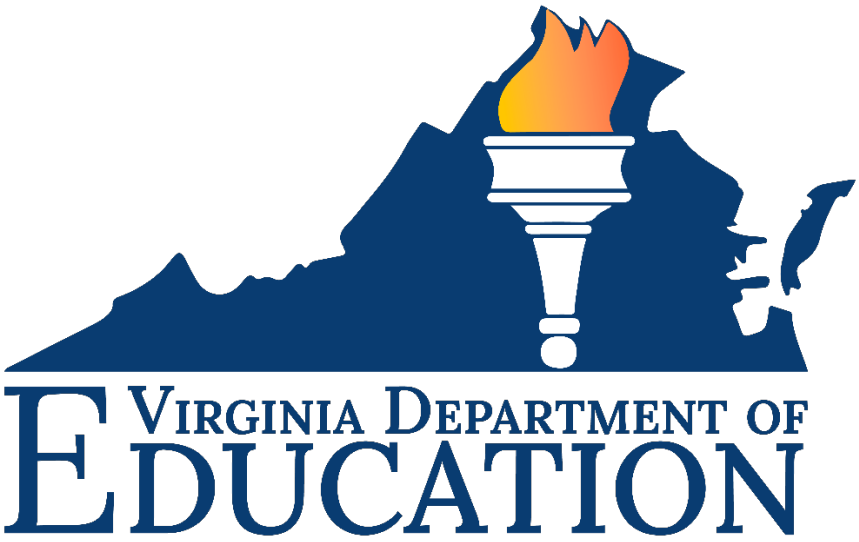
Office of Information Security

Model Security Plan and Best Practice Guidance in Cybersecurity for K-12 Schools



Version 1.0

December 2021

Version Log

Version	Date	Description
1.0	December 2021	First version of document.

Contents

Why Do We Need Cybersecurity?

The General Assembly of Virginia has tasked the Department of Education to provide model cybersecurity guidance to K-12 school divisions in Virginia, COV § 22.1-20.2. The law is intended to protect student data from misuse and dissemination. Although a focus of a division's security plan should be on student data, the obvious needs to protect all data in a division is clear.

A report was issued by the K-12 Cybersecurity Resource Center and the K12 Security Information Exchange (K12 SIX). The report titled "The State of K-12 Cybersecurity: 2020 Year In Review" offers valuable insight into the nationwide problem that schools face in cybersecurity.

Among the valuable information are the following key points:

- The K-12 Cyber Incident Map documented 145 data breach incidents involving public schools (representing 36 percent of all incidents disclosed during the year). These breaches most often involve the unauthorized disclosure of student data but may also include significant amounts of data about school district staff, including educators.
- For the second calendar year running, at least 75 percent of all data breach incidents affecting U.S. public K-12 school districts were the result of security incidents involving school district vendors and other partners.
- During 2020, the K-12 Cyber Incident Map documented 50 instances of U.S. public K-12 school districts being impacted by ransomware, a particularly virulent type of malware designed to facilitate the extortion of money from victims.
- Correlation of attack data shows larger school districts are at a significantly greater risk for experiencing a cyber incident than other types of school districts, as are school districts located in more densely populated parts of the county.
- Spear phishing attacks against school business officials and their vendors continue to plague K-12 districts across the country. Since 2016, the median amount of money stolen in such attacks is $2 million per incident. During 2020, a record-setting $9.8 million was stolen from a single school district.

The concerns facing all K-12 environments are real, expensive, and detrimental to student learning opportunities and outcomes. We have no choice but to adopt basic cybersecurity hygiene and best practice information on our divisions to ensure we are protecting data and access to data to the best of our ability.

What is a Cybersecurity Program?

A cyber security program is a documented set of an organization's information security policies, procedures, guidelines, and standards. More than that, however, it includes a school division's culture and attitudes surrounding cybersecurity and all of the efforts made toward protecting data.

A security program should provide a roadmap for effective security management practices and controls. Having a strong security program helps an organization ensure the confidentiality, integrity, and availability of client and customer information, as well as the organization's private data through effective security management practices and controls.

Confidentiality
Concerned with controlling access to data so that only authorized users can access or modify it.

Integrity
Focuses on keeping data clean and untainted, both in when the data is in use and when it's stored. Users should be able to trust that data was not modified except by those who are authorized.

