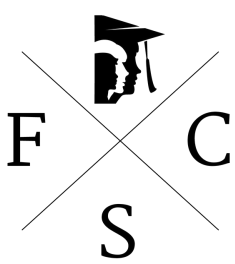
CYBERSECURITY
unboxed



FORSYTH COUNTY SCHOOLS
TECHNOLOGY SERVICES

LOCKSTEP TECHNOLOGY GROUP

CYBER.FORSYTHK12.ORG

Table of Contents

Introduction

School districts have always been a 'soft target' for cyber-attacks – largely due to shortcomings in staff, training, and security tools. That concern has only elevated in the wake of the COVID-19 pandemic, with academic institutions becoming a primary target for hacking and phishing schemes.

Why are schools a valuable focus for bad actors? Districts have lots of data, from both staff and students, and limited resources to train for and combat threats. This data can be sold on the dark web, held for ransom, or even targeted for use by terrorists.

The public education sector is a relatively rare example of a non-competitive industry – we serve well-defined geographic areas and aren't in active contention for funding. As such, FCS feels that we have a responsibility to work WITH our peers to strengthen the sector's overall cybersecurity posture. We hope you share this vision and will help spread this valuable work.

This workbook is not intended to cover every detail of cybersecurity, but to give a framework for districts to work through and learn from each other. Our desire is that every district reading this will upcycle the information, both within their own organization and with their neighbors, to make staff and student information more secure.

Much of the information within this workbook was developed through the joint work of Forsyth County Schools and Lockstep Technology Group. We have been partnering with Lockstep for more than twenty years and have the highest respect and confidence in their ability and knowledge.

This document will cover three focus areas, sixteen categories, and eighteen security domains that we feel are the foundations of a school district's cybersecurity program. A focus area, at a high level, is divided into three main parts. Although there is overlap, the three parts are **People, Process**, and **Products**. We think this overlap will be self-evident, so we did not make note of that in this workbook.

Under the three focus areas are sixteen categories. This is not to imply that there are no other areas that are not equally as important; rather, it has been our experience that these form the foundation of a comprehensive program.

The sixteen categories are:

Cybersecurity Committee, Mission, Vision, and Beliefs, Planning, Policy and Procedure, Communication, Training, Creating a Cyber Team, Asset Management, Physical Security, Patching, Data Classification, Incident Response, Firewalls, Unpack What You Own, Privacy Controls, Intrusion Detection, Prevention, and Remediation.

Security domains are areas that we check to ensure we have our fundamentals in place to provide protection against common threats and attacks. This is not to imply that if you follow

these secure domains, you will never get hacked. Rather, if you do get hacked you will have a plan in place to get your district up and running again quickly and efficiently.

If you genuinely want to keep your district 100 percent safe, we recommend unplugging from the internet and removing all electronic devices.

Figure 1: That's one way to do it.

We have included an overview of our Security Gap Assessment that Lockstep Technology Group helped us develop. It covers eighteen security domains and shows the cyber fundamentals within each domain.

The eighteen security domains are:

Asset Management, Business Continuity and Disaster Recovery, Configuration Management, Continuous Monitoring, Cryptography, Data Classification, Endpoint Security, Human Resource Security, Governance, Identification and Authentication, Incident Response, Maintenance, Network Security, Physical and Environmental Protections, Risk Management, Secure Engineering and Architecture, Security Awareness and Training, and Vulnerability and Patch Management.

Though we've broken down the key facets of an effective cybersecurity program, they all run interdependently and work best when addressed together. For many of these topics, a much more extensive explanation can be found in the '**FCSS Information Security Policies and Procedures**' document.

People

Cybersecurity Committee

It is our belief that cybersecurity is not only a technological issue, but one that affects nearly every part of district operations. If the district puts all the cybersecurity concerns solely on the technology program, then all the other departments can wash their hands of any concerns or responsibility.

However, since every department uses computers, accesses the internet, has online resources, or software, they cannot – and should not – release themselves from being part of the solution. For a cybersecurity program to be effective, every district employee must see themselves as a part of cybersecurity detection and prevention. We used this concept to layout our design of the cybersecurity committee.

