Voorhees Township School District

Cyber Security Defense Gap Analysis

Planning tool for hardening organizational cyber security posture

Department of Technology

Revised
02-11-2026

Introduction to CIS Controls

The CIS Controls® started as a simple grassroots activity to identify the most common and important real-world cyber-attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive action for defenders, and then share that information with a wider audience. The original goals were modest—to help people and enterprises focus their attention and get started on the most important steps to defend themselves from the attacks that really mattered.

Led by the **Center for Internet Security® (CIS®)**, the CIS Controls have matured into an international community of volunteer individuals and institutions that:

- Share insights into attacks and attackers, identify root causes, and translate that into classes of defensive action
- Create and share tools, working aids, and stories of adoption and problem-solving
- Map the CIS Controls to regulatory and compliance frameworks in order to ensure alignment and bring collective priority and focus to them
- Identify common problems and barriers (like initial assessment and implementation roadmaps), and solve them as a community

The CIS Controls reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.), who have banded together to create, adopt, and support the CIS Controls.

Evolution of the CIS Controls

The CIS Controls started like many similar activities; experts were gathered together, and shared and argued until they reached an agreement. This can be very valuable, depending on the people at the table and their experience. Through documenting and sharing the output, all enterprises can benefit from the work of people they cannot hire or even meet. You can improve the outcome (and your confidence in it) through selecting experts that represent a wide range of knowledge, bringing consistency to the process, and ensuring use of the best-available information (especially about attacks). In the end, you are still depending on the good judgment of a relatively small group of people, captured in an informal and narrative way.

CIS has been on a multi-year path to bring more data, rigor, and transparency to the process of best practice recommendations (the CIS Benchmarks™ and the CIS Controls). All of these elements are essential to the maturation of a science to underlie cyber defense; and, all are necessary to allow the tailoring and "negotiation" of security actions applicable in specific cases, and as required through specific security frameworks, regulations, and similar oversight schemes.

In the earliest versions of the CIS Controls, a standard list of publicly known attacks were used as a simple and informal test of the usefulness of specific recommendations. Starting in 2013, CIS worked with the Verizon Data Breach Investigations Report (DBIR) team to map the results of their large-scale data analysis directly to the CIS Controls, as a way to match their summaries of attacks into a standard program for

defensive improvement.

CIS has recently released the Community Defense Model (CDM), which is their most data-driven approach so far. In its initial version, the CDM looks at the conclusions from the most recent Verizon DBIR, along with data from the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), to identify what we believe to be the five most important types of attacks. We describe those attacks using the MITRE Adversarial Tactics, Techniques, and Common Knowledge® (MITRE ATT&CK®) Framework in order to create attack patterns (or specific combinations of Tactics and Techniques used in those attacks). This allows us to analyze the value of individual defensive actions (i.e., Safeguards1) against those attacks. Specifically, it also provides a consistent and explainable way to look at the security value of a given set of defensive actions across the attacker's life cycle, and provide a basis for strategies like defense- in-depth. The details of this analysis are available on the CIS website. The bottom line is that they have taken a major step towards identifying the security value of the CIS Controls, or any subset of them. While these ideas are still evolving, CIS is committed to the idea of security recommendations based on data, presented transparently. For additional information, reference https://www.cisecurity.org/ controls/v8/ .

These activities ensure that the CIS Security Best Practices (which include the CIS Controls and CIS Benchmarks) are more than a checklist of "good things to do," or "things that could help"; instead, they are a prescriptive, prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and in alignment with all industry or government security requirements.

Version 8.0 of the CIS Controls

When CIS begin the work of a new version, they sat down to establish "design principles" that will be used to guide the process. These serve as a decision "touchstone" to remind us of what is really important, and of the goals of the CIS Controls. While these have been fairly consistent since the earliest versions of the CIS Controls, we have been refining our thinking over the last couple of versions to focus on the role that the CIS Controls play in the total picture of enterprise security.
Our design principles include:

- **Offense Informs Defense**
  - CIS Controls are selected, dropped, and prioritized based on data, and on specific knowledge of attacker behavior and how to stop it
- **Focus**
  - Help defenders identify the most critical things they need to do to stop the most important attacks
  - Avoid being tempted to solve every security problem—avoid adding "good things to do" or "things you could do"
- **Feasible**
  - All individual recommendations (Safeguards) must be specific and practical to implement
- **Measurable**
  - All CIS Controls, especially for Implementation Group 1, must be measurable
  - Simplify or remove ambiguous language to avoid inconsistent interpretation
  - Some Safeguards may have a threshold

