SOUTHWESTERN ILLINOIS COLLEGE DISTRICT 522

BOARD POLICY

TITLE:	**Acceptable Use of Information Technology Resources**
CODE:	**7016**
DATE ADOPTED:	**March 2002**
DATE REVIEWED:	**11/07; 01/10; 06/11; 11/19; 08/20;01/23; 08/23**
DATE AMENDED:	**12/07; 02/10; 07/11; 12/19; 09/20; 03/23; 09/23**

1. Purpose

Southwestern Illinois College provides extensive computing and network communications services. These services, known collectively as Information Technology (IT), are part of the campus infrastructure, and their purpose is to support the College's teaching and public service missions. Technology and information services administered by the College, including any service arrangements that involve resources hosted off-campus, are part of the campus technology environment for the purposes of this policy. Unless explicitly noted, these policies apply to all computing and network communications equipment in all units of the College and to all individuals (employees, students, Persons of Interest, vendors etc.) with access to Southwestern Illinois College computing resources, confidential or personal material, and Personally Identifiable Information (PII).

All members of the College community are given notice of this policy by virtue of its publication, and are subject to it on the same basis. Ignorance of this policy does not relieve anyone of his or her responsibilities under it.

2. Definitions

SWIC Network: the computer and data communications infrastructure at the College. It includes the campus backbone and local area networks, all equipment connected to those networks (independent of ownership), all equipment registered to any domain name owned by the College and all applications and information services administered by the College (including, but not limited to, eSTORM, InfoShare, PeopleSoft, Office 365, course management systems, and e-mail.)

VPN: SWIC's Virtual Private Network (VPN) provides an end-to-end encrypted tunnel which allows authorized users secure access to the SWIC Network from any location.

Collaboration Platforms: Collaboration software tools which enables communication for audio meetings, video meetings, and virtual classrooms, with built-in features such as chat, screen sharing, and recording.

Bulletin Board: Non-public facing electronic message forum for internal use by employees or POIs.

IT: the College's Information Technology division.

College units: the various departments and divisions and offices of the College.

Confidential: Southwestern Illinois College information that is non-public or is intended to be non-public. The types of data, level of security, and conditions for release are based on the requirements of applicable laws, regulations, policies, contracts and agreements, respect of privacy and identity information, and other operational needs

Personal Material: Personal material or content such as a faculty members' course material created and stored on SWIC's network.

Personally Identifiable Information (PII): As defined in Board Policy Statement 7017; sensitive Information collected for business purposes such as an Individual's Social Security Number or credit card information, when disclosed, could result in harm to the individual whose privacy has been breached.

Administrative Safeguards – administrative actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect the College's information assets and to manage the conduct of the college community in relation to the protection of those information assets.

Persons of Interest (POI): individuals who have a relationship with the College but with an affiliation other than employee or student. This may include, but not be limited to, contractors and individuals in partner organizations such as food service or bookstore.

Vendor: Outside parties who are contracted to provide products and/or services to the college.

Non-public personal information (NPI) –any personally identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available.

Gramm-Leach-Bliley Act (GLBA): The GLBA requires companies that qualify as "financial institutions" to take several affirmative steps in order to prevent the unauthorized collection, use, and disclosure of NPI. It imposes these obligations under two "Rules": (i) the Privacy Rule, and (ii) the Safeguards Rule.

3. Underlying Principles

a) The principles of academic freedom apply in full to electronic communications. The institution has adopted the academic freedom principles as articulated by the American Association of University Professors and has incorporated these into the faculty memorandum of understanding.
b) The use of computing, audio and video recording, data and network services provided by the College is subject to all applicable state and federal laws, as well as applicable College policies.
c) The definition of types of data includes, but is not limited to, voice, data and video that traverse SWIC's network infrastructure, that interface with the Internet, that interface with outside services, and that traverse between authorized external services and the SWIC Network.
d) All standards of behavior, courtesy, and etiquette that govern vocal and written communications also extend to electronic communications.
e) IT is responsible for the design, operation, and management of the computing and network communications services provided. When IT becomes aware of any use of SWIC's Network resources that violates provisions of College policy, presents a security risk, or degrades services to

