STATE OF ALABAMA
DEPARTMENT OF EDUCATION

Eric G. Mackey, Ed.D.
State Superintendent of Education

September 8, 2023

M E M O R A N D U M

TO: City and County Superintendents of Education

FROM: Eric G. Mackey
State Superintendent of Education

RE: Cybersecurity Measures for Local Education Agencies (LEAs)

Cybersecurity measures are necessary to protect school systems from escalating threats of ransomware, data theft, and financial crimes. These measures are crucial to prevent interruptions to school operations, permanent loss of personal data, theft of funds, and the expensive, unbudgeted recovery costs associated with such incidents. To help safeguard each school system against these damaging crimes, it is imperative that each LEA complies with the following requirements:

1. Cyber Awareness Training
2. Cybersecurity Incident Response Plan Development
3. Multi-Factor Authentication (MFA)

First, because phishing emails continue to be a leading point of entry for ransomware and other forms of cybercrime, it is essential that all employees are informed and trained to recognize and appropriately respond to phishing emails. To facilitate cyber awareness training, each LEA will use the cybersecurity awareness software provided to them by the state to complete the following:

1. Require a minimum of one training per year for all employees* with district email accounts. Current employees shall complete the assigned training within the first 60 days of the school year, and employees added after the beginning of the school year shall be assigned and complete training within the first 30 days of employment.

   *Bus drivers and other employees with little or no access to the district network may be excluded from the required training, if necessary.

2. Assign all employees with an email address one phishing test monthly throughout the calendar year. Provide additional training opportunities for employees based on phishing test results.

3. Provide monthly reports for both training completion and phishing tests to the LEA superintendent or designee.

4. Maintain required records and reports on both phishing and training as part of the annual cybersecurity funding application or comprehensive monitoring.

System technology coordinators may email support@AL-K12-cyber.org for assistance with using the software and for a list of recommended training modules and phishing tests.

Next, given the unpredictable nature of cyber incidents, it is vital that school districts are well-prepared to respond promptly and effectively. To facilitate this preparedness, all school systems are required to develop a Cybersecurity Incident Response Plan. The Cybersecurity Incident Response Plan is a written document that helps organizations before, during, and after a confirmed or suspected security incident. This plan clarifies roles and responsibilities and provides guidance on key activities. Beginning with the 2023-2024 school year, the following is required:

1. All LEAs shall develop a Cybersecurity Incident Response Plan by **April 5, 2024**.

2. The Cybersecurity Incident Response Plan shall follow the required format, guidelines, and components that will be provided in a separate correspondence.

3. A team consisting of the superintendent, technology coordinator, applicable technical staff, human resource director, chief school financial officer, and communications director shall work collaboratively to develop the plan.

4. The plan shall be reviewed quarterly and updated, as needed, to stay current with emerging threats, protection measures, available resources, and other factors.

The incident response plan training will be provided in five locations throughout the state. Each LEA should send a minimum of one representative to the training. Stipends to assist with travel expenses will be considered. Participants are encouraged to attend the training in the closest proximity to the district. The LEAs that already have a Cybersecurity Incident Response Plan should plan to attend one of the trainings to ensure alignment and compliance with the requirements and collaborate with other LEAs. More information regarding the specific dates and locations will be emailed to technology coordinators and superintendents in the near future.

Finally, cybercriminals often conduct their crimes by compromising user accounts with elevated access to software applications and technology infrastructure. These include accounts used by network administrators, accounting staff, district-level data staff, human resource staff, some contractors, and others. To mitigate the risk of unauthorized access to such accounts, school systems must implement additional security measures. In addition to other protection and prevention measures, school systems must protect data and infrastructure from unauthorized user access by implementing at least one additional security measure in addition to a username and strong password. This can include traditional two-factor authentication, also known as MFA, or another method. Specific requirements related to the MFA will be provided to technology coordinators in a separate correspondence.

Implementing all the above requirements will contribute significantly to enhancing the cybersecurity posture of Alabama school systems, thereby helping to safeguard valuable data and resources from potential threats. Your cooperation and prompt action in implementing these measures are greatly appreciated.

Certain specific information has been intentionally excluded from this memorandum for security purposes. Should you have any questions or require further clarification, please submit a ticket to the ALSDE Service Desk using the following email address: servicedesk@alsde.edu or call Mrs. Tuyen Collins at 334-694-0797.

EGM:BTP

cc: LEA Technology Coordinators
LEA Data Managers
Dr. Brandon T. Payne
Mr. Chuck Marcum
Mr. David Pope
Mrs. Stacy Royster
Mrs. Tuyen Collins

FY23-3055