



K12 SIX ESSENTIAL CYBERSECURITY PROTECTIONS FOR THE 2023-2024 SCHOOL YEAR

– IMPLEMENTATION STANDARDS VERSION 1.0 –

Developed by K-12 IT practitioners, for K-12 IT practitioners—and aligned to nationally-recognized cybersecurity frameworks—the [K12 SIX Essential Cybersecurity Protections](#) are a short list of pragmatic cybersecurity controls that all school systems should prioritize for implementation. Updated for the 2023-24 school year, they are designed to defend school communities from the most common cyber threats they face, including those recently identified by the K12 Security Information eXchange (K12 SIX), Cybersecurity & Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and school cyber insurance providers.

This companion document—**Implementation Standards**—further defines expectations for each K12 SIX recommended protection in the form of a four-scale rubric: ‘at risk,’ ‘baseline,’ ‘good,’ and ‘better.’ At a minimum, school districts should focus on meeting the ‘baseline’ standard of practice. More protection is offered by meeting more advanced standards of practice.

Nonetheless, implementation of these protections should not be construed as a guarantee of the cybersecurity of managed IT systems and data, nor should the implementation of these protections be considered a substitute for instituting a comprehensive, cross-organizational cybersecurity risk management program. While K-12 IT staff have a critical role to play, organizational risk management—including for cybersecurity issues—is a core governance responsibility of policymakers and leaders across the organization.















Other key features of the Implementation Standards include:

- Tips on how to determine whether your school system has correctly implemented the recommended K-12-specific protective measures
- Expected impacts to staff and student experiences and workflows based upon the direct experience of K-12 IT leaders
- Guidance on the relative costs of implementing recommended protections in financial terms, technical complexity, and IT staff time
- Alignments to the most current versions of the National Institute for Standards and Technology Cybersecurity Framework ([NIST CSF v1.1](#)), the Center for Internet Security Critical Security Controls ([CIS Controls v8](#)), and CISA’s [Cybersecurity Performance Goals](#) (CPGs v1.0.1)
- NEW: This year’s edition includes a glossary for terminology used in the document.

K12 SIX Essential Cybersecurity Protections for the 2023-2024 school year (summarized on the following page) consists of fourteen cybersecurity controls—grouped into five categories—that every school district and K-12 organization should strive to implement.



K12 SIX ESSENTIAL CYBERSECURITY PROTECTIONS: 2023-2024 SCHOOL YEAR

Recommended Protection	Description
1.0 Sanitize Network Traffic to/from the Internet	
 1.1 Block malicious web content	Block access to known malicious online content
 1.2 Defend against email attacks	Protect users from email-based scams and fraud
 1.3 Segment & limit exposed services	Establish safeguards for access to critical internal and external services
2.0 Safeguard Devices	
 2.1 Restrict administrative access	Limit privileged user accounts to reduce the impact of attacks
 2.2 Apply endpoint protection	Ensure devices used for school remain safe whether accessed on or off premises
3.0 Protect Identities	
 3.1 Protect user logins	Implement multi-factor authentication (MFA) to safeguard against compromised passwords
 3.2 Improve password & account management	Prevent account compromise, sharing, and re-use—commonly responsible for data breaches
 3.3 Minimize 3rd party risk	Mitigate risks introduced by relying on vendor tools and services
4.0 Practice Continuous Improvement	
 4.1 Install security updates	Protect against known vulnerabilities through timely patching of IT systems, computers, and equipment
 4.2 Backup critical systems	Ensure continuity of operations by enacting policies to enable the timely restoration of data and systems
 4.3 Manage sensitive data	Enact policies to regularly archive and/or delete sensitive data and documents
5.0 Communicate and Collaborate	
 5.1 Train to improve cybersecurity awareness	Reinforce cyber hygiene practices and precautions to prevent cyber attacks
 5.2 Plan for cyber incidents	Prepare for cyber incidents by developing and testing an incident response plan
 5.3 Contribute to a collective defense	Share information about threats, vulnerabilities, incidents, and best practices with partners and peers



Finally, please note that this document was created with the substantial input and advice of K12 Security Information eXchange (K12 SIX) members, all of whom are practicing K-12 IT leaders. K12 SIX is grateful for their leadership and support. Nonetheless, errors and omissions in this document are the responsibility of K12 SIX alone, and recommendations and report contents do not necessarily represent the views of individual working group members or initiative sponsors.

Questions or comments about this product series can be directed to K12 SIX at <https://www.k12six.org/contact>.

About the K12 Security Information eXchange

The K12 Security Information eXchange (K12 SIX) is a cyber threat information sharing hub for K-12 organizations—including school districts, charter schools, private schools, and regional and state education agencies—to aid in preventing and mitigating attacks. This non-profit member community is a cost-effective forum for crowdsourcing security information among a vetted, trusted group of professionals with a common interest, using common technology and with supporting, independent analysis from the K12 SIX security staff and the Global Resilience Federation multisector network of information sharing communities. Visit www.K12SIX.org to learn more.

The development of the K12 SIX Essential Cybersecurity Protections for the 2023-2024 School Year was made possible with the support of CDW Education.