others, IT may suspend or terminate network access and use and/or notify appropriate disciplinary and/or legal authorities. Where feasible, IT will provide prior notification of actions that affect network use and access. IT's responsibilities include, but are not limited to:

i.) The choice of protocols supported by the network,
ii.) The definition of technical standards necessary for efficient operation of the network and for the security of transmitted data and networked computers.
iii.) Delivery paths for network communications, including telecommunications lines, switches, hubs, routers, etc.
iv.) Institutional services utilizing network communications.
v.) Application of network management policies adopted by the institution to ensure inter-operability of department local area networks (LANs),
vi.) Monitoring the overall system to ensure the reliability, robustness and security of the College network infrastructure, and serving as the institutional representative to the Internet community, under the auspices of the Chief Information Officer, and ensuring that the College is a responsible member of that community.

4. Proper and Authorized Use of SWIC Network

IT is charged with ensuring the integrity of SWIC Network computers and communications. IT takes active steps to ensure the physical integrity of the infrastructure, including routine monitoring of performance and reliability. Units that provide access to the SWIC Network are responsible for ensuring that use is limited to legitimate users and is consistent with College policies and contractual obligations that govern the software and services offered on the SWIC Network. The use of SWIC Network resources is a privilege, not a right, which may be suspended or terminated by IT when, in its judgment, this policy has been violated by the user.

a) **Purpose of SWIC Network**: SWIC Network exists to support the educational and public service missions of the College, and its use should be limited to those purposes.
b) **Appropriate Use of SWIC Network**: All use of SWIC Network resources must be consistent with our public, educational status, and any use inconsistent with that status is prohibited. No individual may use SWIC's Network resources for commercial or profit-making purposes or other purposes unrelated to the mission of the College. As with all College computing and network facilities, the SWIC Network may not be used for improper or illegal purposes, such as unauthorized use of licensed software, intentional efforts to breach security, unauthorized audio or video recording, sending unauthorized mass mailing, or the transmission of computer viruses.

i) **Ownership of Network Identifiers**: College-supplied network identifiers (network IDs), College identification numbers, and computer-sign-ons (UserID's) are the property of the College. The College may revoke these identifiers or sign-ons at any time.
ii) **Responsibility to Maintain Privacy of Passwords**: Passwords, passcodes, or similar authentication information associated with an individual, an individual's network IDs or computer account shall not be shared without authorization.
iii) **Proper Identity Required**: Electronic mail and other forms of electronic communication must carry the proper identity of the sender at all times. Information servers (e.g., Web servers) must display the email address and identity of the unit or person responsible for maintaining the information.
iv) **Appropriate Use of Capacity**: Users of SWIC's Network must make reasonable efforts to use SWIC's Network resources in ways that do not unreasonably affect others. College units may set guidelines on capacity utilization within their unit for purposes of resource allocation.

v) **Appropriate Use of Online Services**: Internet services such as social networking, audio or video streaming, podcasting, etc. will be used primarily for instructional and institutional needs. Hosting of any Internet Services will be centralized within IT for proactive management. Activities associated with unauthorized hosting of social networking, peer-to-peer networks, video or audio streaming, podcasting, etc. will be suspended immediately upon discovery. If malicious activity is suspected, the appropriate legal, administrative, and Student Conduct processes will be followed.

vi) **Appropriate Use of Collaboration Platforms:** Only meeting organizers (e.g. professor or SWIC staff) will have the rights to record a collaboration session. All participants utilizing a collaboration platform must be informed that a session is being recorded.

vii) **Appropriate Use of the Employee Bulletin Board**: The electronic message board provided through the email system is a forum available for internal use for members of the College Community. Messages posted may include non-SWIC related notices of interest to the College Community, e.g. advertisements of items for sale.

