

POLICY TITLE: **Computer Resources, Network Use, and Computer and Network Security** 3.11
RESPONSIBLE DIVISION: Information Technology & Telecommunications Page 1 of 3
DATE APPROVED/SIGNATURE: January 2006

1. The computer and network resources owned and operated by Southwestern Community College are intended for the use of its students, employees, and other authorized individuals for purposes related to instruction, learning, research, and administrative operations. Authorized individuals who use the computer network must take all appropriate actions to properly use the equipment and protect the security of associated data and electronic records.
2. Security refers to the protection of computer resources from accidental or intentional disclosure, modification, or destruction. The College's Information Technology (IT) and Telecommunications Department strives to maintain the highest level of network security to protect the integrity of all files, electronic records and student and financial databases. Southwestern Community College abides by the guidelines and policies of the NC Information Resource Management Commission (IRMC).
3. All college employees, requesting access to the College's network and to the financial and student databases, must complete and sign an Information Technology Services User Authorization Form indicating they understand and comply with the terms and conditions in accordance with college policies related to computer resources, network use, and computer and network security.
4. Access to all college information databases is based on an individual's job responsibilities and access requirements related to the position. Only minimum access rights, necessary for the performance of assigned duties, will be granted.
5. User access will be reviewed periodically and internal audits will be performed to guard against unauthorized access and security violations.
6. Violations of computer security and improper use will not be allowed and must be reported to the Computer Operations staff or College Administration. Violations include, but not limited to the following:
 - a. Deliberately downloading, uploading, creating, or transmitting computer viruses.
 - b. Destroying or modifying directory structures or registries; or interfering or tampering with another user's data or files.
 - c. Developing programs that infiltrate or negatively impact the performance of a computer or network operations.
 - d. Attempting to obtain unauthorized computer access or network privileges, or attempting to access the files of another user.

POLICY TITLE: Computer Resources, Network Use, and Computer and Network Security 3.11
RESPONSIBLE DIVISION: Information Technology & Telecommunications Page 2 of 3
DATE APPROVED/SIGNATURE: January 2006

- e. Using hardware or software “sniffers” to examine network traffic, except by appropriate College personnel to diagnose the network for bottlenecks or other problems.
- f. Using another person’s password or sharing of one’s own password; users who choose to share their passwords are responsible for the outcomes resulting from the use of their account login and password information.
- g. Committing any form of vandalism on computers, network or telecommunications equipment, software, or attempting to defeat or circumvent any security measures or controls.
- h. Where unauthorized, consuming food or beverages in computer labs, computer classrooms, or in any other areas restricted for the protection of computer or network equipment.
- i. Wastefully using finite resources, such as large amounts of bandwidth for extended periods of time.
- j. Connecting unsanctioned products (software or hardware) to the College network, or installing products for personal use – other than laptop computers using wireless connections or network connections intended specifically for public access.
- k. Using chat rooms or Instant Messaging, other than in support of the research, educational, and administrative purposes of the College.
- l. Sending hate or threatening email, chain letters, and anonymous or pseudonymous messages – note: email policies are specified in College policy 3.37
- m. Viewing, copying, or distributing obscene, pornographic or lewd content that might be offensive to others.
- n. Using College computer resources for political campaigns or the distribution of political material.
- o. Using College computer resources for fraud, financial gain, or for any commercial or illegal activity.
- p. Disclosing student information in violation of the provisions of the federal statute known as the Family Educational Rights and Privacy Act of 1974.
- q. Violating copyright laws and/or fair use provisions by downloading or uploading pirated or illegal material, including, but not limited to, software and music files; inappropriately reproducing or disseminating Internet materials, except as permitted by law or by written agreement with the owner of the copyright.

POLICY TITLE: Computer Resources, Network Use, and Computer and Network Security 3.11
RESPONSIBLE DIVISION: Information Technology & Telecommunications Page 3 of 3
DATE APPROVED/SIGNATURE: January 2006

7. All electronics connecting the Colleges network(s) to the Internet and other outside networks will be configured with filters and access controls to prevent security breaches.
8. Wireless connectivity to the College's network will be configured using separate "Internet only" VLANs or connected by use of authentication protocols and servers to enforce access measures that only allow wireless connections from permitted computer devices.
9. All College web servers will be located on a publicly reachable network segment separated from the internal network by a DMZ firewall.
10. College firewalls will be configured to use network address translation (NAT) to hide internal IP addresses.
11. All file and application servers are to be constantly updated with the latest releases and services patches.
12. Remote access to the College network is permitted through dial-up connections using secure IP addresses over VLANs.
13. High speed remote access to the College network is available through encrypted virtual private network (VPN) connectivity.

Reservation of Rights and Limits of Liability

1. Southwestern Community College reserves all rights in the use and operation of its computer resources, including the right to monitor and inspect computerized files or to terminate service at any time and for any reason without notice.
2. The College makes no guarantees or representations, either explicit or implied, that user files and/or accounts are private and secure. No right of privacy exists in regard to e-mail or Internet usage.
3. The College is not responsible for the accuracy, content, or quality of information obtained through or stored on the College network.
4. The College reserves the right to limit the allocation of computer resources.
5. The College makes every effort to maintain computer resources in good working condition but is not liable for damages incurred by loss of service.
6. The College is not liable, legally, financially, or otherwise, for the actions of anyone connecting to the Internet through the College network(s).