Education



1.0 Sanitize Network Traffic to/from the Internet

This category of protections is designed to defend against threats targeting school-managed devices, services, and applications exposed to the internet. It consists of three controls:

- 1.1 Block malicious web content
- 1.2 Defend against email attacks
- 1.3 Segment & limit exposed services



1.1 Block Malicious Web Content



Most school districts have implemented web filtering to protect minors from inappropriate online content, such as pornography. Those same tools can often also be leveraged to prevent students and staff from inadvertently accessing malicious web content, whether on campus or off.

Malware’s initial point of entry onto a school district device is often via a visit to a malicious website, sometimes spurred by a phishing email. In many cases, malware blocking functionality may be built into the tools that school districts already have access to or employ for compliance with the *Children’s Internet Protection Act* (CIPA).

How do I know if my district’s malware filtering is working?
 Visit <https://www.wicar.org/> from a district-owned device on the district network. If you see a red “something is not right” warning, your district may be at avoidable risk.

1.1 Block Malicious Web Content	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> Filtering only for CIPA compliance No web-based malware control 	<ul style="list-style-type: none"> Malware blocking enabled in available tools Deployed to staff and student users 	<ul style="list-style-type: none"> Malware blocking enabled in available tools Deployed to all devices, including those managed by facilities/operations Filtering includes URL, DNS, keyword, geolocation, and/or content <p><i>Alternative: Allow list only</i></p>	<ul style="list-style-type: none"> Malware blocking enabled in available tools Deployed to all devices, including those managed by facilities/operations Malware is logged, reported, and reviewed Out-of-compliance systems and devices are identified and remediated Dynamic/real-time filtering including URL, DNS, keyword, geolocation, and content <p><i>Alternative: Allow list only</i></p>
Impact on Users	At avoidable risk	Low	Low	Medium
Implementation Cost	N/A	Low	Medium	Medium
Alignments	NIST CSF v1.1: Protect PR.PT; CIS Controls v8: 9.2 Use DNS Filtering Services; CISA CPG v1.01: 2.W No Exploitable Services on the Internet, 2.X Limit OT Connections to Public Internet			



1.2 Defend Against Email Attacks



Email-based phishing attacks are designed to trick students and staff into revealing information, installing malware, and/or transferring money to scammers. Messages typically appear to originate from someone “known” and often convey a sense of urgency.

School staff are commonly targeted by online criminals via email-based phishing scams to compromise passwords, steal paychecks, steal W-2 tax forms, or trick them into purchasing gift cards. Business email compromise (BEC) schemes target school district staff with financial authority with sophisticated lures seeking to steal millions of dollars, primarily via ACH/invoice fraud.

One way to assess your district’s resilience to email-based phishing scams: Review staff email logs for potential phishing lures and compromises. Is spam filtering effective? Are staff comfortable reporting concerns?

1.2 Defend Against Email Attacks	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> Email or spam filtering suppressed or not enabled 	<ul style="list-style-type: none"> Vendor default email or spam filtering enabled 	<ul style="list-style-type: none"> Default spam filtering enabled, including SPF and DKIM Attachments scanned for malware Office suite macros blocked, if applicable IT staff alerted when anomalous emails are received 	<ul style="list-style-type: none"> Default spam filtering enabled, including SPF, DKIM, and DMARC Attachments scanned for malware and executables Office suite macros blocked, if applicable IT staff alerted when anomalous emails are received or sent and act promptly to mitigate issues Outgoing email monitored for the unauthorized release of sensitive data
Impact on Users	At avoidable risk	Low	Low	Medium
Implementation Cost	N/A	Low	Medium	High
Alignments	NIST CSF v1.1: Protect PR.PT; CIS Controls v8: 9.6 Block Unnecessary File Types, 9.7 Deploy and Maintain Email Server Anti-Malware Protections; CISA CPG v1.01: 2.N Disable Macros by Default, 2.M Email Security			



1.3 Segment & Limit Exposed Services



Sensitive software and services should not be broadly accessible to unauthorized users or systems, whether via the internet or internal school district networks. In some cases, services can introduce vulnerabilities to attack simply by being turned on.

School systems should restrict access to sensitive systems from unauthorized devices and users, including students and guests. For instance, remote desktop access may be enabled to ensure staff can access critical applications and files off-campus. Yet, a federal cybersecurity advisory (“[Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data](#)”) warned that authorities “frequently see malicious cyber actors exploiting exposed Remote Desktop Protocol services to gain initial access to a network and, often, to manually deploy ransomware.”

Is my school district at risk? Check your firewall rules for services allowing port 3389 (and/or RDP access). Using Shodan (<https://www.shodan.io>), scan your public IPs for exposed RDP.