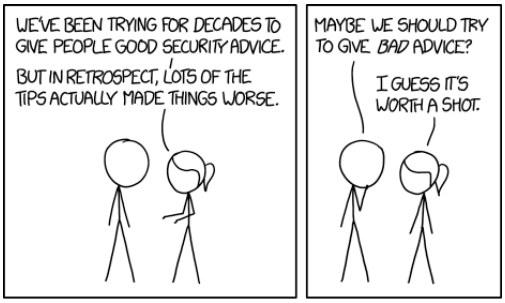


Figure 2: Hopefully your committee wouldn't approve this advice.

An effective cybersecurity committee should be comprised of decision makers from each district department and each school level. The committee should have regular meetings to discuss and understand the cyber concerns of the organization and to establish a working blueprint from which to move forward.

Meetings should be held at least quarterly, but monthly is preferred, and should focus on the district's current and future cybersecurity posture. It is imperative that the committee knows the facts, even if it paints the technology department, or any other department, in a bad light.

We recommend that the Technology Department act as a leader and expert adviser to the group but have limited voting powers. Avoid "stacking" the committee with technology personnel, else it may appear that the committee is nothing more than a rubber stamp to Technology Department initiatives. Our monthly meetings are used to discuss what cyber events have occurred since the last meeting, work performed by our cyber team, and any new people, processes, or products we feel would put our district in a better position.

For example, we brought up MFA to the committee and addressed the importance of requiring it for critical district functions. We discussed the need for it, the concerns people would have about it, and a timeline if implementation was voted on. A lot of discussion took place around

how it would affect teaching and learning for students. A particular concern was that it required people to have and use their cellphone. Many staff members did not like this and said they would not do it.

To allay staff concerns, we worked with the committee to find suitable compromises for this issue and several other noted points. After addressing the primary concerns, the committee decided on an implementation timeline and training pathways. This collaborative process helped to ensure success with far more buy-in (and far less friction) than had it simply been pushed by the Technology Department. Districts can view our cybersecurity members and meeting dates on our district cybersecurity webpage at: https://cyber.forsythk12.org

Mission, Vision, and Beliefs

First, we need to define what each of these are as they relate to cybersecurity.

Vision – is where the district cyber program is going. The goals we have for the program and where we will end up after our intentions are met.

Mission – is actionable items to achieve the cyber programs vision. It should help you establish a plan of action and move forward in its intended direction.

Beliefs – what the district believes about the program, employees, or students. These should be commonly held set of understandings that everyone can hold onto.

You may be thinking that this is just busy work to elevate your department in importance. Though promoting the work of the committee is valuable, ensuring the committee follows articulable standards is more important. Stephen Covey has done a lot of work around vision and mission, and has a great quote that emphasizes the value of having a strong foundation.

> *"If you don't set your goals based upon your Mission Statement, you may be climbing the ladder of success only to realize, when you get to the top, you are on the wrong building"*

Prior to working on cybersecurity policies and procedures for your organization, it is important to first know: **Where we are**, **where we are going**, and **what we know to be true**. You must be able to articulate this information to staff and stakeholders, else one runs the risk of losing credibility. Since there are many articles noting the importance of Vision, Mission, and Beliefs, we will not try to convince you of their significance. Districts can view our Mission, Vision, and Beliefs on our district cybersecurity webpage at: https://cyber.forsythk12.org

Planning

Those who fail to plan, plan to fail.

A truer statement cannot be used to describe the importance of planning for a cyber event. Cybersecurity has many components that, without planning, it is difficult to establish what everyone is doing or needs to do. This begins the work of designing a policy and procedure manual.

Though it will take time to prioritize the various parts of the plan for your district, the first step to protecting your digital assets is to understand what it is you're protecting. This will be discussed in more detail elsewhere in the document, just understand that this is but one part of the planning process.

Figure 3: This is not a good plan.

The planning phase of our cybersecurity program begins with our first cybersecurity committee meeting. After outlining where the district is and our current cyber concerns, we set the expectation that we cannot delay implementing critical needs. Once the committee understood the issues, we began to address the needs by criticality. It's important to share the problems EVEN if you do not have a remediation plan – inaction is not acceptable.

Policy and Procedure

The pen is mightier than the sword.

Does your district have a modern and actionable policy and procedure manual to support the operation of a safe and secure network? This need is often overlooked because it is heavy on documentation and not seen as important as a product that could be purchased. Do not underestimate the value of creating this document as it sets the tone and expectation of the entire program for all staff members.