viii) **Appropriate Use of VPN access**: The remote access granted is for official use only. Unauthorized or inappropriate use of this access is equivalent to unauthorized or inappropriate use of SWIC's Network resources which may result in disciplinary actions. Access is granted on a yearly renewal, is subjected to training compliance, and can be revoked at any time for non-compliance.

c) Use by Faculty, Staff, and Persons of Interest (POI)

i) **Passwords and College Units**: Faculty, staff, and POI including student employees, must not under any circumstances share their login ID and passwords with others, such as vendors, other employees, and supervisors.

ii) **Use Unrelated to College Positions**: Use by College employees and POIs unrelated to their College positions must be limited in both time and resources and must not interfere in any way with College functions or the employee's or POI's duties. It is the responsibility of employees to consult their supervisors if they have any questions in this respect.

iii) **Cyber Security Training:** GLBA Safeguard rule requires all College employees and POIs with access to the SWIC network comply with annual cyber security training. Failure to comply will result in suspension of access until such training is coordinated.

d) Use by Vendors: Vendors may not use SWIC's Network except as specified by written College contract. It is the responsibility of the vendor to ensure that their access of SWIC's network and data adhere to all general College policies; be familiar with various state and federal laws regarding privacy and security of confidential information maintained by the college; and to assure resources are provided in a secure manner.

i) **Vendor Risk Analysis**: In accordance with GLBA Safeguard Rule, all vendors with potential access to SWIC's data must submit HECVAT forms that will be used to perform a detailed risk assessment prior to engagement.

ii) **Account and password security:** Disclosure of any account information or passwords to anyone is prohibited. The use of any other account ID or password to access SWIC's resources is prohibited.

iii) **Appropriate Use of VPN access**: The remote access granted is for official use only. Unauthorized or inappropriate use of this access is equivalent to unauthorized or inappropriate use of SWIC's Network resources which may result in account termination.

e) Use by Students:

i) **Responsibility for Passwords**: Students must not share their passwords with others, even with friends. Students are responsible for ensuring that their computers are secure from unauthorized use. When working as employees, students are covered under section c) above.

ii) **Appropriate Use of Online Services**: Students will comply with institutional guidelines as published in Board Policy and in the Student Rights and Conduct statement.

f) Use by Non-College Users: Non-College individuals and organizations may not use SWIC's Network, except as specified by written College contract or that which is intended to be available to the general public, such as the Southwestern Illinois College web site. It is the responsibility of the contracting unit to ensure that content and usage of SWIC's Network adhere to all general College policies and that resources are provided in a secure manner. For purposes of this policy, a contracting organization shall be deemed to be a unit of the College, and designated officials of the organization may exercise the responsibilities of College administrators as described in this policy, except that the contracting organization may not exercise or supersede the authority of the Chief Information Officer

i) **Limited to College-related activities**: Legitimate non-College users may use their College provided accounts and Internet access only in conjunction with their authorized College-related activities.

ii) **Authorized Organizations**: SWIC Network resources may be used in support of organizations approved by the Chief Information Officer. While it is appropriate for the home pages of these organizations to provide some information about external organizations, clubs, commercial entities, etc. SWIC Network-connected equipment may not be the primary repository for that information.

iii) **College-sponsored External Entities**: Any College program that, in the interest of collaboration, wishes to provide an external entity with Internet access or to host non-College materials on a SWIC Network-connected server must first consult with IT about alternatives and secure approval from the Chief Information Officer.

5. Protection of Information in Electronic Media

5.1 Status of Information in Electronic Media

Information and data maintained in electronic media are protected by the same laws and policies, and are subject to the same limitations, as information and communications in other media. Confidential and sensitive PII information must remain secure from unauthorized access and may be flagged and audited during transmission for compliance. Before storing or releasing personal material (by email, in collaboration forums, or any other means); network users should understand that most materials on College systems are, by definition, public records. As such, they are subject to laws and policies that may compel the College to disclose them. The privacy of personal materials kept in electronic data storage and electronic mail is neither a right nor is it guaranteed.

