K12 SIX Cybersecurity Standards:
2021-2022 School Year

The K12 SIX Essential Cybersecurity Protections are a short list of actionable cybersecurity controls that all school districts should prioritize for implementation. Organized into four overarching categories, they are designed to defend against the most common cyber threats facing school districts, including those recently identified by the Federal Bureau of Investigation (FBI) and the Cybersecurity & Infrastructure Security Agency (CISA).

This companion document—***K12 SIX Cybersecurity Standards***—further define implementation standards for each of K12 SIX recommended protective measures 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 for each recommended protective measure. More protection is offered by meeting higher level standards of practice. Nonetheless, the implementation of these protective measures should not be construed as a guarantee of the cybersecurity of school district-managed IT systems and data, nor should the implementation of these protective measures be considered a substitute for instituting a comprehensive cybersecurity risk management program.

Other key features of the *K12 SIX Cybersecurity Standards* include:

- Tips on how to determine whether your district has implemented the recommended K12-specific protective measures
- Expected impacts to staff and students based upon the direct experience of K12 IT leaders
- Guidance on relative costs of implementing recommended protections in financial terms, technical complexity, and IT staff time
- Alignments to both the NIST Cyber Security Framework (v1.1) and the CIS Controls (v8)

Finally, please note that this document was created with the substantial input and advice of K12 Security Information Exchange (K12 SIX) working group members, all of whom are practicing K12 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. Feedback from the K12 community is welcomed and will be used to improve future iterations of this work.

1.0 Sanitize Network Traffic to/from the Internet

1.1 Filter Out Malware

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 downloading malware, whether on campus or off.

Malware's initial point of entry onto a school district device is often via a web page visit to a malicious website, sometimes spurred by a phishing email. Even if a hostile link sneaks through the district's email filter, it is possible to stop the attack via network-based malware filtering. In many cases, this functionality may be built into the tools that school districts already 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 Filter Out Malware	At Risk	Baseline	Good	Better
Protective Measures	• No online malware control	• Malware blocking enabled in available tools • Deployed to staff and student users	• Malware blocking enabled in available tools • Deployed to staff and student users—and servers *Alternative: Allow list only*	• Malware blocking enabled in available tools • Deployed to staff and student users—and servers • Malware is logged, reported on, and reviewed • Out-of-compliance systems and devices are identified and remediated *Alternative: Allow list only*
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			

1.2 Campaign Against Email Scams

Phishing is a type of social engineering attack designed to trick students and staff into revealing information, installing malware, and/or transferring money. Email is a common vector, but attacks can involve fake URLs and be delivered via voice, fax, and/or SMS messages. Phishing attacks typically appear to originate from someone “known” and often convey a sense of urgency.

In 2020, the FBI recorded twice as many phishing incidents as any other computer crime. In recent years, dozens of school districts have fallen prey to business email compromise (BEC) attacks leveraging fake construction invoices, costing victim districts millions of dollars. Other common school-specific phishing emails attempt to steal staff paychecks, steal staff W-2 tax forms, or trick staff into buying and transferring gift cards to criminal actors.

One way to assess your district’s resilience to email-based phishing scams: Implement phishing testing for teachers and/or staff, whether via a formal program or via less formal means.

1.2 Campaign Against Email Scams	At Risk	Baseline	Good	Better
Protective Measures	• Web and spam filtering suppressed or not enabled	• Default web and spam filtering enabled	• Default web and spam filtering enabled • IT purges phishes, and sends notices when phishing attacks are discovered	• Default web and spam filtering enabled, including for properly configured SPF/DKIM/ DMARC • Phishing training and testing required for staff on a recurring schedule • IT purges phishes and warns users when phishing attacks are discovered
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: 9.7 Deploy and Maintain Email Server Anti-Malware Protections, 14.2 Train Workforce Members to Recognize Social Engineering Attacks			

1.3 Block Malicious Documents

Embedding a malicious macro in an office suite file or document – sometimes referred to as malicious document or 'maldoc' – is a popular tactic used by criminals to bypass anti-virus software and gain unauthorized, persistent access to sensitive school data and IT systems. These maldocs may be delivered via email (often in the form of a social engineering attack) or made available for download from compromised websites.