Availability
While confidentiality is about making sure that only the people who need to access the data can get to it, availability is about making sure that it's easy to access that data should an authorized person need to.

Frameworks

Frameworks for cybersecurity provide a guide for collecting data, analyzing risk, responding to attack, and documentation. For most school divisions, frameworks may be too complicated or based on business environments for effective use. Instead, consider using this document as a framework for baseline cybersecurity. It is our goal to continue to provide best practice information and suggested activities for cybersecurity. This document takes recommendations and foundations from each of these frameworks to produce a best practice guide. If a division requires a more robust implementation, consider following one or more of the frameworks below.

- *Center for Internet Security (CIS) Controls*
  A list of 20 mission-critical controls spread across three categories: basic, foundational, organizational.
- *Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)*
  Consisting of 197 control objectives organized into 17 domains, the CCM focuses solely on cloud computing.
- *Control Objectives for Information Technology (COBIT)*
  Instead of basing compliance on individual security controls, COBIT 2019 starts with stakeholders' needs, assigns job-related governance responsibilities to each type, then maps the responsibility back to technologies. Ultimately, COBIT's goal is to ensure appropriate oversight of the organization's security posture.
- *Cybersecurity Maturity Model Certification (CMMC)*
  Both a set of best practices and a requirement for organizations that solicit DoD contracts. CMMC lists five maturity levels, primarily based on whether the data an organization collects, transmits, stores, and processes is Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).
- *Factor Analysis of Information Risk (FAIR) Cyber Risk Framework*
  Takes an explicit approach to cyber risk management so that organizations can quantify risk regardless of the cybersecurity framework they use.
- *International Office of Standardization (ISO) 27001*
  Includes requirements for establishing, implementing, maintaining, and continually improving an ISMS influenced by the organization's needs, objectives, security requirements, processes, size, and structure. Its best practices include setting controls and processes.

- *MITRE ATT&CK*
  When MITRE began documenting common cyberattack tactics, techniques, and procedures (TTPs) used against Windows enterprise networks, ATT&CK became the baseline acting as a common language for offensive and defensive researchers. MITRE is responsible for establishing and trademarking the Common Vulnerabilities and Exposures (CVE) list.
- *National Institute of Technologies (NIST) Cybersecurity Framework (CSF)* - Originally intended for critical infrastructure owners and operators, NIST CSF can be used by any organization. Many companies outside of the critical infrastructure industry also use the CSF, especially if they need to meet other US federal data protection requirements.
- *National Institute of Technologies (NIST) SP 800-53* - provides a catalog of security and privacy controls for all U.S. federal information systems.

Minimal Requirements and Artifacts of a Division Security Program

Requirements for a school division cybersecurity program include policies and procedures that address disaster recovery and resiliency, incident response and breach notification, review and audits, security awareness training, data retention and disposition, and data sharing.

Disaster Recovery and Resiliency

A Disaster Recovery Plan (DRP) is a guide that helps an organization maintain resiliency.

What is a disaster? There are three categories - natural, man-made, and a hybrid. A natural disaster can be defined as a storm, tornado, pandemic, earthquake, or similar. A man-made disaster can be the accidental or willful destruction of a system or data by a person's actions or lack or actions. Hybrid disasters are combinations of both. Imagine a hybrid disaster as a natural disaster that is triggered in some way by a man-made disaster - perhaps a dam break that causes a flood or the failure of an air conditioning unit that causes heat to destroy a data center.

Disasters happen every day. Don't think of disaster recovery planning as something that will never be used. If a current plan is dusty or doesn't exist, there is work to do. Disasters are not once-in-a-lifetime. You may be affected by a down-stream or up-stream disaster. You may have a water line break in the middle of a school. A power failure could wreak havoc. You may have another pandemic strike. All disasters will attack confidentiality, integrity, and/or availability of systems and data.

Resiliency is the ability to bounce-back, to shift, to adapt, to continue. Resiliency is different from Business Continuity. The International Standards Organization defines Business Continuity as "the capability of an organization to continue the delivery of products or services at acceptable predefined levels following a disruption." Resilience is defined as "the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper." Survive and prosper.

Continuity keeps us going in the face of a power outage. Resiliency keeps us going for a lifetime in the face of a constantly changing environment.

The Disaster Recovery Plan (DRP) is an essential element of a security program. Its purpose is to inform and provide guidance for the preparation and/or recovery of a disaster. It should be easily read and understood by non-technical peoples including Board members and Superintendents. Unless you are following a framework like NIST 800-53 or NIST CSF or similar, there is no set template for a DRP. How you decide to organize the elements of a plan are up to you.