1.3 Segment & Limit Exposed Services	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> Remote Desktop (RDP), File Transfer (FTP), Telnet File Shares (SMB), POP and/or IMAP exposed to internet without protective measures 	<ul style="list-style-type: none"> RDP, FTP, Telnet, SMB, POP and/or IMAP exposed, but behind an application gateway, proxy, or IP Access Control List (ACL) 	<ul style="list-style-type: none"> RDP, FTP, Telnet, SMB, POP, and/or IMAP exposed, but with MFA protecting abuse Network Level Authentication (NLA) enabled Segmentation restricts students from accessing internal-facing systems, software, and services they have no need to access At least annual external vulnerability scans 	<ul style="list-style-type: none"> Remove public internet-facing RDP, FTP, Telnet, SMB, POP, and IMAP exposure NLA enabled Internal networks comprehensively segmented by defined roles Continuous external vulnerability scans
Impact on Users	At avoidable risk	Low	Medium	Medium
Implementation Cost	N/A	Low	Medium	Medium
Alignments	NIST CSF v1.1: Protect PR.PT; CIS Controls v8: 12.2 Establish and Maintain a Secure Network Architecture; CISA CPG v1.01: 2.W No Exploitable Services on the Internet, 2.X Limit OT Connections to Public Internet, 2.F Network Segmentation			



2.0 Safeguard Devices

This category of protections is designed to harden both end-user (student, staff, admin) devices and IoT devices managed by other departments (such as facilities/operations). It consists of two controls:

- 2.1 Restrict administrative access
- 2.2 Apply endpoint protection



2.1 Restrict Administrative Access



Attackers who target school districts often leverage elevated rights—necessary for modifying and installing software—on district-managed devices. Restricting access to those elevated rights substantially complicates the ability of threat actors to install malware, steal credentials, and compromise other district-owned devices.

An unintentional download of a malicious application to any device on the district network—whether a teacher/staff/student device or an IoT device managed by facilities/operations—can lead to the compromise of the district’s entire IT system. This cost-effective control can be instrumental in mitigating worst-case cybersecurity incidents.

How do I know if my district has correctly restricted local admin rights? On any Windows user machine at a command prompt check “net localgroup administrators” for the user’s membership and if found, your district may be at avoidable risk.

2.1 Restrict Administrative Access	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> Admin rights are granted to staff, students, and/or devices managed by facilities/operations by default 	<ul style="list-style-type: none"> Admin rights are disabled by default for all users, including for devices managed by facilities/operations Exceptions are manually managed 	<ul style="list-style-type: none"> Admin rights are disabled by default for all users, including for devices managed by facilities/operations A temporary exception process exists, allowing for temporary accounts and/or temporary rights elevation 	<ul style="list-style-type: none"> Admin and poweruser rights are disabled by default for all users, including for devices managed by facilities/operations District-approved software and drivers can be installed without local admin rights Automated processes audit and remove users from administrator groups IT staff use least privileged accounts for routine (WWW and email) activities
Impact on Users	At avoidable risk	High	Medium	Medium
Implementation Cost	N/A	Low	Low	Medium
Alignments	NIST CSF v1.1: Protect PR.AC; CIS Controls v8: 12.8 Establish and Maintain Dedicated Computing Resources For all Administrative Work; CISA CPG v1.01: 2.Q Hardware and Software Approval Process			



2.2 Apply Endpoint Protection



Advanced Endpoint Protection (AEP) protects district-managed devices from viruses and malware. AEP solutions defend against new and emerging threats that may be missed by legacy anti-virus products.

Software vulnerabilities, phishing campaigns, and malicious websites can grant attackers a foothold on district-managed devices. After gaining this foothold, attackers will often install malicious software to maintain persistence, perform reconnaissance, pivot to other network assets, and exfiltrate sensitive data. Advanced endpoint protection can help prevent this type of malicious activity on your district’s network.

How do I know if endpoint protections are installed and working? On a Windows device, craft an eicar.txt file with the EICAR test string: https://en.wikipedia.org/wiki/EICAR_test_file. Change the file extension to ‘.com’ and observe the result. If the file is not detected, hidden, deleted, or otherwise removed, your district may be at avoidable risk.

2.2 Apply Endpoint Protection	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> No endpoint protection, or endpoint protection unmanaged 	<ul style="list-style-type: none"> Implement next generation anti-virus (NGAV) product for all devices running Windows or macOS—and all servers—with tamper protection enabled 	<ul style="list-style-type: none"> Implement extended detection and response anti-malware (XDR) product and/or endpoint detection and response (EDR) product for all district-managed devices and servers, with tamper protection enabled 	<ul style="list-style-type: none"> XDR product installed + EDR product for all district-managed devices and servers, with tamper protection enabled 24/7/365 managed detection and response (MDR)/security operations center (SOC) coverage <p><i>Alternative: Implement application allow-listing on all district-managed devices, e.g., via Windows Defender Application Control (WDAC), AppLocker, or similar service</i></p>
Impact on Users	At avoidable risk	Low	Low	Low
Implementation Cost	N/A	Low	High	High
Alignments	NIST CSF v1.1: Protect PR.PT; CIS Controls v8: 10.1 Deploy and Maintain Anti-Malware Software; CISA CPG v1.01: 3.A Detecting Relevant Threats and TTPs			



3.0 Protect Identities

This category of protections is designed to protect the personal information of school community members—and sensitive operational records, such as those maintained by accounting, facilities, transportation, and HR—from unauthorized access, changes, and exfiltration. It consists of three controls:

- 3.1 Protect user logins
- 3.2 Improve password and account management
- 3.3 Minimize 3rd party risk



3.1 Protect User Logins



Users need more than a password to adequately protect district-managed accounts from unauthorized logins and abuse. One strong option is Multi-factor Authentication (MFA). To login to an account or complete a transaction, MFA requires two or more independent credentials: something the user knows (such as a password); something the user has (such as a security token or authentication app); and something the user is (by using biometric verification methods).

