FORSYTH COUNTY SCHOOLS

CYBER SECURITY

TECHNOLOGY SERVICES

Table of Contents

Security Measures

First

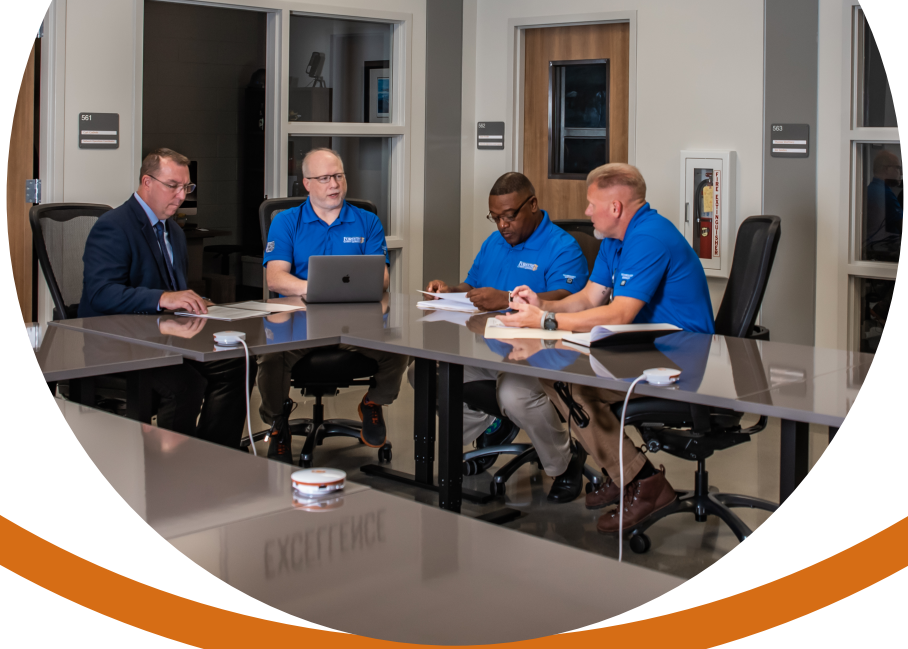
- Cybersecurity Committee
-Vision, Mission & Beliefs
-Planning, Policy & Procedure
-Communication
-Training
-Createa Cyber Team

Second

- Asset Management
-Physical Security
-Patching
-Data Classification
-Incident Response

Third

- Firewalls
-Unpack What You Own
-Intrusion Detection, Prevention & Remediation



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.

FCS feels that we have a responsibility to work WITH our peers to strengthen the sector's overall cybersecurity posture.

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. 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.

Although we have broken down the key facets of an effective cybersecurity program in this workbook, 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 "FCS Information Security Policies and Procedures" document.

Introduction

Focus Areas

- People
- Process
- Product

18 Security Domains

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

16 Categories

- Cybersecurity Committee
- Mission, Vision & Beliefs
- Planning
- Policy & 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 & Remediation

People

Cybersecurity Committee

It is our belief that cybersecurity is not only a technical issue, but one that affects nearly every part of district operations. 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, all district employees must see themselves as a part of the cybersecurity detection and prevention. We used this concept to layout our design of the cybersecurity committee.

An effective cybersecurity committee should be comprised of decision makers from each district department and each school level. They 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. They should meet at least quarterly but monthly is preferred.

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 cellphones. 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.

View our cybersecurity members and meetings dates on our district cybersecurity webpage:
https://cyber.forsythk12.org

Vision Mission & Beliefs

Vision

A secure digital environment for all Forsyth County Schools students and staff.

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

To provide adaptable, modern governance to support the use, operation, and maintenance of the district's digital information systems

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

- *All students and staff should have a secure digital experience.*
- *Cybersecurity is a district concern, not only a technology concern.*
- *A cohesive response is necessary for the security and safety of our organization.*
- *All FCS students and staff are the first, best line of defense against cyber threats.*
- *Regular training is an effective tool against cyber threats.*
- *Cyber risk is an ever-evolving landscape that requires ever-evolving guidance.*
- *Stakeholders should be informed about cyber risks so that appropriate decisions can be made.*

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

Key Findings & Recommendations

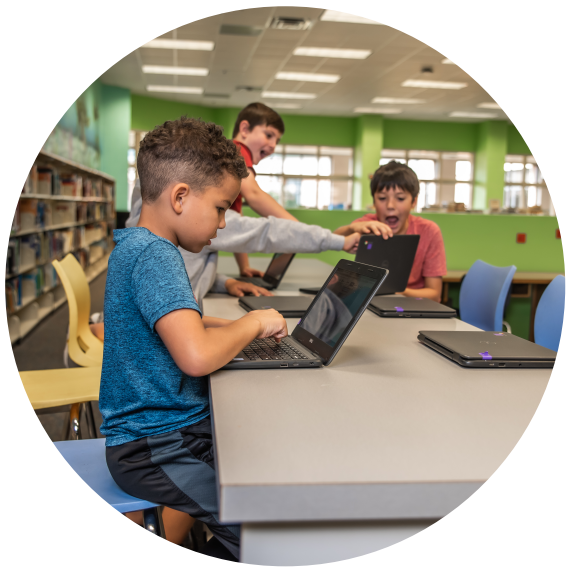
Planning

Cybersecurity has many components that, without planning, can make it difficult to establish what everyone is doing or needs to do. This begins the work of designing a policy and procedure manual. Although 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.