The procedure manual lays out the steps the district will take to secure the digital experience for students and staff. It outlines the expectations for each department and each employee. Developing this is time consuming and generally does not fit the skillsets of a technology

department. Knowing this, we worked with Lockstep to helping us develop of our policy and procedure manual. Districts can view our document on our district cybersecurity webpage at: https://cyber.forsythk12.org

Communication

It is not enough for you to understand a problem – you must also be able to be able to convey that information to people without your level of technical ability. Regardless of audience – cybersecurity committee, school staff, stakeholders, or the community – communication is key. Having a clear and concise procedure manual will help ease communication.

Training

Figure 4: I bet you know of at least one 'Dave' in your organization.

You can have the most advanced firewall, best-of-breed software, and even dedicated artificial intelligence devices for cybersecurity rendered useless by the actions of one person. Without effective and ongoing training, any technology can be circumvented by careless users.

Training is often the most difficult part of an effective cybersecurity program since it involves every person in the district and is extremely time-consuming. Further, it relies on the Human Resource Department to help train all new hire employees and school leadership to afford time for their staff to take part in ongoing training.

Compounding the issue is that cyber training geared towards the needs of K-12 is limited and of varying degrees of quality. Understanding this, we worked with Lockstep to create a series of entry-level videos for cybersecurity basics. These videos are required viewing for all new employees as part of their onboarding process. Existing staff must also watch these training videos as part of their annual training requirements.

A primary part of confirming the effectiveness of this training is to expose staff to phishing campaigns. Using different bait – perhaps purporting to be from our LMS or from a cherished fast-food chain offering free food – we can gauge how well people can spot these deceptive messages. It's important that staff understand this isn't meant as a 'gotcha!'; rather, it's used to better target areas for enhanced training. We use a product through Microsoft, but there are many good products out there that will do an excellent job.

The hard part about training staff is that they are already overworked, and they do not have the time to be trained on something new. They may also see digital security as a technology issue and not a responsibility of each employee. This is a mindset that must change for districts to be secure. Districts can view our training videos on our district cybersecurity webpage at: https://cyber.forsythk12.org

Create a Cyber Team

One can have the greatest suite of tech tools available, but if there is no one to confirm/investigate the findings, those tools will never fulfill their capabilities. One should form a Cybersecurity Team to act on digital findings, even if the team is a single person.

Figure 5: Don't let this be your team.

Granted, forming a team of existing personnel can be difficult with one's already maxed out staff... and creating a new position is a near impossibility (or even filling the position should one be created) in today's environment. Nevertheless, there is no substitute for the insight and intelligence provided by humans.

If using existing staff, be sure to allow them to dedicate some part of their time to examine logs, investigate anomalies, and evaluate your current setup. Documentation – an often-overlooked part of operations – is also a critical function of a cyber team.

But how do you get the right person – or people – to be on the team? In some instances, you might only have 1-2 people on staff, so the choice may be limited. However, if one has a well-staffed department, an ideal candidate would be detail-oriented, focused, and like to solve puzzles. One can build upon this natural talent by fostering training and certifications in the cyber field.

As the team grows, communication skills begin to show their importance. The ability to convey complex situations to non-technical staff should be a key function of your cyber team.

The design we use for a cybersecurity team in Forsyth County is similar to how our network and systems teams were built: 1 engineer (this slot is yet to be approved but is on the roadmap), 1 administrator, and at least 1 support specialist.

Process

Asset Management

If you don't know what you have, how can you protect it?

When many school districts are asked what they want to protect, they will often reply with something like student and teacher data. Though that's a good answer, it is incomplete. You know WHAT you need to protect, but do you know WHERE it is located?

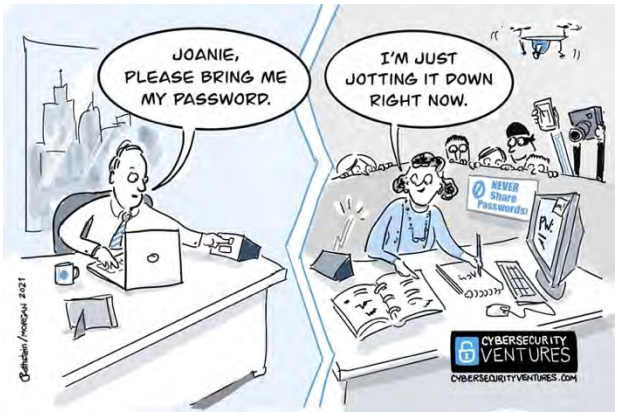
Some obvious places are their Learning Management System, Human Resource Software, or Student Information System. But is that it? Do your schools or instructional departments ever purchase software and/or programs without a security/privacy review?