One of the biggest shortcomings of traditional user ID and password logins is that passwords can be easily compromised. The goal of MFA is to create a layered defense that makes it more difficult for an unauthorized person to abuse school logins to district-managed devices and systems, even in the case when those passwords may be compromised or cracked. Implemented correctly, this protective measure can be very effective.

How do I know if my district is protecting logins with MFA? Login for the first time to a district account from a personal device at home. You should get a prompt to verify your access via a code provided either by SMS or an authentication

3.1 Protect User Logins	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> Sole reliance on passwords for authentication 	<ul style="list-style-type: none"> Require MFA for all teachers and staff to access high-risk systems, including operations /facilities staff Require MFA for district-managed social media accounts 	<ul style="list-style-type: none"> Require MFA for all teachers and staff to access all district-managed systems, including operations/facilities staff Require MFA for vendors and social media accounts Opt-in MFA for students 	<ul style="list-style-type: none"> Implement adaptive MFA for all staff (with exception groups, as appropriate) to access all district-managed systems, including operations/facilities staff Require MFA for vendors and social media accounts Require FIDO2 keys for high-risk staff and systems Require MFA for students
Impact on Users	At avoidable risk	Medium	Medium	High
Implementation Cost	N/A	Low	Medium	Medium
Alignments	NIST CSF v1.1: Protect PR.AC; CIS Controls v8: 6.3 Require MFA for Externally-Exposed Applications, 6.4 Require MFA for Remote Network Access, 6.5 Require MFA for Administrative Access; CISA CPG v1.01: 2.H Multi-Factor Authentication (MFA)			



3.2 Improve Password & Account Management



Passwords remain the primary means of providing student and staff access to sensitive school district accounts and systems. Unfortunately, users tend to generate weak passwords and/or reuse passwords even after they have been compromised.

Many school cyber incidents involve reuse of stolen credentials or brute force attacks on logins. School districts lacking updated password management policies aligned to best practices are significantly increasing risks to their school community.

How do I know if my district may have a password management problem? If you can change your primary district password to one that you have used recently, your district has not restricted password reuse.

3.2 Improve Password & Account Management	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> • Password practices allow for short, reused passwords • User accounts not routinely deprovisioned or disabled • User accounts/ passwords are shared 	<ul style="list-style-type: none"> • Staff use at least 12-character long passwords, changed on first use • Password re-use restricted • At least bi-annual resets for accounts not protected by MFA • Account lockout after X failed logons • Departing user accounts disabled at least annually 	<ul style="list-style-type: none"> • Staff use passphrases—at least 16-characters—changed on first use, MFA enforced • Password re-use restricted • Resets and lockouts triggered by evidence of attempted compromise • User accounts disabled within 7 days of notification of exit 	<ul style="list-style-type: none"> • Staff use passphrases—at least 16-characters—changed on first use, MFA enforced • Password re-use restricted • Resets and lockouts triggered by evidence of attempted compromise • User account permissions modified within 3 days of exit/role change
Impact on Users	At avoidable risk	Medium	Medium	High
Implementation Cost	N/A	Low	Low	Medium
Alignments	NIST CSF v1.1: Protect PR.AC, PR.AT; CIS Controls v8: 5.2 Use Unique Passwords, 6.3 Require MFA for Externally-Exposed Applications, 6.4 Require MFA for Remote Network Access, 6.5 Require MFA for Administrative Access; CISA CPG v1.01: 2.G Detection of Unsuccessful (Automated) Login Attempts, 2.B Minimum Password Strength, 2.C Unique Credentials, 2.D Revoking Credentials for Departing Employees			



3.3 Minimize 3rd Party Risk



From disruptions to data breaches and leaks, school districts must mitigate risks introduced by the reliance on vendors and suppliers.

[K12 SIX research](#) reveals that a significant vector for school data breaches are vendors and non-profit partners. Recent high-profile cyber incidents experienced by, e.g., [Illuminate Education](#) serve to underscore the cybersecurity risks of outsourcing critical functions. CISA encourages both school systems to [consider cybersecurity during procurement](#) and vendors to demonstrate a commitment to [secure-by-design practices](#).

How can I assess my current 3rd party risk?
 Review contractual provisions for key vendors to identify security assurances—beyond student data privacy provisions—including timely vulnerability disclosure and incident notification assurances.

3.3 Minimize 3rd Party Risk	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> Vendor accounts and/or passwords not managed Cybersecurity not part of vendor evaluation No master list of vendors/suppliers 	<ul style="list-style-type: none"> Vendor accounts manually expired; default vendor passwords changed Cybersecurity included in vendor evaluation process A master list of district vendors/suppliers list created 	<ul style="list-style-type: none"> Vendor accounts automatically expired; default vendor passwords changed Cybersecurity a significant factor in vendor evaluation process Current vendors/suppliers cataloged and updated at least annually Timely vulnerability disclosure and incident notification incorporated into contracts; data sharing agreements restrict improper sharing 	<ul style="list-style-type: none"> Vendor accounts automatically expired; default vendor passwords changed and periodically audited All 3rd party applications/services in use (including free software) evaluated for cybersecurity risk Current vendors cataloged and continuously updated to stay current Timely vulnerability disclosure and incident notification incorporated into contracts; data sharing agreements reviewed annually for all data exchanges involving PII
Impact on Users	At avoidable risk	Low	Low	Medium
Implementation Cost	N/A	Low	Medium	High
Alignments	NIST CSFv1.1 Identify.SC2; CIS Controls v8: 15 Service Provider Management; CIS CPG v1.01: 1.I Vendor/Supplier Cybersecurity Requirements, 1.G Supply Chain Incident Reporting, 1.H Supply Chain Vulnerability Disclosure			



