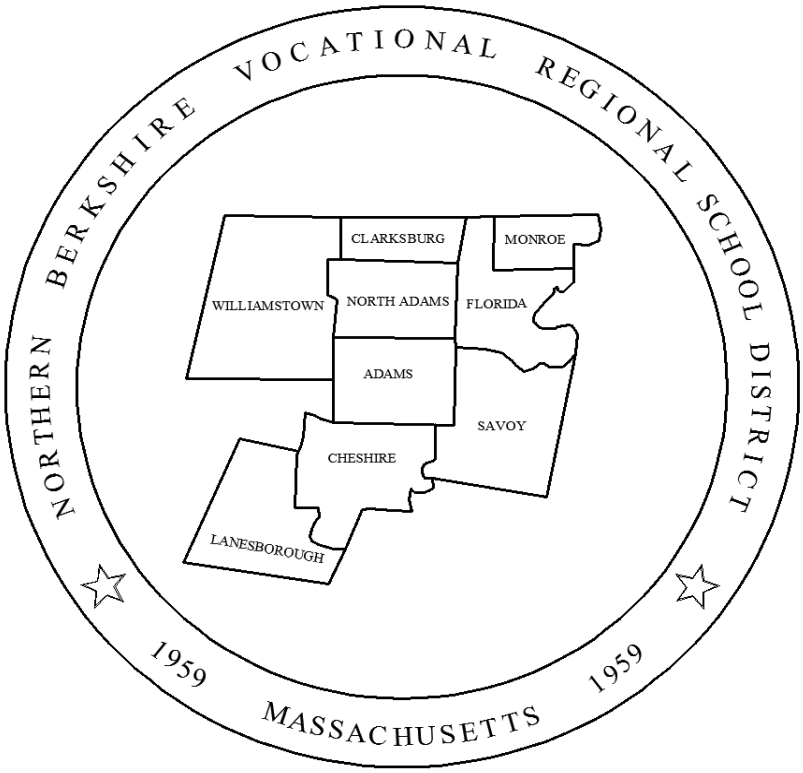
Northern Berkshire Vocational Regional School District

McCann Technical School



Cybersecurity Plan

2021-2024

The McCann Technical School community believes that effective use of technology is essential for all students to improve student learning, increase achievement, and prepare students for employment in the modem workplace.

Essential tasks in this application is the training of all staff and students in proper use and safeguarding of information and the ability to recognize, react and communicate suspicious activity to our IT personnel and administrators. This cybersecurity plan outlines a process for protecting our systems, our information and training students and staff in cybersecurity methods and practice. We routinely incorporate changes to our security profiles as directed by our contracted service providers and security software professionals. Our information technology instructors also serve as our IT operational and security team.

NETWORK/INTERNET SECURITY

The school network is part of the McCanntech.org domain where users must be authenticated before they can access the computers or files contained within the network. Authenticated users must provide a username and password in order to access either the school computers or the files contained on the school network.

Physical access to the network is restricted. All servers and networking equipment are secured in either dedicated rooms or cabinets with restricted access. Access to the wired network is accomplished using port-security to prevent users from swapping out school computers for their own, and any unused wired ports are disabled/shutdown when not in use. Access to the school wireless network is restricted using either certificates and/or authentication. Guest network access on the wireless also secured, with no access to the internal network. Outside access to the network is protected by a SonicWall Firewall/IDS/IPS system. Remote access to the network is currently not allowed beyond the DMZ.

All sensitive files are stored on our internal servers where applicable such as financial and personnel files. Access to all files on the network are restricted by user and/or position/title as set forth by files permissions. All servers are backed up nightly to a dedicated server, with a copy of the backups stored offline. Email is provided by Google Educational Suite; all backups of the system are handled by them.

All computers on the internal network are protected with both Antivirus and Antimalware software provided by ESET that is updated daily. Software updates, patches, and upgrades are installed regularly as they become available

All computer data drives are destroyed upon equipment replacement or failure.

IT RESPONSIBILITIES

Our IT department will:

1. Ensure all operating system and application software updates and patches are promptly installed.
2. Conduct routine inspections of our systems for anomalies on a daily basis.
3. Safeguard and back up our financial data on a daily basis.
4. Install encrypted software when necessary.
5. Monitor both external and internal email and infrastructure transactions.
6. Provide security passwords for our internal Wi-Fi network.
7. Implement all software updates and changes as required of our providers and other governmental organizations.
8. Provide recommendations for security protocols or systems to the administration.
9. Maintain all servers and information back-up systems.
10. Develop and provide staff/student training in the proper use of systems and of safeguarding information.

CYBERSECURITY TRAINING

All staff will receive updated computer cybersecurity training at the beginning of each school year to include such topics as:

- Reasons for Data Protection:
  - Information Theft
  - Identify Theft
  - Data Manipulation
  - Data Destruction
  - Social Engineering
  - Phishing Attacks
  - Scareware
  - Spyware and Adware
  - Keyloggers
- Changes in cybersecurity protocols or information on recent attacks that may cause reasons of concern, will be sent to staff periodically throughout the school year as received or as necessary.
- Students receive computer, network, **Wi-Fi** and cybersecurity training at the beginning of the school year.
- All employees, staff, and students must sign an acceptable use policy.