~~CONFIDENTIALITY OF ELECTRONIC INFORMATION/ SECURITY AWARENESS~~
NETWORK SECURITY

FILE: IIBGA

~~With the increased utilization of technology and networked software to provide access to important information, it becomes increasingly important that all users understand the role they play in protecting the confidentiality of information. Whether information is accessed locally from a single workstation, a network server or over a dedicated Internet circuit, each user has significant responsibility to safeguard that data. Users must be cognizant of their personal responsibility in safeguarding confidential school system information.~~

~~**Anti-Virus Protection**~~

~~Electronic devices shall use approved anti-virus programs for protection of all hardware, software and downloaded information.~~

~~**Employee Access to Data**~~

~~Employees shall be given access (assignment of network user ID and password) to confidential data only after reading and signing the *Acceptable Use Policy agreement form*. It shall be the responsibility of each employee's supervisor to verify that each individual accessing information is properly trained and aware of the responsibilities for maintaining confidentiality.~~

~~Employees should save confidential data to their home directories on network servers rather than workstation hard-drives. Data saved to the network is protected by anti-virus software and other electronic devices. Workstation hard-drives may not be backed up properly and are far more susceptible to viruses, spyware, and adware problems than are network servers. Workstations are not generally protected from electrical surges and spikes that can damage hard-drives. Data saved to a network server is far more secure than data saved to a workstation.~~

~~**Authentication**~~

~~All users must authenticate to programs before being allowed access to systems containing confidential data. The combination of a unique user ID and a valid password is the minimum requirement for granting access to an information system. A unique user ID must be assigned for each employee so that individual accountability can be established for all system activities. Inactive user IDs arising from employee or contractor movements will be removed/disabled preventing further access to confidential information. The authentication system shall limit unsuccessful logon attempts. Password management capabilities and procedures are established to ensure secrecy of passwords and prevent exploitations of easily guessed passwords or weaknesses arising from long-life passwords.~~

~~Transylvania County Schools adheres to State Board Policy EEO-C-018 and procedures regarding authorized use and access to the student information records system.~~

~~**Remote Access**~~

~~Electronic systems and software applications may be remotely accessible today from any source capable of Internet access. Users of such systems should take every precaution to prevent compromising confidential data. Such precautions include security of the actual device used for access. Devices used to access these systems should have the latest anti-virus software/definition files installed along with controls for adware and spyware in place.~~

~~**File Transfer of Electronic Information**~~

~~Employees shall not transfer confidential data electronically over an Internet circuit without using appropriate encryption technologies. Appropriate encryption technologies shall be specified by the Director of Technology.~~

~~**Audit Technology**~~

~~*Purpose* -To provide the authority for members of Transylvania County Schools Information Technology Staff to conduct a security audit on any system at Transylvania County Schools.~~

~~Audits may be conducted to:~~

- ~~Ensure integrity, confidentiality and availability of information and resources~~
- ~~Investigate possible security incidents to ensure conformance to Transylvania County Schools security procedures~~
- ~~Monitor user or system activity where appropriate~~

~~*Scope* - This policy covers all computer and communication devices owned or operated by Transylvania County Schools. This policy also covers any computers or communications devices that are present on Transylvania County Schools premises, but which may not be owned or operated by Transylvania County Schools.~~

~~*Policy* - When requested, and for the purpose of performing an audit, access to needed equipment/services will be required.~~

~~This access may include:~~

- ~~User level and/or system level access to any computing or communications device~~
- ~~Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on Transylvania County Schools equipment or premises~~
- ~~Access to work areas (labs, offices, cubicles, storage areas, etc.)~~
- ~~Access to interactively monitor and log traffic on Transylvania County Schools networks~~

~~*Enforcement* - Any employee found to have violated this policy may be subject to disciplinary action.~~

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 ____________