4.0 Practice Continuous Improvement

This category of protections is designed to shed light on high-priority IT management and maintenance activities that directly contribute to cybersecurity risk reduction. It consists of three controls:

- 4.1 Install security updates
- 4.2 Backup critical systems
- 4.3 Manage sensitive data



4.1 Install Security Updates



Technology developers release updates to their tools in the form of patches to enhance functionality and address security vulnerabilities. Timely installation of security updates prevents malicious actors from exploiting known vulnerabilities.

Regular and timely patching of all school district IT systems—operating systems, applications, servers, and appliances—is an important component of an effective cybersecurity risk management program. Malicious actors can exploit vulnerabilities—within hours of their becoming publicly disclosed—to gain a foothold in school networks, in some cases bypassing existing protections.

How do you know if your school district may be at risk? On a student/ teacher device, check to see when software updates were last installed. For example, on a Windows computer, go to Settings > Update & Security > Windows Update > View Update History to see a list (and the date) of the most recent updates. If the latest installed update is over 30 days ago, your district may be at avoidable risk.

4.1 Install Security Updates	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> Critical security updates not always applied within 30 days 	<ul style="list-style-type: none"> Critical security updates applied within 30 days to all operating systems, applications, servers, and appliances—including those managed by operations/facilities 	<ul style="list-style-type: none"> Critical security/known-exploited updates applied within 14 days to all operating systems, applications, servers, and appliances—including those managed by operations/facilities All other security updates applied within 30 days to high-risk IT systems and applications 	<ul style="list-style-type: none"> All security/known-exploited updates applied within 14 days to all operating systems, applications, servers, and appliances—including those managed by operations/facilities Periodic auditing and remediation of systems and appliances found to be missing security updates
Impact on Users	At avoidable risk	Low	Low	Low
Implementation Cost	N/A	Medium	Medium	High
Alignments	NIST CSF v1.1: Protect PR.PT; CIS Controls v8: 7.3 Perform Automated Operating System Patch Management, 7.4 Perform Automated Application Patch Management, 12.1 Ensure Network Infrastructure is Up-to-Date; CISA CPG v1.01: 1.E Mitigating Known Vulnerabilities			



4.2 Backup Critical Systems



Ensuring the ability to quickly restore IT operations from backups has long been a staple of IT best practices. Given the rise of ransomware actors targeting school districts, the need for immutable backups—i.e., backups that cannot be altered or changed—has become essential.

Ransomware actors target backup systems—whether on-site or in the cloud—to diminish the ability of victims to recover from their attacks. While continuous cloud backups can protect school districts from downtime due to hardware failures and physical incidents, they do not necessarily protect against malicious actors seeking to delete or corrupt backups. School districts should strive to follow the 3-2-1 backup rule: storing at least three copies or versions of data on two different pieces of media, one of which is offsite. The offsite backup needs to be immutable.

How do you know if your school district's backups are immutable? If IT staff can delete district backups, they also can be deleted or corrupted by malicious actors. Your district may be at avoidable risk.

4.2 Backup Critical Systems	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> Backups made irregularly, if at all 	<ul style="list-style-type: none"> One backup stored offline and/or immutable At least 30 days of backups 	<ul style="list-style-type: none"> At least 1 immutable backup At least 1 copy of backup stored offsite At least 3 months of backups 	<ul style="list-style-type: none"> At least 1 immutable backup on 2 different media types At least 1 copy of backup stored offsite and encrypted at rest At least 6 months of backups Onsite backup hosts isolated on own network, protected by MFA
Impact on Users	At avoidable risk	Low	Low	Low
Implementation Cost	N/A	Medium	Medium	High
Alignments	NIST CSF v1.1: Protect PR.IP; CIS Controls v8: 11.2 Perform Automated Backups; CISA CPG v.1.01: 2.R System Backups			



4.3 Manage Sensitive Data



School districts are entrusted with collecting and managing sensitive data about students, families, staff, and district operations in compliance with federal, state, and local laws. School districts should seek to minimize the risks associated with data breaches and leaks by proactively archiving or deleting sensitive data on a regular basis consistent with applicable records retention and privacy laws.

A significant number of K-12 cyber incidents involve unauthorized access to sensitive data about not only current but former students and staff. Old data can be found in many places, including in emails, vendor databases, file transfer servers, reports and extracts, as well as in district databases and file stores. Much of this data can (and should) be periodically archived or deleted to reduce potential harms stemming from a data breach.

Is my district at risk of a data breach involving former students and staff? Search for .csv files on district systems that are more than 10 years old. How many of those documents could and should have been deleted?

