Link: SCC Policy and Procedures Main page

A-18 POLICY Use of Technology

Southeast Community College (SCC) recognizes the value of computer and other information technology resources to improve student learning, support the mission and vision of the College and enhance the administration and operation of the institution. To this end, the College expects the responsible and legal use of email; computers; computer networks, including the Internet**;** and other electronic information resources in support of the mission and goals of SCC. The Southeast Community College Use of Information Technology Policy**,** and its related procedures (A-18a), provides guidance for all individuals and groups that have, or may require, access to SCC's information resources.

Terms and Conditions of Use

- All users of SCC's electronic information resources and facilities must comply with the College's policies and procedures as detailed in the Student Handbook, the Employee Handbook, and the College catalog.
- The College provides information technology resources to be used as educational and/or work-related tools, including access to the Internet, servers, certain computer systems, software and databases.
- Users have a reasonable expectation of unobstructed use of IT tools and of protection from abuse and intrusion by others sharing these resources.
- Users are responsible for knowing the applicable regulations and procedures of the College and are responsible for exercising good judgment in the use of the College's technological and information resources.

Administrative Responsibility

The Vice President for Technology and designated staff are responsible for implementing, monitoring, and enforcing provisions of the College's Acceptable Use of Information Technology policy, and for developing procedures to ensure appropriate use of the College's information technology assets.

Related Procedure: A-18a
Adopted: 12/21/18
Reviewed: 2/05/18, 02/01/20, 12/12/23
Revised: 02/01/20
Web link:
Tags: access, technology access, acceptable use of technology

Table Of Contents

A-18a PROCEDURE Information Technology

Privacy:

Southeast Community College supports a climate of trust and respect and does not customarily read, monitor, or screen electronic information resources. However, complete confidentiality or privacy of data, email or other information transmitted or stored cannot be guaranteed for several reasons including; the nature of the medium, the need for authorized staff to maintain the systems, and the College's accountability as a publicly funded institution.

When appropriate and needed, the College President may authorize access in various circumstances including, but not limited to,

- situations involving the health or safety of people or property;
- possible violations of the Use of Information Technology policy or other College regulations or policies;
- possible violations of state or federal laws;
- subpoenas and court orders;
- other legal responsibilities or obligations of the College;
- when there is suspected activity that may be harmful to another user, to the campus systems and/or network, or,
- The need to locate, review, or secure information related to College business. Students should be aware that certain aspects of their privacy relating to academic records are governed by the Family Educational Rights and Privacy Act (FERPA).
- Details of FERPA are available on the SCC website: https://www.southeast.edu/consumer-information/
- A synopsis can also be found on the Department of Education website: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

User Responsibility and Account Ownership:

- Users shall not allow other individuals to access/share/use their SCC assigned network, email, or other College-based account information. Employees and students are individually responsible for the proper use of their assigned accounts, and are accountable for all activity associated with the account.

- Users are responsible for safeguarding their assigned accounts and are expected to take proper steps to ensure the integrity of their accounts. This includes, but is not limited to, setting up strong passwords, ensuring credentials are not saved or posted in a place accessible to others, making sure computers are properly locked or logged off when not in use, and by immediately reporting any notice of unauthorized access to the IT Helpdesk.

- Users are expected to support an educational environment free from harassment and discrimination as described in the Student Code of Conduct and the College Handbook.

- Users are expected to utilize technology in a manner that will not impede the College mission or the daily business of the College.

Table Of Contents

- Users are expected to access information that is needed in the context of the performance of their normal duties and to exercise good judgment in the use of such information; particularly, In particular, confidential or demographic data, which pertains to students, employees, and/or College operations.

- Users are expected to be knowledgeable of, and to perform their duties in compliance with, federal, state, and local laws and College policies, including the provisions of the Family Educational Rights and Privacy Act (FERPA) designed to protect the confidentiality of data and the privacy of individuals.

- Employees who supervise students, control electronic equipment, or otherwise have occasion to observe student use of Information Technology equipment shall make reasonable efforts to monitor the use of this equipment to ensure that it conforms to the mission and goals of SCC.

Use of College Resources:

SCC's Information Technology resources, including the network, are intended for the audience noted above and are to be used in the course of official work, study, and/or research. From time to time, SCC will make determinations on whether specific uses of the network are consistent with the acceptable use practice. Acceptable and unacceptable uses of SCC's Information Technology resources include, but are not limited to, the items outlined below.

