels of confidentiality

- Maintain high standards of ethical conduct and avoid dishonest or illegal behavior
- Demonstrate a high level of integrity and responsibility
- Participate on SWC committees and meetings
- Perform other duties as assigned

All IT Department personnel will sign a ***SWC Confidentiality Agreement*** and will abide by all relevant policies and procedures established by SWC in general, or by the IT Department in particular.

Additional information and detailed descriptions of key IT personnel can be located in the ***IT Operational Procedures***, subheading ***IT Department Structure***.

Student Help Desk

The Student Help Desk will report to the Director, or designated representative, and will support a variety of activities within the IT Department. The Student Help Desk's primary focuses will be in the area of user support to staff and students, and assisting IT personnel on other projects as assigned by the Director, or authorized representative. The students will be primarily drawn from the CST program, although any student can apply for a position.

Non-IT Staff

The Director has the ability to give certain key individuals outside the department additional user-rights. These privileges are temporary and are to perform specific trouble-shooting and student support tasks.

Non-IT staff is not authorized to install any hardware or software on any computers owned by SWC without prior consent of the Director. This includes downloading files from the Internet and the installation of software/hardware not owned by SWC. All purchases and repairs of computers, software, or related equipment and materials must have prior authorization by the Director.

All software and hardware related to computer systems, the network, and the phone system are under the IT Department. Certain portable software and hardware components will be available for use by the faculty, staff, and students of SWC. These items must be signed for by a staff or faculty member for a limited time, and may be used off campus in authorized cases. The individual signing for the software/hardware assumes responsibility, including financial, for the prompt return of the said item(s) in good condition.

Additional detail is located in the ***IT Operational Procedures***, under subheading ***IT Resources and Equipment***.

SYSTEMS DOCUMENTATION

All computer systems, including peripherals, will be documented and included in a cross referenced database that will allow the IT staff easy access to information regarding any technical aspects of the colleges information system. The database will be referenced by description, manufacturer, serial number, model number, and other relevant indicators such as an IT number and location. Components to be included in the database will include, but will not be limited to: PCs (possibly including some internal components), PC peripherals, printers, cameras, digital projectors, UPS units, and network components (switches, routers, servers, and media). This database must include all components in use as well as those in storage (except that which has been designated as salvage).

Additional detail is located in the ***IT Operational Procedures***, under subheading ***Systems Documentation***.

Before any changes are made to any of the information systems components, a work request form must be filled out by the employee and approved by the Director or authorized IT staff member. The President or his or her administrative representative must also approve any new purchase.

All changes made to any component of the information systems must have correlated, dated changes in the database by authorized IT personnel. ***See forms IT-B and IT-C****.*

NETWORK STRUCTURE

The basic structure of the computer network at SWC will be Active Directory running on a minimum of two domain controllers on an Ethernet network running TCP/IP. There will be a Primary Domain Controller, Secondary Domain Controller, File Server(s), and other servers as warranted for network applications and Internet services.

Standardization of operating systems, utility programs, application software, and hardware components will be adhered to whenever feasible. Network printers will be used unless special circumstances, such as confidential reporting, require the use of a local printer.

Additional detail is located in the ***IT Operational Procedures***, under subheading ***Network Structure***.

Primary Domain Controller Server

The Primary and Secondary Domain Controllers will be the servers that administer and control the ***swcollege.edu*** domain. These servers will control the permissions of the network and network devices, allowing access to network devices according to the rights assigned to each user. The Domain Controllers will be located in physically secure areas and password protected. Electronic access to these servers will be limited to the Director, and properly authorized personnel.

Protocols

SWC's computer network will use TCP/IP as the primary protocol. TCP/IP addresses will be assigned to each node. The TCP/IP addresses used will be one of the sets reserved for private networks. All workstations, servers, and network devices will use this address set with the exception of those devices that need a public IP address. SWC's Internet Service Provider (ISP) will assign TCP/IP addresses to these exceptions. Internal addresses will be assigned and recorded by the designated IT personnel.

Physical Structure

A minimum of Category 5 cabling will be used for workstation to switch connections, using industry standard pin-outs on RJ45 modular network ends. Gigabit Ethernet, or faster, connections between servers and switches may also be used. Switch to switch connections will be 100mps or greater, using at least Category 5 cabling.