5.2 Process for Requesting Disclosure of Contents of Messages and Files

Disclosure of contents of messages and files can be requested through the regular reporting channels to the Chief Information Officer or official request through FOIA. The Chief Information Officer or FOIA official(s) will carry out the responsibility for implementing this policy and ensuring that the scope of the disclosure is limited to a legitimate College purpose.

5.3 Review of Disclosure

SWIC Network users whose information is accessed or disclosed under the above provisions should use existing College complaint and/or grievance procedures when concerned about the application of this policy.

5.4 Portable Media Devices

Southwestern Illinois College confidential and sensitive PII data in electronic form must remain secure when it is stored or transported using portable media.

Portable electronic media is electronic storage that is designed to be easily portable for transport and use. Examples include, but are not limited to, laptop, tablets, flash drive (thumb drive, USB drive), Smartphone/iPhone, iPod, and CD/DVD.

The following provisions apply to Confidential and sensitive PII data in portable electronic media, and internal storage on portable devices:

a) The storage of confidential and sensitive PII data on Portable Media must be limited to that which is necessary for organizational purposes.

b) When Portable Media or a portable device is no longer needed, the confidential and sensitive PII data must be removed completely and made irrecoverable before either re-use or disposal of the media.

c) Southwestern Illinois College confidential and sensitive PII information may only be stored or handled using Southwestern Illinois College-owned devices and equipment or when using non-Southwestern Illinois College-owned devices that have been pre-approved for use and are configured and operated according to Southwestern Illinois College standards.

6. Responsibilities in Managing SWIC's Network

This section outlines responsibilities in managing SWIC's Network that may affect units and individuals.

a) **Network Design**: IT will work with any unit to develop or modify a network to meet unit needs. Needs directly related to the College's education or public service missions have first claim on resources.

7. Network Design

IT is responsible for the design or approval of departmental local area networks (LANs) that are connected to the campus network and their connections to the campus backbone. The following subsections document policies and procedures relevant to these areas. The term LAN as used here refers to the routers, switches, repeaters, cabling and patch panels, but excludes servers and other computers.

a) **SWIC Network Address Space**: Only IT-approved domains may be operated within SWIC Network address space. Publicly accessible Domain Name Servers must be approved by IT before they are placed in service.

b) **Responsibility for Telecommunications Wiring**: IT is responsible for the telecommunications wiring system on the College's campuses. If portions of this system are used in the construction of a LAN, all such use must conform to campus standards.

c) **Local Network Policies**: Network administrators and the owners of local networks may develop their own network policies, as long as they are not in conflict with College policies. Unit-level policies may not restrict access to campus services, except where specific security concerns require it, and may not contravene policies stated here.
d) **Responsibility of Units**: Units are responsible for the uses of their local area networks and servers. In particular, units are responsible for ensuring that materials published electronically or otherwise placed on their servers are relevant and appropriate to the unit's mission.
e) **Licensing and other Restrictions**: Some servers connected to SWIC Network provide services or software that are restricted by licensing agreements to use by College students, faculty and staff. Some licenses may further limit use to a specific campus or particular units. Servers must be configured such that restricted services or software are accessible only to those who are eligible.
f) **LAN Administrators**: Each LAN must have at least one designated administrator who is responsible for its administration and management, and whom IT may contact if it detects a problem.

8. Network Security

Each individual and unit has certain responsibilities to ensure that their systems are reasonably secure. This section describes security-related roles and responsibilities. It also describes circumstances under which SWIC Network user data can be collected and examined by the Information Security Manager or by an individual managing a LAN, server, or system.

a) **Responsibilities of Network Administrators**: It is the responsibility of every network administrator to have expertise sufficient to maintain appropriate levels of security and system integrity on local LANs. IT will document best practices and procedures for maintaining network security and integrity, in consultation with the campus community and peers nationally. IT provides training, consulting, and general support to network administrators.
b) **Ensuring Integrity of SWIC Network**: In the event that IT judges a LAN to present an immediate risk to the integrity of SWIC's Network equipment, software, or data, or presents a risk to the external network (resulting in potential liability for the College), IT may terminate or restrict the LAN's network connection without notice.
c) **Responsibility of the Information Security Manager:** It is responsibility of the Information Security Manager to analyze information security systems and applications, and to recommend and develop security measure to protect information against unauthorized access, modification, or loss. The Information Security Manager ensures authorized access by investigating improper access, reporting violations, and monitoring requests for new development.