Properly configured, this protective measure prevents educators, staff, and students from inadvertently opening and executing malicious macros in popular office suite applications that have led to ransomware and identity theft in K12 settings.

How do I know if my district is at risk from 'maldocs'? Send yourself a Microsoft Excel spreadsheet with a macro in it from a personal (non-district) email account. If your email is delivered and you can open the file and execute the macro, your district may be at avoidable risk.

1.3 Block Malicious Documents	At Risk	Baseline	Good	Better
Protective Measures	• No document control	• Block Microsoft Word and Excel documents with embedded macros downloaded from the internet	• Block Microsoft Word and Excel documents with macros downloaded from the internet • Block all other macro-capable Office downloads	• Block all documents containing macros, except for those digitally signed by the district *Alternative: All students and staff use Chrome OS.*
Impact on Users	At avoidable risk	Low	Low	Medium
Implementation Cost	N/A	Low	Low	Medium
Alignments	NIST CSF v1.1: Protect PR.PT; CIS Controls v8: 9.6 Block Unnecessary File Types			

1.4 Limit Exposed Services

Internet-exposed services, such as remote desktop protocol (RDP), provide a method for attackers to reach inside a school district's network to create disruption and steal data. In some cases, these services can be vulnerable to attack simply by being turned on.

School districts enable remote desktop access to ensure staff can access critical applications and files off-campus, as well as to facilitate the provision of technical support. A December 2020 joint Cybersecurity Advisory ("Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data")—coauthored by the FBI, CISA, and MS-ISAC—warned school districts that they "frequently see malicious cyber actors exploiting exposed Remote Desktop Protocol (RDP) 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.

1.4 Limit Exposed Services	At Risk	Baseline	Good	Better
Protective Measures	• RDP exposed directly to internet with no protective measures in place	• RDP exposed, but behind an application gateway, proxy, or IP Access Control List (ACL)	• RDP exposed, but with MFA or another second factor protecting abuse • Network Level Authentication (NLA) enabled	• Remove public internet facing RDP exposure • Block internet-facing access to other potentially vulnerable services, such as FTP and SMB
Impact on Users	At avoidable risk	Low	Medium	High
Implementation Cost	N/A	Low	Medium	Low
Alignments	NIST CSF v1.1: Protect PR.PT; CIS Controls v8: 12.2 Establish and Maintain a Secure Network Architecture			

2.0 Safeguard Student, Teacher, and Staff Devices

2.1 Restrict Administrative Access

Attack pathways into school districts often leverage administrative rights on teacher and staff devices. Restricting those rights slows the ability of threat actors to install malware, steal passwords, and pivot their activities to other district-owned devices. It is among the most effective, lowest cost cybersecurity risk management interventions a school district can undertake.

Granting teachers and staff administrative rights to their district-owned devices allows them to download and install potentially malicious programs, as well as programs that have not been vetted or district-approved. An unintentional download of a malicious application to a staff device on the district network can lead to the compromise of the district's entire IT system, as numerous K12 ransomware attacks have demonstrated.

How do I know if my district has correctly restricted local admin rights on end user devices? On any Windows user machine, type "whoami" at a command prompt to identify the username. Then type "net user *username*" and check whether localgroup membership includes administrators. Also check "net localgroup administrators" for the user's membership. If the user has administrative rights, your district may be at avoidable risk.

2.1 Restrict Administrative Access	At Risk	Baseline	Good	Better
Protective Measures	• Staff and/or students have admin rights by default to their district devices	• Admin rights are disabled by default for all students and staff • Exceptions are manually added	• Admin rights are disabled by default for all students and staff • A temporary exception process exists, including temporary accounts and/or temporary rights elevation	• Admin rights are disabled by default for all students and staff • Approved software and drivers can be installed without requiring local admin rights • Automated processes audit and remove users from admin groups
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			

2.2 Apply Endpoint Protection

Advanced Endpoint Protection (AEP) protects student and staff devices from viruses and malware. AEP solutions detect threats that may not have been previously blocked by older anti-virus products.