- **Align**
    - Create and demonstrate "peaceful co-existence" with other governance, regulatory, process management schemes, framework, and structures
    - Cooperate with and point to existing, independent standards and security recommendations where they exist, e.g., National Institute of Standards and Technology® (NIST®), Cloud Security Alliance (CSA), Software Assurance Forum for Excellence in Code (SAFECode), ATT&CK, Open Web Application Security Project® (OWASP®)

In addition, since Version 7, we have all seen significant changes in technology and the cybersecurity ecosystem. Movement to cloud-based computing, virtualization, mobility, outsourcing, Work-from-Home, and changing attacker tactics have been central in every discussion. Physical devices, fixed boundaries, and discrete islands of security implementation are less important, and so we reflect that in Version 8, through revised terminology and grouping of Safeguards. Also, to guide adopters in implementing Version 8, CIS created a glossary to remove ambiguity of terminology. Some ideas have been combined or grouped differently to more naturally reflect the evolution of technology, rather than how enterprise teams or responsibilities might be organized, and always referring back to our guiding principles.

The text of the CIS Controls document is just one step of a process to design, implement, measure, report, and manage enterprise security. Taking this entire work stream into account in the CIS Controls, we can support the total enterprise management process through: making sure that each Safeguard asks for "one thing," wherever possible, in a way that is clear and requires minimal interpretation; that we focus on measurable actions, and define the measurement as part of the process; and, that we simplify the language to avoid duplication.

CIS has always tried to be very conscious of the balance between addressing current topics and the stability of an overall defensive improvement program. We have always tried to focus on the foundations of good cyber defense—and, always tried to keep our eyes on emerging new defensive technology—while avoiding the "shiny new toys" or complex technology that is out of reach for most enterprises.

The NIST Framework for Improving Critical Infrastructure Cybersecurity

Since its release in February 2014, The **NIST *Framework for Improving Critical Infrastructure Cybersecurity*** has become a major part of the national conversation about cybersecurity for the critical infrastructure (and beyond), and we believe it represents an important step towards large-scale and specific improvements in security for the United States and internationally. The Center for Internet Security was an active participant in the development of the Framework, and the CIS Critical Security Controls are called out as one of the "Informative References" that can be used to drive specific implementation.

The Framework is true to its name – "a set of principles, ideas, etc. that you use when you are forming your decisions and judgments" (from the MacMillan Dictionary) – and it provides a way to organize, conduct, and drive the conversation about security goals and improvements, for individual enterprises and across communities of enterprises. But it does not include any specific risk management process, or specify any priority of action. Those "decisions and judgments" are left to the adopter to manage for their specific situation and context. For additional information, go to < **https://www.nist.gov/cyberframework**>

We believe that for the vast majority of enterprises, the best approach to solving these problems is to tackle them as a community – not enterprise-by-enterprise. This is the essence of the CIS non-profit community model, and is embodied in projects like the CIS Critical Security Controls, the CIS Security Configuration Benchmarks, and the National Cyber Hygiene Campaign. We need to band together to identify key actions, create information, share tools, and remove barriers so that we can all succeed.

In that spirit the Center for Internet Security will continue to support the evolution of the Framework, and also help our community leverage the content, processes, and priorities of the CIS Critical Security Controls as an action mechanism in alignment with the NIST Cybersecurity Framework.

	NIST Cybersecurity Framework (CSF) Core				
CIS Critical Security Controls (V8.0)	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
CSC 1: Inventory and Control of Enterprise Assets	2	0	2	1	0
CSC 2: Inventory and Control of Software Assets	2	2	1	1	0
CSC 3: Data Protection	4	9	1	0	0
CSC 4: Secure Configuration of Enterprise Assets and Software	0	11	0	1	0
CSC 5: Account Management	2	3	0	1	0
CSC 6: Access Control Management	1	7	0	0	0
CSC 7: Continuous Vulnerability Management	2	3	0	2	0
CSC 8: Audit Log Management	0	4	8	0	0
CSC 9: Email and Web Browser Protections	0	7	0	0	0
CSC 10: Malware Defenses	0	5	2	0	0
CSC 11: Data Recovery	0	1	0	0	4
CSC 12: Network Infrastructure Management	1	7	0	0	0
CSC 13: Network Monitoring and Defense	0	6	5	0	0

