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. Evaluation 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 / VIRUS PROTECTION

Malware / Virus 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 SBOP-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, technology director, or technology director's designee 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.

4. Wireless Network Access

   Personal wireless devices may use the district's internet resources during school hours and school functions by connecting to the designated BYOD or Public wireless networks. Connecting personal wireless devices to any other wireless network is strictly prohibited. Use of personal wireless hotspots or any other network that bypasses the district's internet filter is strictly prohibited.

F. Advertising and Commercialism

The use of district technology resources or the Internet for one's own commercial gain or profit is not allowed from within the district network. This includes but is not limited to using the district email system to send email advertisements for personal businesses or solicitations.

G. Disaster Recovery of Data and Hardware

The purpose of the procedures and practices listed below is to provide for the continuity, restoration, and recovery of critical data and systems and to ensure timely restoration of data and services in the event of a disaster.

Data Backup

- Critical data will be backed up periodically with multiple copies maintained.
- Server operating system recovery information and data will be backed up on a regular basis to ensure timely recovery from hardware failures.

Risk Reduction

- Critical system hardware will use redundant component where possible.
- Critical servers and hardware will operate from UPS battery backup systems.
- Critical servers will be operated in a high availability mode with totally redundant hardware.
- The Central Data Center for the district will be setup and maintained in accordance with industry best practice standards.

H. Hardware and Software Procurement

The director of technology or designee shall obtain the most cost effective and reliable technology equipment and software and is responsible for establishing standards to ensure smooth and efficient operations. Technology includes computing devices, software, peripherals, telephones, and any other device that utilizes the district network.

All technology acquisitions – whether purchased or acquired via other means – must be reviewed and approved prior to acquisition by the director of technology or designee to ensure compatibility with existing network architecture and with software licensing restrictions. Any technologies that are acquired without prior approval by the director of technology or designee may be denied access to the district network and/or installation on district computing equipment.

I. Hardware and Software Installation and Maintenance

The Technology Department will develop and maintain a process for in-house

installations, maintenance, and repairs and is solely responsible for installations, maintenance, and repairs of technology equipment at all locations. Alteration of district networking equipment, computing hardware and/or installed software by non-technology department personnel is prohibited without prior approval by the director of technology or designee. Installation of personal network and/or computing equipment is strictly prohibited without prior approval from the director of technology or designee.

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: June, 28, 2017

Revised: September 25, 2017 *(technical corrections only)*