Phishing campaigns or other infection mechanisms can grant attackers a foothold into your school district's network by compromising student and staff 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 AEP is 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 detected, hidden, deleted, or otherwise removed, you are likely protected. Otherwise, your district may be at avoidable risk.

2.2 Apply Endpoint Protection	At Risk	Baseline	Good	Better
Protective Measures	• No endpoint protection enabled	• Enable Windows Defender or install similar advanced anti-virus product for all student/staff devices and servers *Alternative: Students/staff use Chrome OS or other systems at low risk for malware*	• Extended detection and response anti-malware (XDR) product installed or similar advanced threat protection (ATP) software + endpoint detection and response (EDR) product for all student/staff devices and servers	• Extended detection and response anti-malware (XDR) product installed or similar advanced threat protection (ATP) software + endpoint detection and response (EDR) product for all student/staff devices and servers • Implement application allow-listing, e.g., via Windows Defender Application Control (WDAC) or AppLocker
Impact on Users	At avoidable risk	Low	Medium	High
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			

3.0 Protect the Identities of Students, Teachers, and Staff

3.1 Protect User Logins

Users need more than just a password to adequately protect their accounts from unauthorized logins and abuse. One strong option to protect user identities is Multi-factor Authentication (MFA). To login to an account or complete a transaction, MFA requires two or more independent credentials to protect user identities: 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 district staff logins, even in the case when those passwords may be compromised or cracked. Implemented correctly, this protective measure is very effective.

How do I know if my district is protecting logins with MFA? Login to a district account from a personal device at home. If you do not get a prompt to verify your access via a code provided either by SMS or an authentication application, your district may be at avoidable risk.

3.1 Protect User Logins	At Risk	Baseline	Good	Better
Protective Measures	• Sole reliance on passwords for authentication	• Enable Microsoft Azure MFA (or similar) solely for high-risk staff, such as IT staff, principals, senior administration, and school board members	• Enable adaptive MFA for all staff, which works by using contextual information and business rules to dynamically mitigate against potentially risky behaviors of a particular user/group	• Force MFA for all staff (with exception groups, as appropriate)
Impact on Users	At avoidable risk	Medium	Low	High
Implementation Cost	N/A	Low	High	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			

3.2 Improve Password Management

Passwords remain the primary means of providing student and staff access to school district IT systems and to ensuring the confidentiality of sensitive data. Unfortunately, users frequently reuse and share passwords even when they have been compromised—and unencrypted passwords can often be found in scripts used by IT staff and in files on district servers and devices.

Verizon's 2020 Data Breach Investigations Report revealed that over 80 percent of hacking-driven data breaches involved brute force attacks on logins or the reuse of stolen credentials. For the foreseeable future, passwords remain a flawed but necessary method for authenticating users. School districts lacking modern password management policies—covering issues such as password strength, expiration, lockouts and recovery, privileged access, temporary/terminated employees, etc.— expose themselves to needless and unacceptable levels of risk.

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 previously used, your district has not restricted password reuse—one key to an effective password management policy.

3.2 Improve Password Management	At Risk	Baseline	Good	Better
Protective Measures	• Password practices allow for short/reused passwords	• Long passwords • Password reuse restricted • Bi-annual (or more frequent) resets	• Long passphrases • Password reuse restricted • Bi-annual resets, providing on-demand resets are triggered by evidence of compromise	• Force MFA for all staff (with exception groups, as appropriate)
Impact on Users	At avoidable risk	Low	Low	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			

3.3 Stop Online Classroom Invasions

In response to the rise of the COVID-19 pandemic, the use of online video conferencing systems has been widely leveraged to provide remote classroom experiences for students. Left unsecured and publicly accessible, remote classrooms have been widely exploited.

Online classroom invasions are typically caused by the public sharing of what should be confidential information about when and how to access remote learning sessions. In some cases, students are responsible for inviting other students to prank their online classrooms; in other cases, external actors seek to create havoc and harm in online classrooms by posting violent, pornographic, and hateful content. Just as such disruptions are not tolerated in face-to-face classrooms, they have no place in online settings.