Acceptable Use:

- Use of the Internet should be in support of educational and operational objectives consistent with the mission and objectives of Southeast Community College.
- Users should follow proper codes of conduct in electronic communication, including exhibiting exemplary behavior on the network as a representative of our institution.
- Individual credentials are to be used only by the user they are assigned to for authorized purposes and shall not be shared with others.
- All hardware that connects to the SCC network must be installed by an IT staff member.
- Users accessing the SCC network from a remote computer are expected to adhere to the same policies and procedures that apply to use from within SCC facilities.
- SCC's Information Technology resources are intended to be used for College-related business. Occasional and prudent personal use is permitted so long as it does not compromise the functioning of College network and computing resources, interfere with College operations, conflict or interfere with an employee's performance, interfere with the rights or reasonable expectations of another person, involve additional cost or expense to the College, violate any other College policy.

Unacceptable Use:

- SCC's network and resources shall not be used to threaten, harass, intimidate or degrade others. This includes, but is not limited to, electronically transmitting or reproducing materials that are slanderous, defamatory, or discriminatory in nature or that otherwise violate existing laws or Southeast Community College policies and mission.

Table Of Contents

- Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, neither should they share with nor allow other individuals to use their SCC-assigned network, email, or other College-based account information.

- SCC's network may not be used for commercial/for-profit purposes, product advertisement or political lobbying.

- Users shall not knowingly or carelessly perform an act that could interfere with the normal operation of computers, terminals, peripherals, or networks. This includes, but is not limited to, downloading excessive amounts, transferring excessive amounts across the network, propagating viruses or worms, using the campus network to gain unauthorized access to any computer system, or attempting to circumvent data protection schemes or uncover security loopholes.

- Users shall not install any software, including shareware and freeware, for use on SCC's computers without prior review and authorization from appropriate IT staff.

- SCC's network and resources may not be used for downloading entertainment software or other files not related to the mission and objectives of SCC for transfer to a user's home computer, personal computer, or other media. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, exchanging digital copies of music files, and all other forms of software and files not directly related to the instructional and administrative purposes of SCC.

- SCC's network and resources may not be used for downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC).

- Use of SCC's network for any unlawful purpose is prohibited including, but not limited to, gambling, pornography, sharing explicit sexual content, cyberbullying or fraud.

Additional Policies:

In addition to the guidelines listed in this document, Southeast Community College and its employees are required to comply with other laws, policies, procedures, and guidelines. The following are examples, but not a complete list, of some of the other relevant laws, agreements, and policies:

- Family Educational Rights and Privacy Act (FERPA)
- Payment Card Industry Data Security Standards (PCI-DSS)
- Red Flag Rule - Identity Theft Prevention Program PM X-30
- Health Information (HIPPA)
- Gramm-Leach-Bliley ACT
- Nebraska Data-Security Law

Table Of Contents

Related Policy: A-18
Adopted: 12/29/99
Reviewed: 3/17/09, 12/12/23
Revised: 3/17/09, 12/18/18
Web link: TBD
Tags: IT, Information Technology, Technology, Password, Computer Systems

Table Of Contents

A-18b PROCEDURE Cyber Security

Objective:
Reduce the College's risk of a data breach and other cybercrimes through education and awareness. Protect PII and other sensitive information contained within College systems as implemented by the Information Services division.

Activation:
SCC Employees have the following requirements on an annual basis:

1. Regular and temporary employees with an FTE factor equal to or greater than 0.75 must complete one cyber security awareness training per fiscal year. If needed, individuals will be provided with additional training immediately following a failed phishing test.

2. Individuals requesting access to the SCC network via VPN access will complete cyber security training and be enrolled in the SCC Multi-factor authentication group.

3. Part-time regular employees, with an FTE status of less than 0.75, must complete one cyber security awareness training per fiscal year.

4. Part-time temporary employees with an FTE status of less than 0.75, including adjunct, are invited and encouraged to complete one cyber security awareness training per fiscal year.

The following job roles are required to have multi-factor authentication:

- All users on the Administrative team
- All users with VPN access
- All users with Colleague NAE access
- All users with access to Financial or Financial Aid data
- All users with access to HR/personnel data

In situations where an employee has interacted with a real phishing scam or other cybercrime incident (not a training exercise), the Information Services team will:

1. Reset the individual's password to prevent unknown entities from logging into the SCC network.

2. Automatically enroll the individual in additional cyber security awareness trainings that must be completed within 7 days of enrollment.

3. If the individual has VPN access, that access will be temporarily deactivated until the additional training is completed.

4. If the individual is not enrolled in SCC's Multi-factor authentication group, they will be required to set up multi-factor authentication to help prevent potential future login attempts from unknown entities.

Table Of Contents

The Information Services division will track the completion of all cyber security education and protocol.

Related Policy/Procedure: A-18, A-18a
Adopted: 1/27/20
Reviewed: 12/12/23
Revised:
Web link:
Tags: cyber security, cyber security education, multi-factor authentication

Table Of Contents