Career Center of Southern Illinois
6137 Beck Road Red Bud, IL 62278 (618) 473-2222 · Fax (618) 473-2292 · www.gotoccsi.org
Stephanie Mohr, Director · Mitch North, Principal/Asst. Director · Holly Szopinski, Nursing Director

CCSI/ BECK Network Security Plan

I. Purpose

The purpose of this plan is to ensure the secure use of school data information, computer, and network equipment that is utilized by the programs at Career Center of Southern Illinois staff and students. This plan shall be reviewed annually in cooperation with IT Support Contractor.

II. Security Responsibility
   a. The Director of Career Center of Southern Illinois is responsible for over-seeing Campus-wide security management.
   b. Career Center of Southern Illinois contracts with an IT firm to monitor the networks firewall, server activity, and network equipment.

III. Training
   a. Staff of Career Center of Southern Illinois will undergo cybersecurity training focused on cybersecurity threats and the protection of student data.
   b. Students will receive training on the appropriate use of technology policies.

IV. Physical Security
   a. Computers should not be left unattended or unlocked, especially when logged into sensitive systems or data including student or employee information.
   b. The server shall be stored in a locked cabinet, keys to the server cabinet are in the possession of administration only and are only accessed during times of network, server, or back up maintenance.
   c. Contractor access to the systems or servers is to be monitored by an administrator/ technology coordinator.

V. Network Security
   a. Network controls will be implemented to regulate traffic moving between trusted resources and external, untrusted entities. All network transmission of sensitive data shall be encrypted when feasible.
   b. Firewall and technical infrastructure are monitored by IT contractor.
   c. Server is back up to an external hard drive located on campus and is backed up on a cloud-based server managed by IT contractor.
   d. Wireless Access Points
      i. All wireless access points shall conform with the network standards, no wireless access point shall be installed without the permission of the Technology Coordinator.

VI. Access Control
   a. System and application access will be granted based upon the least amount of access to data and programs required by the user, in accordance with a business need-to-have requirement.
   b. Authentication
      i. CCSI shall enforce use of passwords for employees, students, and contractors
      ii. All passwords shall conform to password guidelines established by Tech Coordinator
      iii. Passwords are to be treated as sensitive and confidential information
      iv. Passwords shall not be inserted into email messages or other forms of electronic communication
      v. Passwords shall not be revealed over the phone or shared on forms

vi. Any user who suspects their password has been compromised must report the incident and must change all passwords

VII. Remote access
   a. Remote Access may only be implemented on devices as approved by the Technology Coordinator and/ or Administration.
   b. Remote Access required multifactor authentication, with specific password requirements, not to be shared.

VIII. Incident Management
   a. Monitoring and responding to incidents will be addressed promptly in order to response to internal or external system attacks as early as possible.

IX. Internet Content Filtering
   a. CCSI shall filter internet traffic for content that may be harmful to minors, in accordance with State and Federal Law.
   b. Internet filters are not always effective at eliminating harmful internet content, other steps may need to be taken to protect students from harmful online content.
   c. Students will be supervised when accessing the internet and using school owned devices when on school property.

X. Data Privacy
   a. CCSI considers the protection of personal data of students, employees, and employee families of the upmost importance.
   b. CCSI will conform to with all state and federal privacy and data laws.

XI. Disciplinary Actions
   a. Any employee found to be in violation of policy may be subject to disciplinary action up to and including termination or employment with Career Center of Southern Illinois.