FCS requires all our departments, schools, and teachers to use software that checks the privacy information of online sites and software. Based on the score it receives, it informs the user if the software meets privacy standards. This check does not take the place of an approval process; rather, it informs whether it can even be considered.

Additionally, they are required to maintain documentation of what data is stored in that resource, how it is accessed/transmitted, who has access to it, where the information is kept, and the protection measures in place to prevent unauthorized access. It is critical that this be reviewed annually.

Physical Security

Consider this: You have your home protected by the most advanced cameras, motion sensors, microphones, and pressure sensors. Would you leave your door unlocked? Of course not.



Similarly, organizations will often focus on their digital security while physical security is an afterthought. Physical security is a broad concern and touches more areas than may be initially thought.

Starting at the user level, this would cover things like ensuring they do not leave a logged-in computer unattended, they do not write their password on a sticky note and put it under their keyboard, they do not allow untrusted users (like students) to use staff devices. It includes ensuring they don't reuse/share passwords across multiple accounts and ensuring they set up MFA through a secure platform like the Microsoft Authenticator App.

Wall ports are another concern of physical security. If a bad actor comes into a school and plugs into an open port, where will they end up? Are all ports active? Do they lead to internal resources or just the internet? It is best practice to ensure that open ports are dead or a Network Access Control (NAC) solution is in place to route traffic away from internal resources and to the internet. It is also best practice to plug empty wall ports with a locking device. We use a Belden product to lock all unused ports. Each technician and school based ITS has a key to remove the locks.

Network closets are another key area of concern. All access to the closets should be limited to personnel with a demonstrable need. This has been a big push for us over the last few years and we've generally had good success with it. Keep in mind, though, when you take something away from a school that they are used to having, there is likely to be pushback.

We had many schools using these areas as storage and supply closets. Unfortunately, this generated two major concerns for us. First, it meant that nearly everyone had access to the closet. Many times, the door was propped open or simply left open for easy access, effectively negating physical security elsewhere in the building.

Second was what the schools were storing in the closets. We found weed eaters, gasoline, propane tanks, paper, and chafing dishes with fully fueled burners. This was not a good mixture with expensive electrical equipment.

Working with the schools, we decided which closets could be wholly given over to network use. On those closets, we changed the lock and secured the room. With rooms the school still needed access to, we divided them into a large locking cage that secured the network equipment but still gave them access to the room. This took significant time and money but was a critical part of our physical security.

We then worked to ensure no new building was built without dedicated locking space for MDF and IDF. Additionally, we began installing badge scanners on the MDF so we could open remotely if needed, as well as putting cameras in every closet so we could see who accessed the areas and why.

Our core datacenters were built with cameras and badge scanners, but we decided to go a step further. Beyond securing physical access to the room, each cabinet was outfitted with its own badge scanner. This allowed us to let someone into the data center and give them access to only the cabinet they needed vs every cabinet. We further secured digital access to the data centers. The data centers are on their own network that is only allowed access to from another specific network. So, it stops anyone outside of the access network from ever accessing the data center.

Patching

Behind phishing attacks, unpatched systems are the second-greatest threat to your system's cybersecurity posture. Some vendors – like Microsoft – have regular patch release schedules, while others may only release patches as the need arises.

Regardless of the release schedule, it is critical that you have a defined patching program AND stick to it. Indeed, patching is so critical that it is a core part of the security scoring models from software such as Tenable's Nessus and services like FortifyData and BitSight.

Figure 6: Patch ALL the things.

Many districts focus on patching their servers – which needs to be done – but it is just as important (if not more so) to update client devices (laptops/desktops, smartphones, tablets, IoT devices, security cameras, VoIP systems, copiers, etc.) as those are common attack vectors.

A potential hang-up, though, is that these patches can sometimes have a negative impact on custom and/or third-party applications that have dependencies that get patched. Be sure to work with stakeholders to address these potential incompatibilities so that a proper patch cadence can be supported.