To test your vulnerability for online classroom invasions: Initiate a virtual classroom session and invite a partner playing the role of a student to help. Is it possible for your 'student' partner to invite someone outside the district into the session merely by sharing a link and password? Do you have to approve the outsider before he or she is allowed to join the live session? If not, your district may be at risk of online class invasion.

3.3 Stop Online Class Invasion	At Risk	Baseline	Good	Better
Protective Measures	• No admission controls	• Teachers manually approve admission to online classroom	• Default policies enforced to reduce risk of classroom invasions, such as auto-lobby creation, SSO of students, etc.	• Default policies enforced to reduce risk of classroom invasions • Clear escalation path for issues established • Training/best practices made available to teachers, students, and parents
Impact on Users	At avoidable risk	Low	Medium	Medium
Implementation Cost	N/A	Low	Low	Medium
Alignments	NIST CSF v1.1: PR.AC; CIS Controls v8: 4.1 Establish and Maintain a Secure Configuration Process			

4.0 Perform Regular Maintenance

4.1 Install Security Updates

The developers of hardware and software often release updates to their tools in the form of patches, which may fix known bugs, enhance functionality, and/or fix known security vulnerabilities. For some of the most critical IT systems, security updates are released on a regular basis. Timely installation of these 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 a critical component of an effective cybersecurity risk management program. Malicious actors use known hardware and software vulnerabilities to gain a foothold in school district 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 30-90 days ago, your district may be at avoidable risk.

4.1 Install Security Updates	At Risk	Baseline	Good	Better
Protective Measures	• No security updates policy	• Critical security updates applied within 90 days for operating systems, applications, servers, and appliances	• Security updates applied within 60 days for operating systems, applications, servers, and appliances	• Security updates applied within 30 days for operating systems, applications, servers, and appliances • Periodic auditing of systems and appliances not being updated
Impact on Users	At avoidable risk	Low	Low	Low
Implementation Cost	N/A	Low	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			

4.2 Backup Critical Systems

The regular backing up of critical data, systems, and applications has long been a staple of IT operations resiliency. Given the rise of ransomware actors targeting school districts, the need for immutable backups—i.e., backups that cannot be altered or changed, including by malicious software—has become essential.

Ransomware actors specifically target backup systems—whether on-site or in the cloud—to ensure their victims cannot recover from their attacks. While continuous cloud backups, such as those provided by Google and Microsoft, can protect school districts from downtime due to hardware failures and physical incidents, they do not necessarily protect against sophisticated actors intentionally seeking to delete or corrupt backups. School districts should strive to follow the 3-2-1 rule of thumb: keep at least 3 copies of your data, store 2 copies on different media, and ensure 1 copy is located 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	• Backups made irregularly, if at all	• One backup stored off-line and/or immutable (i.e., backup cannot be deleted)	• At least 1 immutable backup • At least 1 copy of backup stored off site	• At least 1 immutable backup on 2 different media types • At least 1 copy of backup stored off site • Backup hosts isolated on own network, protected by unique user credentials and/or MFA
Impact on Users	At avoidable risk	Low	Low	Low
Implementation Cost	N/A	Low	Low	Medium
Alignments	NIST CSF v1.1: Protect PR.IP; CIS Controls v8: 11.2 Perform Automated 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. As such, school district leaders require a reasonable understanding of data privacy laws to protect the members of their school community. In so doing, 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.

A significant number of K12 cyber incidents include the exposure of sensitive data about not only current but former students and staff that could have been deleted but was not. Old data can be found in many places, including in staff emails, vendor databases, file transfer locations, reports and extracts, as well as in district databases and file stores. Much of these data can (and should) be deleted on a regular basis to reduce data at risk for a breach.

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

4.3 Manage Sensitive Data	At Risk	Baseline	Good	Better
Protective Measures	• No policy or data management controls	• District files are periodically purged based on records retention requirements	• District and vendor files are purged based on records retention requirements	• District and vendor files are purged based on records retention requirements • Sensitive data files are tracked 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			