A DRP should include the following elements:

1. Identification of risk tolerance levels and common threats related to geographic or historical data
2. Inventory and descriptions of major systems
3. Inventory of hardware and software
4. Backup and restoration plan and procedures for each major system
5. Identification of recovery time and recovery point objectives
6. List of responsibilities and roles of local staff
7. Communication plan, contact list, and external vendor contacts and SLAs
8. Locations of alternate sites and/or safe sites
9. Explicit instructions for handling sensitive data in times of crisis
10. Instructions for regular testing and review of the plan

A DRP may include more than the technology elements of a disaster. In some businesses the DRP first addresses human safety and reporting, then moves to assets. A division's comprehensive DRP might include more detailed contact information, notification trees, or emergency closing codes. In our Virginia divisions, the technology DRP may be included in a comprehensive Continuity of Operations Plan (COOP). A division may be unique in how detailed a DRP becomes.

Here are some resources that can help you develop a DRP for a division's technology:

- Example Disaster Recovery Plan Templates
  Word | PowerPoint | PDF | Smartsheet
- University of Iowa Example DRP
- Finding the Right Server Backup Methods for You
- CoSN Technology Disaster Recovery Checklist
- CoSN IT Crisis Preparedness for Natural Disasters

DRP is more than just backups of data it is about resiliency and recovery. Having a properly constructed plan to recover from a disaster can provide peace of mind not only

to an IT staff but to all stakeholders. Information Security includes DRP as a means of protecting CIA in times of crisis.

Incident Response Plan

An incident response plan (IRP) is a set of instructions to help IT staff detect, respond to, and recover from network security incidents. Having an IRP means that the right people, with the right skills, will be involved to help research, mitigate, and control an incident.

An Incident Response Plan (IRP) is a set of instructions to help IT staff detect, respond to, and recover from network security incidents.

To effectively deal with a cybersecurity incident, your division will need a team that can react quickly. An incident response team, with all the needed stakeholders, should be established. The plan assigns tasks and duties to each member of the team. These tasks can include technical tasks, communications, customer support, Board liaison, law enforcement liaison, and more.

Incident Response is a subfield of cybersecurity. It is easy to quickly become overwhelmed with the number of tasks required for proper incident response and reporting. NIST guidance on incident response is a 54 page manual that provides a summary of incident response. This is just one of 10 guides NIST provides.

IRP Elements

1. Include a list of members of a response team, contact information, and alternates
2. Include a list of response team responsibilities
3. Include of list of contact information for other stakeholders including legal, finance, law enforcement, audit, and public relations.
4. Include steps and tasks to perform in the following four phases: Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Event Activity.

IRP Templates

These publicly available templates can help you develop your own plan.

- Cynet Incident Response Template
- IltaNet Incident Response Plan
- FRSecure Incident Response Plan Template
- Exabeam Incident Response Plan 101

Breach Notification

Our schools hold data on our students, staff, admins, and parents. A breach of any type of data can have consequences. The following information is not exhaustive. Please work together with your division's legal counsel to determine breach notification responsibilities and create policy and guidelines.

Adult Data

Breach notification occurs at various governance levels. Work with division leaders to determine local requirements.

Section 18.2-186.6 of the Code of Virginia, which became effective on July 1, 2008, requires an individual or entity that owns, maintains, or possesses personal identifying information of Virginia residents who has a reasonable belief that such personal information was accessed or acquired by an unauthorized individual or entity to report the unauthorized breach to the Office of the Virginia Attorney General and to provide notification to each affected Virginia resident. For further inquiries regarding database breach notification, please contact the Computer Crime Section at 804-786-2071.

As amended in 2019, "personal information" under Virginia's data breach statute means a Virginia resident's unencrypted, unredacted first initial or first name and last name combined with or linked to any of the following data elements:

- Social security number;
- Driver's license number or state identification card number issued in lieu of a driver's license number;
- Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts;
- Passport number [amendment effective July 1, 2019]; or
- Military identification number [amendment effective July 1, 2019].

Student Data

A data breach is any instance in which there is an unauthorized release or access of PII or other information not suitable for public release. This definition applies regardless of whether an organization stores and manages its data directly or through a contractor, such as a cloud service provider.