4.3 Manage Sensitive Data	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> No policy or data management controls 	<ul style="list-style-type: none"> District files are purged and/or archived at least annually consistent with records retention requirements 	<ul style="list-style-type: none"> District and vendor files are regularly purged and/or archived at least annually consistent with records retention requirements Sensitive data files are tracked 	<ul style="list-style-type: none"> District and vendor files are regularly purged and/or archived consistent with records retention requirements Sensitive data files are managed, tracked—tagged as confidential—and logged
Impact on Users	At avoidable risk	Medium	Medium	Medium
Implementation Cost	N/A	High	High	High
Alignments	NIST CSF v1.1: Protect PR.DS; CIS Controls v8: 3.3 Establish and Maintain a Data Inventory, 3.5 Securely Dispose of Data			



5.0 Communicate and Collaborate

This category of protections emphasizes the need for enhanced communication and collaboration within and across school systems. It consists of three controls:

- 5.1 Train to improve cybersecurity awareness
- 5.2 Plan for cyber incidents
- 5.3 Contribute to a collective defense



5.1 Train to Improve Cybersecurity Awareness



Some may consider users the weakest link in a cybersecurity program, but they can be part of the solution. Inspire users to adopt high-impact security practices to help keep your organization safe.

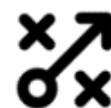
Building a shared understanding of the importance of information security, including users' roles and responsibilities, is paramount to achieving school district security goals. This can be accomplished via a combination of periodic information security awareness training—both broadly focused and targeted toward specific products and departments—and general security awareness campaigns. It is important to ensure training and awareness activities are engaging, reflect best practices, and contribute to a positive security culture.

How do you know if your cybersecurity training is working? Post-training, IT teams should see sustained increases in reporting of phishing and other email threats by end users.

5.1 Train to Improve Cybersecurity Awareness	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> No staff cybersecurity training 	<ul style="list-style-type: none"> General security awareness training done on an at least annual basis 	<ul style="list-style-type: none"> Phishing tests conducted at least once a semester General security awareness training conducted multiple times a year Specific security awareness and threat notifications communicated as warranted 	<ul style="list-style-type: none"> Phishing tests conducted monthly General security awareness training conducted multiple times a year Specific security awareness and threat notifications communicated as warranted Product-specific security training provided, as appropriate, including for staff responsible for operations/facilities technology
Impact on Users	At avoidable risk	Low	Low	Medium
Implementation Cost	N/A	Low	Medium	Medium
Alignments	NIST CSF v1.1: Protect PR.AT; CIS Controls v8: 14.2 Train Workforce Members to Recognize Social Engineering Attacks; CISA CPG v1.01: 2.1 Basic Cybersecurity Training			



5.2 Plan for Cyber Incidents



Experiencing a cybersecurity incident involving the disruption of school, fraud, or a potential data breach is stressful. The actions you take in the hours and days following discovery of the incident are critical to your ability to recover and key to maintaining the trust of your school community.

It is not a question of whether your school district will experience a cyber incident, but when. Cyber incident response planning not only ensures that best practices are followed during an incident, but also helps develop an understanding of the systems, services, processes, and communications needed to improve organizational resilience. Developing and practicing a cyber incident response plan is instrumental to recovering quickly and gracefully from cyber incidents.

In case of a cyber incident, what are the first steps most district should take? Stay calm. Preserve your organization’s ability to investigate and recover by isolating, not prematurely powering off, affected systems. Seek assistance from incident response experts and follow [K12 SIX guidance](#) and your Incident Response runbook/plan.

5.2 Plan for Cyber Incidents	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> No cyber-specific incident response (IR) plan or runbook in place 	<ul style="list-style-type: none"> Basic cyber-specific IR runbook completed with important contacts identified 	<ul style="list-style-type: none"> Basic cyber-specific IR runbook completed with important contacts identified Formal IR plan written and adopted Initial internal tabletop exercise has been completed 	<ul style="list-style-type: none"> Basic cyber-specific IR runbook completed with important contacts identified Formal IR plan written and adopted Tabletop exercises performed regularly with both internal and external parties IR plan updated periodically and integrated with districtwide IR/emergency operations/disaster recovery plans
Impact on Users	At avoidable risk	Low	Low	Medium
Implementation Cost	N/A	Low	Medium	Medium
Alignments	NIST CSF v1.1: Protect PR.IP-9 Response Plans; CIS Controls v8: 17 Incident Response Management; CISA CPG v1.01: 2.5 Incident Response (IR) Plans			



5.3 Contribute to A Collective Defense



Cybersecurity is a collective action problem. By sharing timely information about relevant incidents, vulnerabilities, and threats with K-12 peers through an Information and Sharing Analysis Center (ISAC)—including actionable Indicators of Compromise (IoCs)—we can reduce the cost and burden of protecting school communities nationwide.

With the rise of the K-12 education sector as a target of increasingly sophisticated threat actors, information sharing has taken on paramount importance. Whether by receiving timely updates on emerging issues or facilitating collaboration on K-12-specific cybersecurity strategy and tactics, national and state-specific ISACs provide for the secure, non-public exchange of sensitive cybersecurity-related information without fear of regulatory consequences.

Do you receive cyber threat intelligence via participation in an ISAC? School systems are eligible for membership in the K12 Security Information eXchange (K12 SIX)—designed specifically for the needs of the K-12 sector—and the Multi-State Information Sharing and Analysis Center (MS-ISAC), which serves the broader state, local, tribal, and territorial government community.