Understanding the need to patch is one thing… but doing it is quite another. If your organization is anything like Forsyth County Schools, it can be difficult to find time when it is convenient to patch without disrupting operations or activities. With that in mind, it is critical that one gets district-level support for the patching routine. Once approval has been given, be sure to post a patching schedule and send periodic reminders to stakeholders to ensure they understand the impact.

Data Classification

Not all information is created equal – some is suitable for public access while others contain sensitive operational data or personal details. To ensure that information is properly handled, it is important that an organization implements a data classification framework. Doing so protects a district's data from unauthorized disclosure, regardless of whether it is being transmitted or stored.

Safeguards must be in place to protect confidentiality, integrity, and availability of data. These directives should be created in accordance with applicable statutory, regulatory, and contractual requirements. This includes categories such as student and employee personal data, financial, public relations and marketing information, network and infrastructure, and operations.

Incident Response

So, you've had a breach. Now what? The steps you take next can help mitigate the issue... or worsen it. That's why it is imperative that you have an incident response plan. This plan needs to be clear and understood by all stakeholders.

In short, one needs to understand how to communicate findings, assess damage, assign criticality, gather evidence, remediate the issue, share information securely, notify stakeholders, and close the incident. These are all important steps and should not be minimized to hasten closure and/or to hide the information.

A detailed explanation can be seen in Section 15.0 of the 'FCSS Information Security Policies and Procedures' document on cyber.forsythk12.org.

Product

Firewalls

If any product were to fall into a "Good - I already have that!" category, a firewall would be it. But it's not enough to own a firewall – you need to know how to configure it for proper operation, maintain it, evaluate and understand the logs it generates, and how to remediate issues it detects.

Unfortunately, these skills can sometimes be difficult to come by in a small network environment. Indeed, even large organizations are having trouble finding competent firewall engineers in today's challenging job market. This is where a trusted vendor and/or having a close relationship with a 'sister' school district can pay dividends.

Additionally, how capable is your firewall? What sort of work is it already configured to do? Can it handle decryption for server traffic? Client traffic? How many network interfaces does it have? Can you physically and logically separate different networks? Can it log specific user activity on the network? These are but a few areas of concern for sizing and configuring your firewall.

But your core firewall is not the only one you can take advantage of. Most likely, your primary client and server operating systems also have their own firewall. Don't underestimate its value – it can be an excellent line of defense against malware and intrusions. Indeed, in penetration tests conducted on the FCS network, the OS-based firewall prevented lateral movement on both server and client networks.

The key is defining an application baseline on your devices and being stringent about what is allowed beyond that.

Unpack What You Own

Most – though not all – school districts fall into one of two camps for their identity provider (IdP): Microsoft or Google. If your school district is using one of those as a paid tenant, there are a myriad of security tools available that can provide protection and remediation, as well as comprehensive logging.

Knowing, and using, what you already own can be the first, best step to building your district's cybersecurity framework. For instance, FCS purchases A5 licenses from Microsoft for all staff (and students). This level of product from Microsoft combines many tools that interoperate to provide a comprehensive security barrier and management system. Find out what your provider offers for you.

Georgia schools are also blessed to be supported by a couple of products supplied by the Georgia Department of Education (GaDOE). GaDOE currently provides both a service to analyze

a district's external exposure to cyber risk and one that supplies high-fidelity phishing campaign and training tools.

The first – BitSight – monitors a district's externally facing assets and assesses them for a multitude of vulnerabilities. This information is presented in an easy-to-understand format and provides actionable intelligence for remediation.

KnowBe4, the second product provided by GaDOE, is an industry leader in phishing awareness and training tools. Though it has yet to be fully implemented across the state, many districts already use this product in their organizations.

In short, it is important to understand the products you already own – or discover what may be available from your supporting organizations – so that you can maximize your assets.

Intrusion Detection, Prevention, and Remediation

Your internet-facing assets are under constant bombardment, right? But how do you know? And how do you react? If you don't have hardware and/or software that'll detect these attacks, you're working in the blind.

Most modern firewalls include at least two of the three – intrusion detection and intrusion prevention. The key, though, is to ensure these options are properly configured. If your team lacks the necessary experience to do so, it is well worth the time and money to have a trusted partner/vendor to aid in this task.

Intrusion remediation, though, can be a more difficult hill to climb. Since the type of remediation will depend on the attack, there's no one-size-fits-all solution. What if an account is compromised? Or a server? What about a DDoS attack? Malware on a client computer? These are all likely attack vectors but resolving them requires different tactics.

