~~Information technology (“IT”) systems owned and/or operated by the Transylvania County Board of Education (the “Board”) support the educational and administrative functions of the school district and include computers, networks, and other technological resources. 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, IT integrity and security are of utmost importance.~~

~~A. Network And Information Security~~

~~The school district’s IT systems are valuable assets that must be protected. To this end, IT personnel shall evaluate each IT 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 IT 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 IT system disaster recovery process. Audits of security measures must be conducted annually.~~

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

~~B. Security Awareness~~

~~The Superintendent 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. Virus Protection~~

~~Virus detection programs and practices must be implemented throughout the school district. The Superintendent or designee is responsible for ensuring that the school district network includes current software to prevent the introduction or propagation of computer viruses.~~

~~D. Training for Use of Technological Resources~~

~~Users should be trained as necessary to effectively use technological resources. Such training should include information related to remote access, virus protection, the student information sysem, network and information security, and other topics deemed necessary by the Superintendent or designee. Each school should identify any staff development appropriations for technological training in its school improvement plan. The Superintendent or designee should assist schools in coordinating staff development needs.~~

~~E. ACCESS TO INFORMATION TECHNOLOGY SYSTEMS~~

~~1. **User ID and Password**~~

~~All users of IT 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 IT 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 designee. The Superintendent or designee shall establish password management capabilities and procedures to ensure the security of passwords.~~

~~2. **The Student Information System**~~

~~The Superintendent or designee shall ensure that any school district computers utilizing the student information system pursuant to State Board of Education policy adhere to applicable security requirements, including those related to user identification, password, and workstation security standards. Employees must follow such standards for all computers used to access the student information system, including the employee's personal computer.~~

~~3. **Remote Access**~~

~~The Superintendent or designee may grant remote access to authorized users of the school district's IT systems and shall ensure that such access is provided through secure, authenticated, and carefully managed access methods.~~

~~Legal References: N. C. Gen. Stat. § 115C-523, -524; State Board of Education Policy TCS-C-018~~

~~APPROVED BY BOARD~~
~~AND EFFECTIVE 10/17/05~~
~~REVISED 6/18/12~~