Section 22.1-287.02 of the Code of Virginia requires breach notification to parents for students' personally identifiable information.

Use these additional resources to learn more:

- PTAC / USDOE Breach Notification Checklist
- Free Student Privacy Train-the-Trainer Program for K12
- Future of Privacy Forum

Reporting Ransomware

Victims of ransomware should report it immediately to CISA at www.us-cert.gov/report, a local FBI Field Office, FBI Cyber Investigations, Internet Crime Complaint Center, or Secret Service Field Office. These organizations can assist with identification, removal, and response. Additional help may be available from the Virginia Fusion Center.

Review and Audit

How can you possibly defend against attack if you don't know you are being attacked? The answer is do you audit yourself, have others audit you, and do you perform both functions regularly.

Policies describing the monitoring of logs and activities and self-auditing is a critical component of a successful security program.

Your self-audit may come in the form of testing against known best practices, such as Penetration Test. In addition, you should be able to monitor system and server logs for malicious or inconsistent behaviors. A SIEM (Security Information and Event Management) may be useful in your environment to automate the millions of lines of logs generated.

Intrusion Detection and Prevention systems may be part of your unified next generation firewall. Make sure these functions are accurately configured and report strange behaviors to those stakeholders that can act.

External Audits are crucial to testing your security stance. Beyond the financial audit addendum that most school divisions incur, you should be seeking outside assistance to expose the weaknesses in your security program. There are very affordable solution providers that can provide myriad levels of service. Budget for these services and take advantage of the expertise available.

Security Awareness Training

Policies describing formal Security Awareness Training is a critical component of a successful security program.

Establish policies that allow you to enforce security awareness training across your division. Your users are your biggest threat. That adage may be growing old, but certainly your internal users are the threat vector by which most attackers take advantage. Ransomware requires user interaction. Social engineering attacks via email are abundant. The importance of training your users is clear and will help you establish a dialogue with stakeholders. Your division will be stronger, and your users will be more knowledgeable about the part they play.

Some tips for security awareness training:

1. Establish an annual program that includes quick training sessions for users with network, services, or data access.
2. Track user performance and enforce compliance.
3. Consider performing a training campaign during the school year. Too often, tasks are assigned to teachers and staff in the busy summer months when time is limited.
4. Allow a campaign ample time to be successful. Thinks months, not weeks.
5. Campaigns should include topics such as social engineering, ransomware, hygiene, data sharing, spam recognition, and generic security concepts.
6. Consider requiring training for new hires before network access is granted or within a window of time directly after hire. You may be able to add to your Division's onboarding process.
7. There are many free resources for awareness training. You can also develop your own. However, cloud-based vendors make the management and tracking very easy to accomplish. There are also vendors that can work with SCORM compliant Learning Management Systems.

Data Retention and Disposition

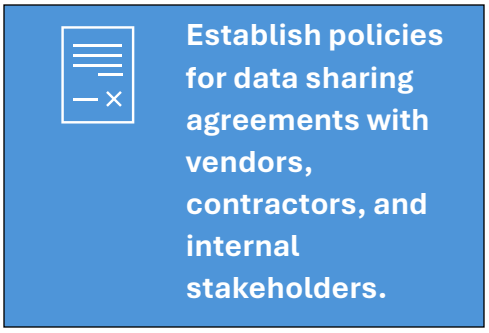
Work with stakeholders and governing authorities to create policy describing retention schedules and proper disposition of data.

The Library of Virginia is tasked by the General Assembly of Virginia to establish schedules for data retention of important documents and the proper disposition of documents and data retrieval devices. The current schedule can be found at the Library of Virginia website.

Here are some important tips when dealing with data retention and disposition:

1. Laws and schedules apply to data in use and data at rest (both digital and analog).

2. Retired hardware elements that contain data should be erased or destroyed as prescribed.
3. Pay attention to the hidden places data may be stored including cameras, fax machines, copiers, and telephone systems.
4. Data that has passed retention schedules should be destroyed unless otherwise provided for in policy. Data should not be kept in archives simply because it can be.
5. Special schedules exist for certain types of data including e-mail, Superintendent correspondence and artifacts, and student records. Be aware of these retention schedules and the special environment you may need to employ to protect data.