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 addressing 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 & Procedure

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. Using outside help may be a good use of funds. You can view our document at: https://cyber.forsythk12.org



Communication

It is not enough for you to understand a problem, you must 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 ease communication.

Training

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 Resources Department to help train all newly hired employees and school leadership to afford time for their staff to take part in ongoing training. We created a series of entry-level videos for cybersecurity basics that are required viewing for new hires and annual training for existing staff.

A primary part of confirming the effectiveness of this training is to expose staff to phishing campaigns. Using different bait we can gauge how well people can spot these deceptive messages. In the last year at FCS, Microsoft Defender has detected and removed approximately 3 million emails using advanced anti-spam, impersonation, phishing and spoofing protections.

Create a Cyber Team

Districts should form a Cybersecurity Team to act on alerts and discoveries. If using existing staff, be sure to allow them to dedicate part of their time to examine logs, investigate anomalies, and evaluate your current setup. Documentation is also a critical part of a cyber team. An ideal team is detail-oriented, focused, likes to solve puzzles , and can convey complex situations to non-technical staff.

At FCS our cyber team is set up similar to our network and systems teams: 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

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 the privacy standards. The approval process still takes place too. They are also 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.

Physical Security

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

Reminders for Physical Security:

- Never leave a logged in computer unattended
- Do not write passwords down
- Do not allow untrusted users (such as students) to use staff devices
- Have MFA set up
- Make sure open wall ports are dead or a NAC solution is in place
- Access to network closets should be limited
    - Here at FCS we have designated closets that are for network use only.
    - We have badge scanners on the MDF so they can be opened remotely if needed.
    - Cameras are in every closet to see who is accessing the areas and why.
    - Core datacenters were built with cameras and badge scanners and each cabinet has its own badge scanner as well. This allows us to let employees into the data center and give them access to only the cabinet that they need vs every cabinet.
    - Data centers are on their own network to stop 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. It is critical that you have a defined patching program AND stick to it.

Many districts focus on patching their servers- which needs to be done- but it is just as important to update client devices as those are common attack vectors. 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.

It is critical that one gets district-level support for the patching routine. Once approved be sure to post a patching schedule and send periodic reminders to stakeholders to ensure they understand the impact.

FCS has had over 900 patches applied to servers in the last year with over 80 being critical.

Data Classification

To ensure that information is properly handled, it is important that an organization implements a data classification framework. Doing so protects the 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.

Categories include:
- Student and employee personal data
- Financial
- Public relations and marketing information
- Network and infrastructure operations

Incident Reponse

It is imperative that you have an incident response plan in place in case of a breach. The plan needs to be clear and understood by all stakeholders.

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.

Product

Firewalls

It's not enough just having 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. These are skills that are hard to come by and this is where a trusted vendor and/or a close relationship with a "sister" school district can pay dividends.

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. They can be excellent lines 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 school districts use Microsoft or Google for their identity provider. If your school district is using one of those as a paid tenant, there are a myriad of security tools variable that can provide protection and remediation, as well as comprehensive logging. FCS uses A5 license 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 blessed to be supported by a couple of products supplied by the Georgia Department of Education. They provide both a service to analyze a district's external exposure to cyber risk and one that supplies high-fidelity phishing campaign and training tools.

Intrusion Detection, Prevention & Remediation

Most modern firewalls include intrusion detection and intrusion prevention. The key 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 will depend on the attack. For example, all vector attacks, such as an account being compromised, a server being compromised, a DDoS attack or a malware on a client computer all require different tactics to resolve them. The time to determine basic remediation steps is BEFORE the event occurs.

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 that can address, but this allows us to focus on the most critical ones.

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 should have mechanisms in place to:

- Facilitate an IT asset management program to implement and manage asset management controls.
- Identify and involve pertinent stakeholders of critical systems, applications, and services to support the ongoing secure management of these assets.
- Assign asset ownership responsibilities to a department, team, or individual that establishes a mutual understanding of requirements
to protect assets.
- Include capturing the name, position, and role of individuals responsible for administering assets as part of the asset inventory process.

Business Continuity & 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 should have mechanisms in place to:

- Identify and document the critical systems, applications and services that support essential missions and business functions.
- Create recurring backups of data, software and system images to ensure the availability of data.
- Prevent the unauthorized disclosure and modification of backup information.
- 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.