The time to determine basic remediation steps is BEFORE the event occurs, else one runs the risk of not properly addressing the issue. As noted in the Cyber Team section, documentation is critical to the process – it ensures a consistent response, and that knowledge isn't siloed.

Assessment

Maturity Gap Assessment

A maturity gap assessment is used to help districts figure out where they stand in their cybersecurity journey and find their strengths and weaknesses. There are many other areas you can address, but this allows us to focus on the most critical ones. The areas are as follows:

Asset Management

Ensure the confidentiality of a district's data through implementing asset management and tracking tools and practices to protect systems and data.

Districts have mechanisms in place to:

1. facilitate an IT asset management program to implement and manage asset management controls.
2. identify and involve pertinent stakeholders of critical systems, applications, and services to support the ongoing secure management of these assets.
3. assign asset ownership responsibilities to a department, team, or individual that establishes a mutual understanding of requirements to protect assets.
4. include capturing the name, position, and role of individuals responsible for administering assets as part of the asset inventory process.

Business Continuity and Disaster Recovery

Ensure a district's primary core functions have the necessary steps to continue operations and recover data in case of a disaster or breach.

Districts have mechanisms in place to:

1. identify and document the critical systems, applications and services that support essential missions and business functions.
2. create recurring backups of data, software, and systems images to ensure availability of data.
3. prevent the unauthorized disclosure and modification of backup information.
4. utilize sampling of available backups to test recovery capabilities as part of contingency plan testing.

Configuration Management

Ensure secure configuration of a district's assets through implementing best practices to protect systems and data.

1. Automated mechanisms exist to prevent the execution of unauthorized software programs.
2. Mechanisms exist to whitelist or blacklist applications in an order to limit what is authorized to execute.
3. Mechanisms exist to restrict the ability of nonprivileged users to install software.

4. Mechanisms exist to configure systems to generate an alert when an authorized installation of software is detected.

Continuous Monitoring

Ensure that a district uses automated mechanisms to analyze network traffic to detect covert data exfiltration.

1. Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.

Cryptography

Ensure the confidentiality of a district's data through implementing appropriate cryptographic technologies to protect systems and data.

Districts have mechanisms in place to:

1. facilitate the implementation of cryptographic protections controls using known public standards and trusted technologies.
2. protect the confidentiality of data being transmitted.
3. protect the integrity of data being transmitted.
4. unauthorized disclosure of information at rest.
5. confidentiality and integrity of information being stored on storage media.
6. database servers utilize encryption to protect their databases.
7. confidentiality and integrity of non-console administrative access.
8. protect wireless access via secure authentication and encryption.
9. securely implement an internal Public Key Infrastructure or obtain PKI services through a provider.

Endpoint Security

Ensure that endpoint devices are appropriately protected from reasonable threats to the confidentiality, integrity, availability, and safety of devices and its data.

Districts have mechanisms in place to:

1. facilitate the implementation of endpoint security controls.
2. utilize antimalware technologies to detect and eradicate malicious code.

Human Resource Security

Ensure a district life cycle management of all accounts from the time of onboarding to the end of employment are effective in securing all employees data.

Districts have mechanisms in place to:

1. define cybersecurity responsibilities for all personnel.
2. communicate with users about their roles and responsibilities to maintain a safe and secure working environment.

3. automatically notify Identity and Access Management personnel or roles upon termination of an individual employment or contract.

Governance

Ensure the development, proactive management, and ongoing review of a district's security and privacy program.

1. Mechanisms exist to define the context of a district's business model and document the mission of an organization.

Identification and Authentication

Implement the concept of "least privilege" through limiting access to a district's systems and data to authorized users only.

Districts have mechanisms in place to:

1. uniquely identify and centrally Authenticate, Authorize, and Audit a district's users and processes.
2. automatically enforce multifactor Authentication (MFA) for all employees, remote network access, third-party systems, applications, and services. Non-console access to critical systems that store, transmit, or process data.
3. manage privileged accounts to identify the account as a privileged user or service.
4. securely manage authenticated users and devices.
5. to enforce complexity, length, and lifespan considerations to ensure strong criteria for password-based authentication.
6. to protect and store passwords via a password manager tool.
7. disable accounts immediately upon notification for users posing a risk to the district.
8. review all system accounts and disable any account that cannot be associated with a business process or owner.
9. periodically review the privileges assigned to users to validate the need for such privileges; reassign or remove privileges, if necessary, to correctly reflect a district's mission and needs.
10. prohibit privileged users from using privileged accounts while performing security functions.
11. prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards and countermeasures.
12. prevent applications from executing at higher privilege levels than the user's privileges.
13. enforce a limit for consecutive invalid login attempts by a user during a defined time period and automatically locks the account when the maximum unsuccessful attempts are exceeded.
14. initiate a session lock after a district's defined time period of inactivity.

