The school system computers, networks, and other technological resources support the educational and administrative functions of the school system. Because employees and students depend on these systems to assist with teaching and learning and because sensitive and confidential information may be stored on these systems, system integrity and security is of utmost importance.

A. NETWORK AND INFORMATION SECURITY

The school system information technology systems are valuable assets that must be protected. To this end, school technology personnel shall evaluate each information technology asset and assign protective controls that are commensurate with the established value of such assets. Appropriate security measures must be in place to protect all information technology assets from accidental or unauthorized use, theft, modification, or destruction, and to prevent the unauthorized disclosure of restricted information. Network security measures must include an information technology system disaster recovery process. Audits of security measures must be conducted annually.

All personnel shall ensure the protection and security of information technology assets that are under their control.

B. SECURITY AWARENESS

The technology director or designee shall provide employees with information to enhance awareness regarding technology security threats and to educate them about appropriate safeguards, network security, and information security.

C. MALWARE PROTECTION

Malware detection programs and practices must be implemented throughout the school system. The superintendent or designee is responsible for ensuring that the school system network includes current software to prevent the introduction or propagation of computer malware.

D. TRAINING FOR USE OF TECHNOLOGICAL RESOURCES

Users should be trained as necessary to use technological resources effectively and in a manner that maintains the security of the network infrastructure and ensures compliance with state and federal law and regulations. Such training should include information related to remote access, virus protection, the state student information and instructional improvement system applications, network and information security, and other topics deemed necessary by the superintendent or technology director. Training may be conducted as part of the technology-related professional development program (see policy 3220, Technology in the Educational Program).

E. ACCESS TO INFORMATION TECHNOLOGY SYSTEMS

Access to the school system's information technology assets will be controlled and managed to ensure that only authorized devices/persons have access.

1. User ID and Password

   All users of information technology systems must be properly identified and authenticated before being allowed to access such systems. The combination of a unique user identification and a valid password is the minimum requirement for granting access to information technology systems. Depending on the operating environment, information involved, and exposure risks, additional or more stringent security practices may be required as determined by the superintendent or technology director. The technology director or designee shall establish password management capabilities and procedures to ensure the security of passwords.

2. Student Information System

   The technology director or designee shall ensure that all school system computers with access to the state student information system application pursuant to State Board of Education Policy TCS-C-018 adhere to relevant standards and requirements established by the State Board of Education, including provisions related to user identification, and password and workstation security standards. Employees must follow all such standards when using any computer to access the student information system, including when using the employee's personal computer.

3. Remote Access

   The superintendent and technology director may grant remote access to authorized users of the school system's computer systems. The technology director or designee shall ensure that such access is provided through secure, authenticated, and carefully managed access methods.

Legal References: G.S. 115C-523, -524; State Board of Education Policy SBOP-018

Cross References: Professional and Staff Development (policy 1610/7800), Technology in the Educational Program (policy 3220), Technology Responsible Use (policy 3225/4312/7320), Internet Safety (policy 3226/4205), School Improvement Plan (policy 3430), Use of Equipment, Materials, and Supplies (policy 6520)

Other References: *State of North Carolina Statewide Information Security Manual* (Enterprise Security and Risk Management Office), available at http://it.nc.gov/document/statewide-information-security-manual

Adopted: January 20, 2009

Revised: June 30, 2009; August 29, 2012, December 12, 2013, March 12, 2015, February 9, 2017, October 5, 2017