- Automated mechanisms exist to prevent the execution of unauthorized software programs.
- Mechanisms exist to whitelist or blacklist applications in order to limit what is authorized to execute.
- Mechanisms exist to restrict the ability of nonprivileged users to install software.
- 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. Districts have mechanisms in place 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 should have mechanisms in place to:

- Facilitate the implementation of cryptographic protection controls using known public standards and trusted technologies.
- Protect the confidentiality of data being transmitted.
- Protect the integrity of data being transmitted.
- Unauthorized disclosure of information at rest.
- Confidentiality and integrity of information being stored on storage media.
- Database servers utilize encryption to protect their databases.
- Confidentiality and integrity of non-console administrative access.
- Protect wireless access via secure authentication and encryption.
- Securely implement an internal Public Key Infrastructure or obtain PKI services through a provider.

Endpoint Security

Ensure endpoint devices are appropriately protected from reasonable threats to the confidentiality, integrity, availability, and safety of devices and its data. Districts should have mechanisms in place to:

- Facilitate the implementation of endpoint security controls.
- 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 employee's data. Districts should have mechanisms in place to:

- Define cybersecurity responsibilities for all personnel.
- Communicate with users about their roles and responsibilities to maintain a safe and secure working environment.
- Automatically notify Identity and Access Management personnel upon termination of an individual's employment or contract.

Governance

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

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

Identification & Authentication

Implement the concept of "least privilege" through limiting access to a district's systems and data to authorize users only. Districts should have mechanisms in place to:

- Uniquely identify and centrally Authenticate, Authorize, and Audit a district's users and processes.
- Automatically enforce 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.
- Manage privileged accounts to identify the account as a privileged user or service.
- Securely manage authenticated users and devices.
- To enforce complexity, length, and lifespan considerations to ensure strong criteria for password-based authentication.
- To protect and store passwords via a password manager tool.
- Disable accounts immediately upon notification for users posing a risk to the district.
- Review all system accounts and disable any account that cannot be associated with a business process or owner.
- 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.
- Prohibit privileged users from using privileged accounts while performing security functions.
- Prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards and countermeasures.
- Prevent applications from executing at higher privilege levels than the user's privileges.
- Enforce a limit for consecutive invalid login attempts by a user during a defined time period and automatically lock the account when the maximum unsuccessful attempts are exceeded.
- 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 should have mechanisms in place to:

- Define specific indicators of compromise and identify the signs of potential cyber related events.
- Address data breaches or incidents involving the unauthorized disclosure of sensitive or regulated data.

Maintenance

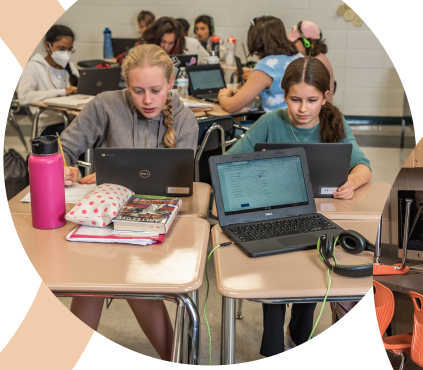
Ensure due diligence is performed by properly maintaining a district's assets across the enterprise. Districts should have mechanisms in place to:

- Have spare parts and/or maintenance support for systems that are business critical.
- 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 district communications. Districts should have mechanisms in place to:

- Monitor and control communications at the external network boundary and at key internal boundaries within the network.
- Limits network access points.
- Prevents the public disclosure of internal network information.
- Designs, implements, and reviews firewall and route configurations to restrict connections between untrusted networks and internal systems.
- Configures firewall and router to deny network traffic by default and allow network traffic by exception.
- Enforces the use of human reviews for Access Controls Lists and similar rulesets on a routine basis.
- Logically and physically segment information flows to accomplish network segmentation.
- 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.
- 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.
- Defines, controls, and reviews organization approved secure remote access methods.
- Use cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions (VPN).
- Routes all remote accessed through managed network control points.
- Restricts the execution of privileged command and access to security relevant information via remote access only for compelling operational needs.



Physical & Environmental Protections

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

- 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 should have mechanisms in place to:

- Prioritize the impact level for systems, application, and services to prevent disruptions.
- Identify and document risks from internal and external threats.
- Remediate risks to an acceptable level.
- Conduct Business Impact Analysis (BIA).

Secure Engineering & Architechture

To align cybersecurity decisions with the districts' architectural strategy and industry recognized secure practices. Districts should have mechanisms in place to:

- Partition systems so that partitions reside in separate physical domains or environments.
- Separate user functionality from system management functionality.

Security Awareness & Training

Develop a security and privacy minded district:

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

Vulnerability & Patch Management

Proactively manage the risks associated with technical vulnerability management controls. Districts should have mechanism in place to:

- Facilitate the implementation and monitoring of vulnerability management controls.
- Ensure that vulnerabilities are properly identified, tracked, and remediated.
- Conduct software patching for deployed operating systems, applications, and firmware.
- 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.
- 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.

Contact

770-887-2461

1140 Dahlonega Highway
Cumming, GA 30040

tech@forsyth.k12.ga.us

cyber.forsythk12.org