Incident Response

Establish and maintain a capability to guide a district's response when security related incidents occur.

Districts have mechanisms in place to:

1. define specific indicators of compromise and identify the signs of potential cyber related events.
2. address data breaches or incidents involving the unauthorized disclosure of sensitive or regulated data.

Maintenance

Ensure due diligence is performed by properly maintaining a district's assets across the enterprise.

Districts have mechanisms in place to:

1. have spare parts and/or maintenance support for systems that are business critical.
2. perform preventative maintenance on critical systems, applications, and services.

Network Security

Ensure sufficient security controls are in place to protect the confidentiality and integrity of a district communications.

Districts have mechanisms in place to:

1. monitor and control communications at the external network boundary and at key internal boundaries within the network.
2. limits network access points.
3. prevents the public disclosure of internal network information.
4. designs, implements, and reviews firewall and router configurations to restrict connections between untrusted networks and internal systems.
5. configures firewall and router to deny network traffic by default and allow network traffic by exception.
6. enforces the use of human reviews for Access Controls Lists (ACL) and similar rulesets on a routine basis.
7. logically and physically segment information flows to accomplish network segmentation.
8. implements security management subnets to isolate security tools and support components from other internal systems by implementing separate subnetworks with managed interfaces to other components of the system.
9. enable Virtual Local Area Networks (VLAN) to limit the ability of devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.
10. defines, controls, and reviews organization approved secure remote access methods.
11. use cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions (VPN).

12. routes all remote accesses through managed network control points.
13. restricts the execution of privileged command and access to security relevant information via remote access only for compelling operational needs.

Physical and Environmental Protections
Minimize risk to district's systems and data by addressing applicable physical security and environmental concerns.

1. Physical security mechanisms exist to allow only authorized personnel access to secure areas.

Risk Management
Ensure that cybersecurity related risk is visible to and understood by the business unit that owns the assets or processes.

Districts have mechanisms in place to:

1. prioritize the impact level for systems, application, and services to prevent disruptions.
2. identify and document risks from internal and external threats.
3. remediate risks to an acceptable level.
4. conduct Business Impact Analysis (BIA).

Secure Engineering and Architecture
To align cybersecurity decisions with the districts architectural strategy and industry recognized secure practices.

Districts have mechanisms in place to:

1. partition systems so that partitions reside in separate physical domains or environments.
2. separate user functionality from system management functionality.

Security Awareness and Training
Develop a security and privacy minded district.

1. Mechanisms exist to provide all employees and contractors with appropriate cyber awareness education and training that is relevant to their job function.

Vulnerability and Patch Management
Proactively manage the risks associated with technical vulnerability management.

Districts have mechanisms in place to:

1. facilitate the implementation and monitoring of vulnerability management controls.
2. ensure that vulnerabilities are properly identified, tracked, and remediated.
3. conduct software patching for deployed operating systems, applications, and firmware.

4. perform quarterly external vulnerability scans outside the network inward via a reputable service provider. Rescans should be continued until passing results are obtained and all high vulnerabilities are resolved.
5. perform quarterly internal scans, that include all segments of the internal network, as well as rescans until passing results and all high vulnerabilities are resolved.

Reference Guide

CyberForsyth - https://cyber.forsythk12.org/

Cybersecurity Committee - https://cyber.forsythk12.org/?page_id=28

Board Policy - https://cyber.forsythk12.org/?page_id=61

Mission, Vision, and Beliefs - https://cyber.forsythk12.org/?page_id=1047

Policy and Procedure Manual - https://cyber.forsythk12.org/?page_id=631

Training Resources - https://cyber.forsythk12.org/?page_id=63

Student Privacy Resources - https://cyber.forsythk12.org/?page_id=1000

Data Classification and Handling Guidelines - https://cyber.forsythk12.org/?page_id=626