Data Sharing

A school division should establish policies for the dissemination of student and business data that conforms to applicable laws including FERPA. The is especially true for student data privacy. Although student data privacy is a subject unto itself, it is also part of the cybersecurity program. Cybersecurity can be enforced with vendors when establishing new contracts or renewing older ones. One helpful resource for such policies and contract addendums is the Student Data Privacy Consortium (SDPC). Each Virginia school division can join the consortium for free on behalf of the Department of Education. The SDPC and its members have already done the hard work of vendor compliance with many of the major EdTech vendors. In your school division, you need only reference the previous agreements and state that you expect the vendor to follow the same rules with your division.

In addition to vendor relationships, internal users should be keenly aware of the type of student information they can share with others. Student data is a protected asset and should be treated with the utmost respect. Establish policies that govern data sharing and dissemination. Use the policies to train stakeholders via table-top exercises, procurement training, or annual security awareness training.

Best Practice Guidance and Controls for Cybersecurity Hygiene

Note: The controls listed in this document are meant to be the most effective and quickly enabled controls that can help to combat ransomware and other known K-12 attack vectors. It is important that these controls not be taken as a complete security program but rather a start toward a larger program that would be governed by a formal framework.

Network Segmentation

Segmentation prevents lateral movement of network traffic and allows the network administrator to specify different constraints, permissions, filtering, quality of service, and priorities for each segment. It allows you to weave together an environment that is transparent to the user, that is more controlled, auditable, and where traffic from one segment may or may not be allowed on another segment.

How does it work in real life? What if we created a VLAN that was solely for administrative computers in the building? We could set rules that prevent any student-designated device or BYOD from accessing (or knowing the existence of) the administrative machine. If a ransomware attack started from a student device, there is a good chance that the spread of such an attack would be contained to the student segment.

Here are some suggested segmentation ideas:

- Administrator devices
- Teacher devices (further segment by grade/subject)
- Student devices (further segment by grade/hall)
- IT devices
- Security devices including cameras & panic systems
- HVAC, fire, kitchen, and plant operations
- Experimental (IOT, Robots, rouge BYOD)

Cyber Insurance

If you have the option of purchasing cyber insurance either as a rider on a school division's existing insurance or a separate product, it is a wise choice. More than likely, an existing general liability insurance policy does not cover the costs associated with data breach and recovery, whether accidental or purposeful. Cyber liability insurance should include both first-party and third-party coverage.

Take a look at the cyber coverage questionnaires from GNY and US RISK. The detailed risk assessment that an insurance company may ask will expose the strength of a program. Don't feel bad if you can't answer every question perfectly, most of the questionnaires are designed to be overkill. You will be asked about controls, how often you test, how often you have others test you, when you reevaluate, previous incidents and breaches, and more. The questions cover physical, logical, and administrative controls.

Among many benefits, cyber liability insurance often covers costs incurred from investigation, monetary loss, downtime, negligence, and interruption. It can also include costs associated with credit monitoring if needed. Legal expenses are also covered. As a school division, you should be covered for ransomware bounty payments if possible. An insurance company will have specific language for dealing with payments and whether it is covered. Payments are often an absolute last resort and can be even illegal.

Insurance might not cover costs associated with breaches caused by a vendor or third party, social engineering attacks, breaches caused by internal users, or advanced persistent threats. These types of attacks are considered preventable with proper security posture.

Average premiums for a $1-$2m coverage window are around $15-$25k per year. Of course, costs depend on a number of factors, customer loyalty, and bulk discounts. The division's financial leadership will be able to work with insurance carriers.

Hardware / Software Useful Lifetime and Replacement Schedules

In today's security environment, we must learn to let go of older technology - both hardware and software. Old technology poses security risks. Older abandoned software has bugs and vulnerabilities. Older hardware is inefficient and can also contain vulnerabilities.

Four tips for changing your school division and encouraging refresh of technology.

- Technology Refresh Policy - Write a policy that describes a refresh cycle for all types of hardware/software in your environment. Use this policy to enforce standards of replacement or retirement. In most cases, a lifespan of 3-5 years is appropriate. If your community understands and supports the policy, they will learn to look forward to replacement and rely on it.
- Budget Planning - Once you have a policy, write your budget to match. Remind budget committees that replacement of older technology is not a wish item. It's security, it's policy, and it's necessary.
- Board and Leadership Support - The more understanding a Board has about how things work, the more they can relay that information to the public. You must convince the Board that technology has a useful lifespan, and that the division has agreed to the terms of that lifespan. When leadership is on your side, you are protected.