NETWORK ACCESS

All staff, faculty, and students of SWC are required to sign an Internet/network/email use agreement. All visitors using computers on campus are required to sign the appropriate use agreement. In special cases such as a one-day workshop, the sponsor of the event, with the consent of the Director, may take personal responsibility for the participants, in which case each individual will not be required to sign the agreement. This agreement will describe the acceptable use policies of SWC and will be a binding agreement between the user and SWC. ***See Form IT-D****.*

Some examples of unacceptable use are:

A. Using the network for illegal activity, including violation of copyright or other contracts (see Copyright, page 9).
B. Using the network for financial or commercial gain.
C. Degrading or disrupting equipment, software or system performance.
D. Vandalizing the data of another user.
E. Wastefully using finite resources.
F. Gaining unauthorized access to resources or entities.
G. Invading the privacy of individuals.
H. Using an account owned by another user.
I. Posting personal communications without the original author's consent.
J. Posting anonymous messages.
K. Downloading, storing, or printing files or messages that are profane, obscene, or that use language or images that offends or tends to degrade others.

Dependent upon the nature of the violation and the frequency of the offenses, sanctions may be enforced by the SWC administration according to SWC policy. All illegal activities will be immediately reported to the President, or designated representative. Sanctions for violations may include:

- A verbal warning
- A written reprimand (copy placed in the employee’s personnel file)
- Restriction of user privileges on the college’s network
- Suspension of SWC network privileges

All authorized users will be given a unique user ID and an initial password. The Director will assign and IT personnel will implement user-rights. The user/password combination will give each user access to individual drives, folders, or files accessible only by the logged in user. Access to most resources will be allowed regardless of workstation used. SWC maintains the ownership of all user accounts along with rights to monitor and access the information therein.

Passwords will be changed every semester, minimum, for security reasons. Users with access to sensitive data are required to change passwords more often.

Additional detail concerning user name, rights, access, and passwords is located in the ***IT Operational Procedures***, under subheading ***Network Access***.

NETWORK SECURITY

In order to obtain the highest degree of security for the systems and data on the SWC network while maintaining appropriate levels of usability and cost efficiency, the adherence to the following policies are mandated. The Main Distribution Facility and all servers will be located in secure areas with access restricted to the Director and authorized personnel. All individuals or groups must follow the policies and procedures listed in the ***Network Access*** section of this manual in order to use any system owned by or connected to the SWC LAN. The default level of access to the SWC systems will be that of a restricted user.

Due to the requirements and access allotted by their position all IT personnel are required to sign the ***SWC Confidentiality Agreement***.

All individuals utilizing SWC equipment or network resources agree not to cause intentional (or through gross negligence) damage or breach/bypass security measures established by the IT Department. Any violation of this policy will be reported to the Director of Technology and/or the President of SWC. Sanctions could include suspension of privileges, termination, or legal action.

The IT Department will maintain an appropriate level of protection from outside intrusions, viruses, and internal security breaches. At a minimum this will include a network proxy server and/or firewall, an up-to-date virus protection, and the use of reasonable password procedures.

POINT-OF-SALE SECURITY

SWC's Point-of-Sale servers, terminals, and other hardware and software will be secured as outlined by the Payment Card Industry Data Security Standard (PCI-DSS)

Additional detail is located in the ***IT Operational Procedures***, under subheading ***Network Security***.

INTERNET USE

Faculty, staff, and students may not download any files on any computers owned by SWC without the prior consent of the Director or an authorized representative. Visitors will under no circumstances be allowed to download any files on to the college's computers. All files approved for download will be documented and dated. *See **Form IT-F**.*

The IT Department will have the ability to monitor and log all Internet (including Email) activity on all computers under SWC jurisdiction, as stated in the Internet Acceptable Use agreement. If created, the log will be reviewed and questionable items will be brought to the attention of the Director. If necessary, the Directory will make a report to the President (or properly designated representatives). Violations of SWC policy or relevant laws will result in sanctions that may include restricted access, probation, suspension, or other actions as decided by the President (or properly designated representative). Notification of this policy will be issued to SWC users every semester.

Additional detail is located in the ***IT Operational Procedures***, under subheading ***Internet Use***.

COPYRIGHT

Copyright is the exclusive legal right, given to an originator or an assignee to print, publish, perform, film, or record literary, artistic, or musical material, and to authorize others to do the same.

