K12 Security Advisory Guidance for Improving Cybersecurity in Mississippi School Districts

Information Security, or Cybersecurity, is a dynamic, ever-evolving field. The days of a school district addressing its data security concerns through the purchase of fireproof cabinets have given way to fighting daily online attacks from overseas parties. The emergence of new threats is happening in a world where near-instant access to student and district information is expected not only by school employees, but also by a broad group of stakeholders. Layer into this the need to protect student data under the terms of federal laws such as the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA) and the Protection of Pupil Rights Amendment (PPRA), and the complexities of school districts' cybersecurity status can seem overwhelming.

Mississippi school district personnel wrestling with cybersecurity challenges have expressed their desire for guidance from the Mississippi Department of Education (MDE). In response, and in cooperation with district technology directors, MDE's Office of Technology and Strategic Services (OTSS) has created a guidance document to advise district administrators, technology directors, and staff on these issues.

The MDE will develop additional chapters in the coming months, growing the list of resources and links that address each subject matter area. Each chapter will guide districts as they develop and implement a comprehensive Cybersecurity Plan.

This guide also serves as a companion to MDE's Cyber Awareness Webinar series, which is available on the Information Security and Data Privacy webpage (link below). Please check that page regularly for guidance document updates and new webinar postings.

Information Security and Data Privacy | The Mississippi Department of Education (mdek12.org)

MISSISSIPPI DEPARTMENT OF EDUCATION

Chapter 3. "To Do"[1]: Policies and Procedures

Introduction: The focus of this chapter is the need "To Do," or specifically to create policy on cybersecurity for your school district.

A. What is cybersecurity policy?

The National Institute for Standards and Technology (NIST) defines "policy" as "statements, rules or assertions that specify the correct or expected behavior of an entity." A cybersecurity policy applies those statements, rules or assertions to how an entity manages and uses information technology. A school district must guide its staff, students, and stakeholders in their use of IT resources through policy.

Well-developed cyber security policies should include both protective elements (identifying unallowed behaviors and prescribing consequences for the same) and proactive elements (creating opportunities for staff to plan for emerging threats).

B. Why are cybersecurity policies important in K12?

Schools handle a vast amount of sensitive data, including student and employee records, financial information, and confidential communication. Cybersecurity policies create safeguards to protect this data from unauthorized access, ensuring privacy and compliance with data protection regulations.

Cybersecurity policies establish preventive measures to reduce the risk of data breaches, thereby preserving the integrity and confidentiality of educational data. Cyberattacks can disrupt educational services, leading to downtime, loss of critical resources, and an interruption in the learning process. Cybersecurity policies help establish measures to prevent and mitigate the impact of such disruptions, ensuring continuity of educational services.

C. What types of cybersecurity policies should we be concerned with?

While different sources may specify different lists of policy topics, the MDE has identified the following twelve (12) subjects as most relevant to Mississippi districts:

1. Data Protection and Privacy - outlines how sensitive student and staff data is collected, stored, processed, and shared.
2. Acceptable Use - defines acceptable behaviors when using the school's technology resources.
3. Password Authentication - establishes rules for creating and managing passwords, and the use of multi-factor authentication.
4. Network Security - defines the measures needed to secure the school's network infrastructure.
5. Device Management - addresses the security standards for both school-provided and personally owned devices connecting to the school network.

[1] Chapter 3. "To Do: Policies and Procedures:" is an excerpt from the MDE's 2023 K12 Security Advisory Guidance for Improving Cyber Security in Mississippi School Districts. For the full guidance, please visit Information Security and Data Privacy section of the MDE website [*Information Security and Data Privacy | The Mississippi Department of Education (mdek12.org)*].

6. Patch and Vulnerability Management - outlines the procedures for monitoring, assessing, and applying software updates.
7. Incident Response and Reporting - defines the steps to take in the event of a cybersecurity incident.
8. Backup and Data Recovery - comprehensive backup strategy should be outlined in this policy.
9. Remote Learning and Telework - addresses the security measures required for accessing school resources from off-site locations.
10. Security Awareness and Training - focuses on educating staff, students, and parents about cybersecurity best practices.
11. Physical Security - includes measures to physically secure devices, servers, and networking equipment to prevent unauthorized access and tampering.
12. Third-Party Vendor Risk Management - outlines the assessment and management of cybersecurity risks associated with these vendors.

Each of these topic areas addresses a unique aspect of cybersecurity policy development. Starting in early 2024, the MDE will provide specific information regarding each policy type listed.

D. How can Districts best work with stakeholders on policy and manage the change that will result?

Developing effective cybersecurity policies in a school district involves collaboration among various stakeholders to ensure comprehensive coverage and alignment with the educational goals. When a district begins policy development work, it should first identify all the parties who should be part of the conversation.

How do you make those determinations? Consider who has the direct knowledge about the behaviors you are trying to address. School administrators' insights into student and staff behavior can help align cybersecurity policies with the educational goals and operational requirements of the school district. At the same time, teachers and instructional technologists can describe technology usage patterns and specific needs for cybersecurity in the classroom.