Inventory

A complete inventory of devices, assigned users, contract and purchase information should be available. Identification of certain BIOS, manufacturers, operating systems, and system types may be needed when responding to an attack. A complete inventory is also helpful when establishing refresh schedules.

Software Approval Processes

Establish a vetting and approval processes for an approved software inventory. As more and more applications and services move to the cloud, the need to govern the use of random websites is even more important. Establish the rules that allow users to request the use of COTS or SaaS products within your environment.

Patch Management

Security vulnerabilities are being detected constantly. Incorporate the use of patch management software to make sure all operating systems and software are kept up to date. There are various management consoles that allow for the patching of computers and mobile devices. Policies should be developed to make sure that patching is constant, regular, and expected. Users interruption should be minimized as much as possible. Communicate your patch strategy to your users.

Anti-Malware / Anti-Virus / APT Detection

Employ anti-malware and anti-virus on all devices capable of supporting such software. Ensure that signature files and program patches are consistently kept up to date.

Auto-Run

Disable auto-run components of operating systems as possible. Do not allow programs from media storage such as USB drives to launch automatically.

Hard Drive Encryption

Activate operating system level encryption on all systems where supported. This is especially desirable on laptops that travel. If a laptop is lost or stolen, the data will be encrypted. Microsoft has built-in encryption technique for Windows Server and Windows. Purchase laptops that contain a Trust Platform Module chip for use with Microsoft Bitlocker or similar endpoint encryption software.

VPN

Consider the use of VPN for all remote traffic that accesses your datacenter or for the use of protected Internet access for remote computers. VPN can ensure your environment is safe from malicious WIFI access points while also allowing users access to internal resources.

Mobile Device Management

Use of MDM software for mobile devices and laptops can allow system administrators the ability to disable, erase, or “brick” a lost or stolen laptop. MDM software can also help with inventory checks. MDM can be used to enforce security policies on Bring-Your-Own-Device environments.

Cloud Configuration Management

In cloud environments, a major vulnerability is misconfiguration of systems due to the complexity of (or lack thereof) what we have created. We've made it too easy to bring a supercomputing instance online to perform a single function. Often, an operator needs no experience whatsoever to launch a new server that could open a hole to the outside world. The simplicity makes us forget. The complexity makes us look for a quick work-around and not train ourselves. Thus, we end up with servers, services, instances, and applications that are misconfigured and vulnerable to attack.

Five common cloud service misconfigurations:

- Disabled logging/monitoring
- Abandonment of test environments without dismantling
- Overly permissive environments that "make it work"
- Lack of encryption for data stores
- Lack of documentation and follow-up

Use of Administrative Functions and Accounts

In an enterprise environment, there is little justification for anyone outside of assigned duties to retain local admin rights to a client computer. In most environments, users are given only the abilities they need in order to operate. The push to cloud and SaaS implementations has made the need for local admin rights even more obsolete. Still, there are instances when a user wants to install their own printer, WIFI, hardware, software, or are using legacy products. Some allowances may still need to be made to help these users perform their work while protecting the enterprise.

The cybersecurity concept of least privilege prescribes only allowing a user the minimum privilege needed to perform their required functions. This concept should be applied to all system access, including administrative accounts. For some, the use of local admin rights is an absolute need. For others, it's a convenience. Minimizing the use of elevated privileges will help protect your enterprise.

Five reasons to remove local admin rights:

- Helps keep malware off computers
- Helps maintain protections that are in place
- Keeps computers in compliance with organizational policies
- Closes vulnerabilities
- Helps defends against attack

Password Policy

Create a password policy if you do not currently have one. This policy should include:

- Complexity and Length

- Password Age
- Not Repeating Passwords
- Hashing stored passwords
- Failed password attempt lock outs
- Not allowing sequential or repeated characters
- Admin and Service account passwords changed once a year

These should be considered best practices when setting up system controls. NIST latest guidelines talk about the length of a password being the most crucial aspect to security. The minimum length of a password should be 8 characters and could be up to 64 allowing any special character and spaces. Moreover, the passwords generated by machines must be a minimum of 6 characters in length. NIST has also advised that a user lock out should occur at 10 attempts and password hints should not be used at all. To see all of the NIST guidelines for password management you can refer to NIST Special Publication 800-63-3.

