Path to Cyber Insurability

1 Control #1: Multifactor Authentication (MFA)

The use of more than one authentication method to confirm a user is who they say they are. MFA should be utilized for all remote access, privileged accounts, password changes, and email access on non-owned/non-managed devices.

2 Control #2: Backups

The process utilized to create and properly store/secure copies of district or community college data to prevent or minimize data loss in the event of a cyber attack or disaster. Utilize 3-2-1 rule - maintain 3 copies of data, on 2 different storage types, and at least 1 off site.

3 Control #3: Cyber Incident Disaster Recovery | Incidence Response Plan

Documentation that shows the predetermined set of instructions and procedures to detect, respond to, and limit the impact of a cyber event or disaster.

4 Control #4: Endpoint Detection and Response (EDR)

Monitors end-user devices to detect and respond to cyber threats like ransomware and malware. Example could be notification when devices are used at unusual times, or performing unusual activities.

5 Control #5: Training and Planning

An audited written plan for patching critical software and hardware. Employee cybersecurity training, including phishing simulations. Segregation of end-of-life software and hardware from the network, and decommission in a timely fashion.

6 Control #6: Secure Email Filter and Configurations

Use protocols that protect email and/or email servers from outside interference by attackers.

7 Control #7: Privileged Access Account Security Measures

Staff should only have access and permissions needed to perform their tasks and nothing more.

Learn More

SCAN ME