If your district technology team needs support, please have them reach out to a METL Executive board member or a member of the METL Cybersecurity Task Force. We are here to help all schools stay secure while teaching and learning.

For more information

www.misecure.org

NATIONAL GOVERNORS ASSOCIATION

misen Michigan Statewide Educational Network

DTMB Technology, Management & Budget

merit

metl Michigan Education Technology Leaders

MAISA MICHIGAN ASSOCIATION OF INTERMEDIATE SCHOOL ADMINISTRATORS
SUPPORTING REGIONAL EDUCATION SERVICE AGENCIES

MISecure

Quick Self-Audit

Introductory Companion to

METL's Essential Cybersecurity Practices for K12

1. People

a. When was your most recent internal conversation about cybersecurity? Who was involved in that conversation? (*Control 17 and 19*)

b. Does your district provide cybersecurity training? For who (admin, staff, students)? (*Control 17*)

c. Who has the keys to your kingdom? Do they use different accounts for daily activities and system administration work? (*Control 4*)

d. Do you have a procedure for assigning appropriate access when staff are hired and for removing access when staff leave or change roles? (*Control 14, 16*)

e. Do you perform regular audits of user accounts to make sure that people have access to what they need, but no more? (*Control 14, 16*)

2. Things

a. Do you know what hardware is connected to your network? (*Control 1*)

b. Do you know what software is in use on all systems? (*Control 2*)

c. Do you know which systems contain sensitive data and who has access? (*Control 13*)

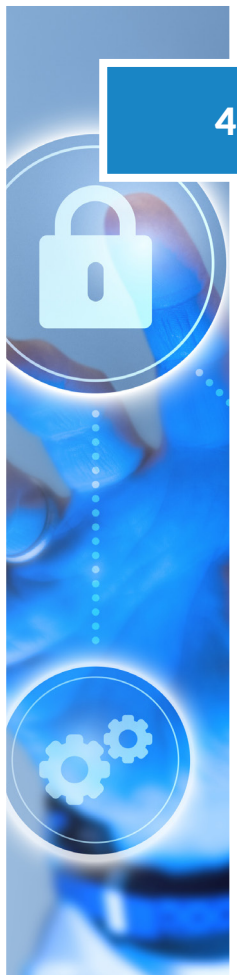
3. Design

a. Do you intentionally deploy and maintain systems with security in mind? (*Controls 5,9*)

b. Are you requiring MFA ('multi-factor authentication') for any logins? Which ones (staff, admin, everyone)? (*Control 16*)

c. Does your district segment your internal network to control the access of data between those networks? Does segmentation include separation of guest network, and HVAC (or other controls) networks from business networks? (*Controls 12 and 15*)

d. Do you provide remote access to your systems? How do you ensure that access is safe and secure? (*Control 12*)



4. Process

a. Do you keep your systems up-to-date? How frequently do you apply updates? (*Control 3*)

b. Do you keep phishing & malware protection enabled and up-to-date everywhere? (workstations, email systems, servers) (*Control 7 and 8*)

c. Do you scan your network for security vulnerabilities? (*Control 11*)

d. Do you control who has access to your wireless network? (*Control 15*)

5. Response

a. Do you know what you would do in the event of a cyber incident? Do you know who would be involved from the district? Do you know who you would call for help? (*Control 19*)

b. Are you doing regular backups? Are you testing and keeping a copy of your backups offline? (*Control 10*)

c. Are you keeping logs so that someone could go back and find out how, when and why something bad happened? (*Control 6*)

d. Can you identify [who, where, how, when] administrative access or system changes have occurred? (*Control 4*)

e. If a district laptop or phone is lost or stolen, is that data still secured? (*Control 13*)

These 20 questions will help you to ***think*** about cybersecurity practices in your district. Start the conversation ***today***.

This Quick Self Audit references cybersecurity best practices and "controls" that are outlined in more detail in the Essential Cybersecurity Practices for K12, which can be found at www.misecure.org.