Are you concerned about the impact of your policies? Legal and compliance experts offer guidance on legal and regulatory requirements related to cybersecurity, privacy, and data protection.

Do you think the perspective of outsiders might help? External cybersecurity experts and consultants, whether in your community or not, can provide valuable insights and best practices.

Finally, how are you going to get the cybersecurity policy message out in an understandable way? Getting your district's communications and public relations team involved early is important for not only writing good policy but also effectively communicating it to all stakeholders.

The stakeholders listed above are not the only parties you may want to engage in the work of cybersecurity policy development. However, the more stakeholders who feel they've had a voice in that work, the more voices you have supporting changes that come from that work. Stakeholders who are actively involved in policy discussions can become your most positive change agents.

E. How do you develop cybersecurity policies?

First, form your team. Take the stakeholders you identified in the previous step and add your district's IT professionals, legal experts, compliance officers, and management. You want to balance interest and expertise with the need for diversity of opinions.

Next, after your group is formed, have different individuals and/or teams research and report to the group on specific topics, such as:

- The high-level goals and objectives of any cybersecurity policies, such as protecting data, ensuring compliance, and reducing cyber risks.
- The organization's assets, data types, critical systems, and potential cybersecurity risks that impact them from various cyber threats and vulnerabilities.
- Applicable laws, regulations, industry standards (e.g., GDPR, HIPAA, ISO 27001), and best practices that are relevant to education.

Once the group has a good understanding of the district's cybersecurity landscape, begin to categorize potential policy areas into high-level domains like data protection, access control, incident response, network security, etc. This makes policy management more organized.

Now begins the work of writing policy. There are a few strategies to follow in developing your actual policies:

- Use clear, concise, and easily understandable language for each domain.
- Address specific risks and compliance requirements.
- Specify roles and responsibilities for policy enforcement and compliance.

Once you have draft policy language, circulate it among key stakeholders, including legal, IT, and management teams, for review. Incorporate feedback and make necessary revisions to improve clarity and effectiveness. Once the language is finalized, you must obtain necessary approvals from management and other relevant stakeholders to ensure adoption.

When it's time to communicate the policies to all employees, rely on your stakeholder group. Encourage them to reach out to their district colleagues and counterparts to start speaking the language of cybersecurity policy. Your stakeholder group will be critical in ensuring all students and staff understand their roles in maintaining cybersecurity.

Finally, maintain thorough documentation of all policies, procedures, incidents, and training programs for future reference and analysis.

F. How do you implement your cybersecurity policies?

Implementing cybersecurity policies in school districts requires a systematic approach that involves planning, communication, training, and ongoing evaluation.

Planning requires that all resources that are affected by the policies be tracked, verified, and secured based on the functional areas the policies pertain to. The documentation gathered by your policy team can be used to identify all those areas and the potential impacts.

Communication to all stakeholders who may be affected by the new policies should be ongoing and multi-directional. Have your policy team make updates to the stakeholder groups they represent. Give

those groups multiple opportunities and channels to ask questions about policy or business process changes.

Train your stakeholders on the importance of the policies you have implemented and, if possible, provide regular, engaging learning tools and opportunities. Keep your stakeholders informed of cybersecurity updates, incidents, and relevant information on a regular, ongoing basis. Provide regular reports on the effectiveness of cybersecurity measures and incident response activities.

Continuously evaluate the effectiveness of cybersecurity measures, policies, and procedures. Stay informed about emerging threats, technologies, and best practices to adapt policies and practices accordingly for ongoing improvement.

G. How do your cybersecurity policies support your cybersecurity plans?

Cybersecurity policies are a crucial component of an organization's broader cybersecurity strategy and plans. They provide the necessary framework, guidelines, and rules to ensure that the organization's cybersecurity objectives are effectively met. They direct student and staff behavior by providing guidance and direction to individuals within the organization regarding appropriate conduct, security protocols, and best practices.

Policies help in planning and allocating appropriate resources, including budget, personnel, and technology, to support the cybersecurity objectives outlined in the cybersecurity plan. They guide investment decisions and resource allocation based on identified risks and priorities.

Policies encourage a culture of continuous improvement by incorporating mechanisms for regular reviews, updates, and enhancements. They help in gathering feedback, analyzing incidents, and making necessary adjustments to enhance the overall effectiveness of the cybersecurity plan.

Cybersecurity Plans outline active steps with policies and procedures that function as support to those active processes and action plans with clear timelines and authorizations.

H. Summary and Next Steps

Cybersecurity policies are essential tools that support and reinforce the cybersecurity plans of an organization. They provide the necessary structure, guidelines, and regulations to ensure effective implementation, maintenance, and evolution of cybersecurity strategies and plans. Policies provide a flexible framework that allows for regular updates and adjustments to address new and evolving cybersecurity threats. They help the organization stay agile and adapt its cybersecurity plans to changing threat landscapes and technological advancements.

In early 2024, MDE will begin providing topic-specific guidance (see Section C of this document) to districts who seek to create their own policies. While that list of policy topics address the major areas of cybersecurity for most school districts, some may have specific concerns not included. Please reach out to MDE for questions about policy topics which do not appear on the list.