5.3 Contribute to a Collective Defense	At Risk	Baseline	Good	Better
Protective Measures	<ul style="list-style-type: none"> No participation 	<ul style="list-style-type: none"> District participates in an ISAC and/or local cybersecurity collaboration group 	<ul style="list-style-type: none"> District participates in one or more ISACs District has established a process to handle responsible cybersecurity disclosures District website hosts a security.txt web file to facilitate disclosures by third parties 	<ul style="list-style-type: none"> District participates in one or more ISACs District has established a process to handle responsible cybersecurity disclosures District website hosts a security.txt web file to facilitate disclosures by third parties District proactively shares timely information and IOCs on threats, vulnerabilities, and incidents with trusted peers and partners
Impact on Users	At avoidable risk	Low	Low	Low
Implementation Cost	N/A	Low	Low	Medium
Alignments	NIST CSF v1.1: ID.RA, RS.AN, RS.CO; CIS Controls v8: 7 Continuous Vulnerability Management, 17.2 Establish and Maintain Contact Information for Reporting Security Incidents; CISA CPG v1.01: 4.A Incident Reporting, 4.B Vulnerability Disclosure/Reporting, 4.C Deploy Security.TXT files			



GLOSSARY

3-2-1 Rule: A method for protecting data by keeping three copies, two on different media, and one offsite.

Account Lockout: A feature that locks a user account after too many incorrect login attempts.

Adaptive MFA: Multi-factor Authentication that uses context and behavior patterns to decide if extra steps are needed.

Administrative Rights: Permissions allowing a user to make major changes to a computer or network.

Advanced Endpoint Protection (AEP): A concept focusing on continuous monitoring and defense against cyber threats at their endpoints.

Allow List: A list of entities approved to access a certain system.

Appliances: Hardware performing specific functions, like routers, switches, filtering, etc.

Auditing and Remediation: The process of reviewing and fixing potential security issues.

Biometric Verification Methods: Security measures using unique biological characteristics like fingerprints or facial recognition to check identity.

Brute Force Attacks: Attempts to gain system access by trying all possible passwords or decryption keys.

Business Email Compromise (BEC): A scam tricking employees into transferring funds or sensitive info by impersonating an executive.

Center for Internet Security Critical Security Controls (CIS Controls v8): A set of actions for cyber defense providing ways to stop the most common attacks.

Children's Internet Protection Act (CIPA): A U.S. law to control children's access to harmful online content.

Cybersecurity and Infrastructure Security Agency (CISA): The U.S. agency defending the country's critical infrastructure from physical and cyber threats.

CISA's Cybersecurity Performance Goals (CPGs v.101): Guidelines from CISA to enhance cybersecurity posture and performance for critical infrastructure.

Cloud Backups: Copies of data stored on remote servers, accessed over the internet.

Compromise: Unauthorized or unwanted access to a system, often to steal data or cause harm.



Cyber Insurance Providers: Companies offering coverage for costs related to recovery after a cybersecurity event.

Cyber Threats: Potential dangers or disruptions to a technology system.

Cybersecurity Risk Management Program: An approach to secure an organization's information by identifying threats, assessing vulnerabilities, determining impacts, and planning responses.

Cybersecurity Risks: Potential dangers related to cyber attacks, including data breaches, business disruption, financial loss, and reputation damage.

Data Breach: An event where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Data Management Controls: Strategies and procedures that manage the full data lifecycle needs of an enterprise.

Data Purging: The process of permanently removing select data from various storage locations.

Data Sharing Requirements: Rules for an organization to share data with third parties, detailing what, with whom, for what, and when.

Data Tagging: Assigning labels or tags to data to organize, categorize, and retrieve it efficiently. Can be used to assign sensitivity levels to data.

Default Vendor Passwords: Initial passwords given to a vendor for access. Changing these is crucial for security.

Deprovisioning: Removing an individual's access to certain systems and services when not needed, like when an employee leaves.

DomainKeys Identified Mail (DKIM): Email authentication method that detects forged sender addresses.

Domain-based Message Authentication, Reporting and Conformance (DMARC): Email authentication protocol protecting a domain from unauthorized use.

Email-based Phishing Attacks: Cyber attacks where the attacker tricks the email recipient into revealing sensitive information or installing malware.

Encrypted Backup: Data transformed using an algorithm to make it unreadable without the decryption key.

Endpoint Detection and Response (EDR): Security tools monitoring endpoint and network events, responding to, and recording this info for further analysis.



Exfiltrate: The unauthorized copying, transfer, or retrieval of data from a computer or server.

Extended Detection and Response (XDR): Security tech collecting and correlating data from multiple security layers to improve threat detection and provide incident response.

Federal Bureau of Investigation (FBI): The domestic intelligence and security service of the United States.

FIDO2 Keys: An open standard for password-less authentication. FIDO2 security keys use the key and biometric data or a PIN to access accounts.

FileShares via SMB (Server Message Block): A protocol for sharing resources on a network, used by multiple operating systems.

File Transfer Protocol (FTP): A network protocol for transferring computer files between a client and server.

Geolocation Filtering: Controlling access to internet content based on the user's geographical location.

Hardware and Software Vulnerabilities: Weaknesses in an information system that could be exploited to compromise security.

Immutable Backups: Backups that cannot be changed or deleted, essential for preventing data loss from ransomware attacks.

Incident Notification: The process of alerting an organization about a security incident that may impact its operations or security.