Copyright infringement (piracy, etc.) is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce, distribute, adapt, or publicly perform or display a copyrighted work. In the file-sharing context, downloading or uploading of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or “statutory” damages affixed at not less than $750 and not more than $30,000 per work infringed. For “willful” infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys’ fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

Examples of Inappropriate Uses of Copyrighted materials

1. Posting copyrighted materials on the open web without permission.

2. Copy from consumable materials (workbooks, test booklets, etc.)

3. Copying and distributing or placing on reserve the same excerpts for more than one semester without permission

4. Copying large portions of materials, especially to avoid purchasing a copy.

5. Copying music for use in performance.

E-MAIL USE

E-mail users will be required to sign an Internet/network/email use agreement before their accounts are activated. Legally, SWC retains its ownership of the e-mail system employed at the college and has the right to monitor its use. However, due diligence will be used to treat electronic mail with the same privacy and professionalism as physical mail.

Spam e-mail will not be tolerated. Spam e-mail originating from SWC’s e-mail server(s) may result in the sender’s account being deactivated. Individual users are also responsible for using good judgment in regards to content and virus issues when sending and receive e-mail while using the college’s e-mail server(s).

Limitations may be assigned by the Director on the storage size of individual accounts on the server and on individual message size.

Additional detail is located in the ***IT Operational Procedures***, under subheading ***E-Mail Use***.

REQUESTS FOR SERVICE

A Work Order form will be available for faculty and staff requiring assistance. Work Order forms will include the date of request, name and department of requester, work to be done, and justification. *See* ***Form IT-B****.* The requests will be filed with and reviewed by personnel of the IT staff. The IT staff will make recommendations to the Director. The Director will review all work requests. Work requests that require the purchase of equipment or materials will need to follow the policies established by the ***Purchasing Procedure***.

Any qualified IT staff can do basic trouble-shooting, without prior approval by the Director. The staff member completing the work must complete ***Form IT-C*** (if applicable) and submit it to the Director.

Additional detail is located in the ***IT Operational Procedures***, under subheading ***Requests for Service***.

PURCHASING PROCEDURE

All faculty and staff wishing to purchase computer systems, hardware, software, network devices, or consumables must fill out an Acquisition Request; see ***Form IT-G***, for new acquisitions. The Director will review the requests for procurements and if approved, will make recommendations to the President or administrative representative for purchase.

Additional detail is located in the ***IT Operational Procedures***, under subheading ***Purchasing Procedure***.

Video Surveillance and Recording

SWC uses a video surveillance and recording system in order to help protect students, staff, faculty, property, and community members on campus.

Video footage of students, staff, or visitors may be retrieved, viewed, archived, or audited for the purpose of determining adherence to official SWC policies or Student Code of Conduct, and local, state, and federal laws.

Video recordings may be released to third parties in compliance with local, state, and/or federal laws.

The surveillance equipment will be used in a professional, ethical, and legal manner, avoiding unnecessary intrusion upon privacy and other civil liberties, and in compliance with SWC polices of nondiscrimination, sexual harassment, and freedom of expression.

Surveillance equipment will not be installed or used in areas where there is a reasonable expectation of privacy according to accepted norms (restrooms, lockers, individual dorm rooms).

Surveillance footage will not be accessed, disclosed, or used except as outlined in this policy.

Only individuals authorized by the SWC President or Board of Trustees shall have access to the surveillance equipment, or be permitted to retrieve archival video footage.

Audio recording capabilities will **not** be enabled, if available.

Cameras may be placed in locations on a temporary basis for investigative purposes, as authorized, for situations such as theft, etc.

Recorded video will be kept for an initial time period, as storage space allows, with oldest videos being overwritten as space requires. Video may be archived for longer periods as authorized.

IT OPERATIONAL PROCEDURES

The IT Operational Procedures are rules and guidelines established within the IT Department that govern the intradepartmental activities and daily functions of the IT staff. These procedures are located in the ***IT Operational Procedures*** section of this manual. This manual is correlated to the policies established within the ***Information Technology Department Policies***, and contains additional detail on the procedures followed by the IT Department to ensure that the stated policies are enforced.

All request for services provided by the SWC IT Department need to be submitted to the Director of Technology by completing the appropriate form located in supplement: **IT Department Policy Forms**. Unless stated otherwise in the Information Technology Department's policies and procedures, all requests will be processed within two to three working days whenever feasible. If the request is denied, the Director will contact the individual and explain why the application was not approved and, when possible, offer an alternative solution.

As the procedures that are set forth in this document are intradepartmental in nature, changes may be made with the approval of the Director of Technology.

POLICY STATEMENT

-

POLICY DEFINITIONS

End of Policy