Additional Resources

Ransomware Guide from MS-ISAC

https://www.cisa.gov/publication/ransomware-guide

These ransomware best practices and recommendations are based on operational insight from the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinatingly incident response.

The K-12 Cybersecurity Resource Center

https://www.k12cybersecure.com

Since the K-12 Cyber Incident Map was launched by Doug Levin of EdTech Strategies in March of 2017, it has grown to become the definitive source of publicly-disclosed school cybersecurity incident data in the United States. To date, it is has documented well over 1,000 school cyber incidents, resulting in mass identity theft, the loss of hundreds of millions of taxpayer dollars, and the loss of significant instructional time.

The K-12 Cybersecurity Resource Center is the home of the Map and is devoted solely to reporting news and information related to school cybersecurity and privacy issues. It is maintained as a free, independent resource for the K-12 community in partnership with the K12 Security Information Exchange (K12 SIX).

K12 SIX

https://www.k12six.org

The K12 Security Information Exchange (K12 SIX) is a new national non-profit dedicated solely to helping to protect K-12 schools – public and private – from cybersecurity threats, such as ransomware and phishing attacks. It was launched in late 2020 as an affiliate of the Global Resilience Federation in response to the growing cybersecurity challenges facing schools nationwide and in recognition of the unique challenges and context of K-12 operations. For more information, please visit https://www.k12six.org.

CoSN

http://www.cosn.org

CoSN (the Consortium for School Networking) is the premier professional association for school system technology leaders. CoSN provides thought leadership resources, community, best practices and advocacy tools to help leaders succeed in the digital transformation. CoSN represents over 13 million students in school districts nationwide and continues to grow as a powerful and influential voice in K-12 education.

CoSN CETL

https://cosn.org/certification

The CETL® credential is a true measure of today's education technology leaders, identifying those who have mastered the framework skills and knowledge needed to bring 21st-Century skills to schools. The CETL® program is also a professional development tool that can be used to guide education technology leaders' study of learning technologies.

Trusted Learning Environment

https://trustedlearning.org/

The TLE Seal is the nation's only data privacy seal for school systems, focused on building a culture of trust and transparency. The Trusted Learning Environment (TLE) Seal Program was developed by CoSN (the Consortium for School Networking), in collaboration with a diverse group of 28 school system leaders nationwide and with support from AASA, The School Superintendents Association, the Association of School Business Officials International (ASBO) and ASCD.

Cybersecurity & Infrastructure Security Agency (CISA)

https://www.cisa.gov/cybersecurity

CISA leads the Nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services and American way of life.

Center for Internet Security (CIS)

https://www.cisecurity.org/

he Center for Internet Security, Inc. (CIS) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

A community-driven nonprofit, responsible for the CIS Controls and CIS Benchmarks, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

International Association of Privacy Professionals

https://iapp.org

The IAPP is the largest and most comprehensive global information privacy community and resource. Founded in 2000, the IAPP is a not-for-profit organization that helps define, promote and improve the privacy profession globally.

ISACA

https://isaca.org

As a trusted leader for more than 50 years, ISACA helps enterprises thrive with performance improvement solutions and customizable IS/IT training that enable organizations to evaluate, perform, and achieve transformative outcomes and business success.

US Department of Education – Protecting Student Privacy

https://studentprivacy.ed.gov

The U.S. Department of Education is committed to protecting student privacy. We administer and enforce student privacy laws such as the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA). In addition, we provide technical assistance to help schools and school districts safeguard information about students.

US Department of Education – Cyber Considerations for K-12 Schools and School Districts

https://rems.ed.gov/docs/Cybersecurity_K-12_Fact_Sheet_508C.PDF

The U.S. Department of Education has published a fact sheet for schools and schools districts on threats and how to prepare for threats. It includes a 6 step planning process for ensuring you are ready for an incident.

The K-12 Blueprint

https://www.k12blueprint.com/toolkits/security

The K-12 Blueprint offers the latest tools, research data, device information, best practices, deployment strategies, and success stories showing real-world results so that today's education leaders can plan and implement successful technology initiatives.

The K-12 Blueprint Security toolkit - developed with generous support from CDW-G* - includes resources and materials to help school technology leaders make the best decisions to ensure the safety of all school information.

Virginia IT Agency – Threat Management Division

Dean Johnson, Director of Treat Management

Dean's department at VITA can put your IP addresses and Domains into his monitoring tools at no charge.