9. Bandwidth Guidelines

SWIC Network and its connections to the Internet are a shared, finite resource. While every effort is made to provide adequate bandwidth for College purposes, bandwidth may not be available for every use.

a) **New Applications**: Extensive use of new applications that require very large amounts of bandwidth on the campus backbone must be discussed with IT beforehand, so that appropriate planning can take place.
b) **Degrading Network Performance**: If use of a computing or network service by a project or individual seriously degrades network service to others, IT will try to help the project or individual obtain the needed service in a way that does not seriously impact others. If a network upgrade is required, the unit or user may be asked to pay all or part of the cost.
c) **Responsibilities of Network Administrators**: Network administrators are responsible for monitoring and managing traffic on their LANs to protect the quality of service from adverse impact by users whose applications require substantial bandwidth or other network resources.

10. Website Usage

This section addresses issues specific to Southwestern Illinois College website usage and is related to: Commercial Advertising, Compliance, Copyright, Links, Logos and Other Trademarks, Nondiscrimination, Personal Business, and Web Accessibility. Institutional Web Pages include: all Web sites using the swic.edu domain (examples: swic.edu, fac.swic.edu, estorm.swic.edu, blackboard.swic.edu) external services (such as for social networking, collaboration platforms, blogging, micro-blogging), and all web pages representing Southwestern Illinois College to the community.

a) **Commercial Advertising**: Commercial advertising is only permitted on pages published on Southwestern Illinois College Web servers to the extent allowed by other policies. No graphic or text may imply Southwestern Illinois College endorsement of commercial products or services. A disclaimer should be displayed if non-endorsement is not evident from the context (see links- below.)

b) **Compliance**: All official Southwestern Illinois College Web pages that comply with College policies and guidelines will be eligible to display a seal or mark that certifies such compliance.

c) **Copyright**: Copyright laws apply to electronic publishing as well as to print publishing. Publishers must have permission from the copyright owners to copy and display text, graphics, or photographs on their pages. In the alternative, publishers must have a reasonable basis for believing their use of copyright materials of others constitutes fair use or that the materials are in public domain. Electronic publications are subject to the same Southwestern Illinois College policies and standards.

d) **Links**: Links from a Southwestern Illinois College page to any non-College site must not imply College endorsement of the site's products or services. A disclaimer should be displayed if non-endorsement is not evident from the context. Links that violate this policy must be deactivated.

e) **Logos and Other Trademarks**: The approved College logo must appear on the published entry page (home page) for all College related sites using the swic.edu domain (including intranet sites). For external services and all other web pages representing Southwestern Illinois College to the community, the approved logo may only be used or displayed with the approval of the Public Information and Marketing unit. All pages must also clearly communicate the name of the unit publishing the page. All representations of Southwestern Illinois College or campus names, logos, or other trademarks must conform to Southwestern Illinois College's Graphics Standards Manual.

f) **Nondiscrimination**: All Web pages must comply with the Southwestern Illinois College's Board Policy on nondiscrimination.

g) **Personal Business:** Southwestern Illinois College resources may be used to create Web pages about an individual or an individual's interests but may not be used to create Web pages for personal business, personal gain, or partisan political purposes, except as permitted by the College or by law.

h) **Web Accessibility**: Southwestern Illinois College is committed to making all its electronic information accessible in compliance with applicable state and federal laws and to following Southwestern Illinois College standards of Web Accessibility.