Internet of Things (IoT): The network of physical devices with software, sensors, and network connectivity that enables data exchange.

IP Access Control List (ACL): A list of permissions determining access and actions on an IP network.

Keyword Filtering: A technique to block content if certain keywords are found.

Least Privileged Access: The principle that users should have the minimum levels of access needed to complete their job functions, reducing security breach potential.

Malware: Software designed to disrupt, damage, or gain unauthorized access to a computer system.

Managed Detection and Response (MDR): A service providing threat hunting and response services, and possibly incident response services.

Mission-Critical IT Systems and Applications: Essential IT systems and software applications, whose failure could have serious consequences.



Multi-factor Authentication (MFA): A security measure requiring multiple authentication methods to verify user identity.

Network Level Authentication (NLA): A technology used in Remote Desktop Services requiring user authentication before session establishment.

Next Generation Anti-Virus (NGAV): Antivirus software using sophisticated methods like AI and behavioral analysis to detect threats.

National Institute for Standards and Technology Cybersecurity Framework (NIST CSF): A voluntary framework for critical infrastructure organizations to manage cybersecurity risk. Version 1.1 consists of five core functions: Identify, Protect, Detect, Respond, and Recover.

Office Suite Macros: A series of commands used to automate repetitive tasks or, maliciously, to deliver malware.

Operating Systems: The primary software controlling all the hardware and software on a computer.

Operations/Facilities: The infrastructural aspects of an organization, including physical locations, equipment, and technology systems.

Organizational Risk Management: The forecasting and evaluation of risks together with the identification of procedures to avoid or minimize their impact.

Password Reuse: The practice of using the same password for multiple accounts, which increases risk.

Password Strength: The effectiveness of a password in resisting attempts at guessing or cracking. Increased by length, complexity, and unpredictability.

Personally Identifiable Information (PII): Information that can identify an individual. Must be protected to ensure privacy and comply with federal and state laws.

Phishing Campaigns: Coordinated efforts to trick individuals into revealing sensitive information, usually by impersonating a trustworthy entity.

Phishing Email: A cyber attack that uses email to trick the recipient into revealing personal information or installing malware.

Phish Testing: A training technique using simulated phishing emails to test employee ability to identify and avoid phishing attacks.

Pivot: The method attackers use to move deeper into a network in search of targeted data and systems.

Product-Specific Security Training: Training focused on the security features and potential vulnerabilities of specific software or hardware products.



Protective DNS: A security solution that blocks dangerous DNS responses, preventing users from accessing malicious domains.

Protective Measures: Actions, procedures, or technologies implemented to reduce the risk or impact of a cyber threat.

Proxy: A server that acts as an intermediary for requests from clients seeking resources from other servers.

Ransomware: Malicious software designed to block access to a system or data, often by encrypting it, until a ransom is paid

Records Retention Requirements: Regulations that define how long certain data or records must be kept before deletion or destruction.

Remote Desktop Protocol (RDP): A proprietary protocol by Microsoft providing a user with a graphical interface to connect to another computer over a network.

Security Awareness Campaigns: Campaigns aimed at increasing awareness of cyber threats and promoting safe online behaviors.

Security Operations Center (SOC): A centralized unit in an organization dealing with security issues on an organizational and technical level.

Security Updates/Patches: Updates or modifications provided by developers to fix security vulnerabilities, improve functionality, or enhance software and hardware performance.

Segmentation: In networking, separating a network into smaller parts, or subnets, to improve performance and security.

Sensitive Data: Information that must be protected against unwarranted disclosure due to legal, ethical, proprietary, or privacy considerations.

Smishing: A form of phishing in which an attacker uses an SMS text message to trick recipients into clicking a link and sending the attacker private information or downloading malicious programs to a smartphone

Spam Filtering: A program used to detect and prevent unwanted and unsolicited emails from reaching a user's inbox.

Spray Attack: A form of cyber-attack or hacking technique where an attacker indiscriminately attempts multiple login attempts or access requests using a list of usernames and/or passwords.

Sender Policy Framework (SPF): A method to prevent email spoofing by defining which IP addresses are allowed to send mail for a particular domain.



Telnet: A command and protocol for accessing remote computers, now mostly replaced by SSH for security reasons.

Temporary Exception Process: A procedure allowing temporary permissions or access to users under certain conditions or for limited periods.

Third-Party Vendors: Companies or individuals providing services or products to an organization but not part of the organization itself.

Threat Actors: Entities who carry out cyber attacks, can be individuals, groups, or state-sponsored entities, potentially including employees or students

URL Filtering: A type of web filtering that blocks access to specific websites by comparing web addresses to a list of banned URLs.

Vendor Account Expiry: The process of making a vendor's account inactive after a specified period or after completion of a project or task.

Vendor Evaluation Process: A system of quantitative and qualitative measures used to assess a vendor's cybersecurity, capabilities, performance, and overall suitability for a task or project.

Vendor Files: Files or data that are stored or processed by third-party service providers.

Vetted: The process of thoroughly investigating an individual, software, system, or organization before granting approval or acceptance.

Vulnerability Scans: The systematic identification, analysis, and reporting of technical vulnerabilities in a system.

Web Filtering: The process of blocking access to specific websites, pages, or functions on the internet, typically used to prevent access to inappropriate or malicious content