Murfreesboro City Schools

ADMINISTRATIVE DIRECTIVE

Administrative Directive Title: **School Cybersecurity Preparedness**	AD Number: **3.205.1**	Adopted: November 2024
Policy References: Board Policy 3.205 – Security	Revised:	

Cybersecurity is defined as the process of protecting information by preventing, detecting and responding to unauthorized access of confidential or safety sensitive information.

The Technology Supervisor is responsible for the implementation of school cybersecurity procedures, including:

1. The implementation of training on "cyber hygiene" including, recognizing and reporting phishing attempts, using strong passwords, requiring multifactor authentication, and keeping software updated;
2. Establish and exercise a cyber incident response plan outlining what should be done before, during, and after a cyber incident;
3. Implement well-informed processes when new technologies are adopted within the school environment;
4. Stay informed on the cyber risk environment and connect with K-12 cyber partners who can help provide strategic and cost-efficient cybersecurity actions;
5. Invest in impactful security measures.

DATA BREACH RESPONSE

The Technology Supervisor will be responsible for developing a plan in the event that a cybersecurity threat or incident occurs. The plan shall include the following:

1. Validate that the data breach occurred;
2. Investigate the breach;
3. Assemble an incident response team to begin mitigation efforts;
4. Notify the parties effected by the breach;
5. Determine whether to notify law enforcement or other regulatory agencies;
6. Assess the data breach to determine the cause as well as ways to minimize future risks.

When applicable, the plan shall be implemented in a prompt manner to minimize the risk of any further data loss as well as to mitigate any negative consequences of the breach.

Legal References
TCA 49-6-4217