CSC 14: Security Awareness and Skills Training	0	9	0	0	0
CSC 15: Service Provider Management	4	2	1	0	0
CSC 16: Application Software Security	0	14	0	0	0
CSC 17: Incident Response Management	0	0	0	6	3
CSC 18: Penetration Testing	3	2	0	0	0

**NIST Security Functions associated with each CIS Critical Security Control*

The true power of the CIS Controls is not about creating the best list, it is about harnessing the experience of a community of individuals and enterprises to actually make security improvements through the sharing of ideas, tools, lessons, and collective action. To support this, CIS acts as a catalyst and clearinghouse to help us all learn from each other. Since Version 6, there has been an explosion of complementary information, products, and services available from CIS, and from the industry-at-large. Please contact CIS for the following kinds of working aids and other support materials, https://www.cisecurity.org/controls/v8/ .

Using or Transitioning from Prior Versions of the CIS Controls

CIS Controls Implementation Groups (IGs)

Historically, the CIS Controls were ordered in sequence to focus an enterprise's cybersecurity activities, with a subset of the first six CIS Controls referred to as "cyber hygiene." However, this proved to be too simplistic. Enterprises, especially small ones, could struggle with some of the early Safeguards and never get around to implementing later CIS Controls (for example, having a backup strategy to help recover from ransomware). As a result, starting with Version 7.1, CIS created CIS Controls Implementation Groups (IGs) as the recommended new guidance to prioritize implementation.

The CIS Controls IGs are self-assessed categories for enterprises. Each IG identifies a subset of the CIS Controls that the community has broadly assessed to be applicable for an enterprise with a similar risk profile and resources to strive to implement. These IGs represent a horizontal look across the CIS Controls tailored to different types of enterprises. Specifically, we have defined IG1 as "basic cyber hygiene," the foundational set of cyber defense Safeguards that every enterprise should apply to guard against the most common attacks (https://www.cisecurity.org/controls/v8/). Each IG then builds upon the previous one: IG2 includes IG1, and IG3 includes all CIS Safeguards in IG1 and IG2.

CIS Controls Implementation Groups (IGs)

IG1

An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.

Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off- the-shelf (COTS) hardware and software.

IG2 (Includes IG1)

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.

Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

IG3 (Includes IG1 and IG2)

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

Voorhees Township School District Implementation of CIS Critical Security Controls (V8.0)

The CIS Critical Security Controls are a relatively small number of prioritized, well-vetted, and supported security actions that the district has taken to assess and improve our current security state. This is not a one-size-fits-all solution, in either content or priority - we must understand what is critical to our organization, data, systems, networks, and infrastructures, and we must consider the adversary actions that could impact our ability to be successful in our programs and/or operations. Even a relatively small number of Controls cannot be executed all at once, so we are using them to develop a plan for assessment, implementation, and process management. This document marks the district's transition from version 6.1 to version 8.0 of the CIS Controls.

The Controls were developed based on specific knowledge of the threat environment as well as the current technologies in the marketplace upon which our communications and data rely. One of the key benefits of the Controls is that they are not static; they are updated regularly and are tailored to address the security issues of the day. This version of the Controls reflects deliberation and consideration to ensure that every control and sub-control is accurate, essential, concise and relevant.

Each of the Critical Security Controls (CSC) is presented on the following pages providing all associated CSC Sub-Control identifiers with a thorough description, identified asset type, CIS Implementation Group rating, and NIST Cybersecurity Framework Core Security Function(s). Tools currently available to the district's IT department for addressing each Sub-Control are listed, and our process for meeting the required task(s) for each is described.

CIS Critical Security Controls – Voorhees Township School District Gap Analysis

For each of the CSC Sub-Controls in this document there is a "Status" component. The Status section contains both a rating and a description representing the condition of our current efforts as they relate to completion of the stated objective(s). Information is provided here by district IT department staff following internal reflection and evaluative discussions. Although the narrative portion of this component is self-explanatory, the rating scale used here for each Sub-Control is as follows:

Aspiring (**1 Point**) – Task(s) is under consideration, however not currently being pursued as more information, resources or assistance is required.

Developing (**2 Points**) – Task(s) is partially addressed using available tools and processes, however additional effort and resources are needed to see it through completion.

Maintaining (**3 Points**) – Task(s) has been met satisfactorily using current tools and processes, however focus does not expand beyond what has been stated in the document.

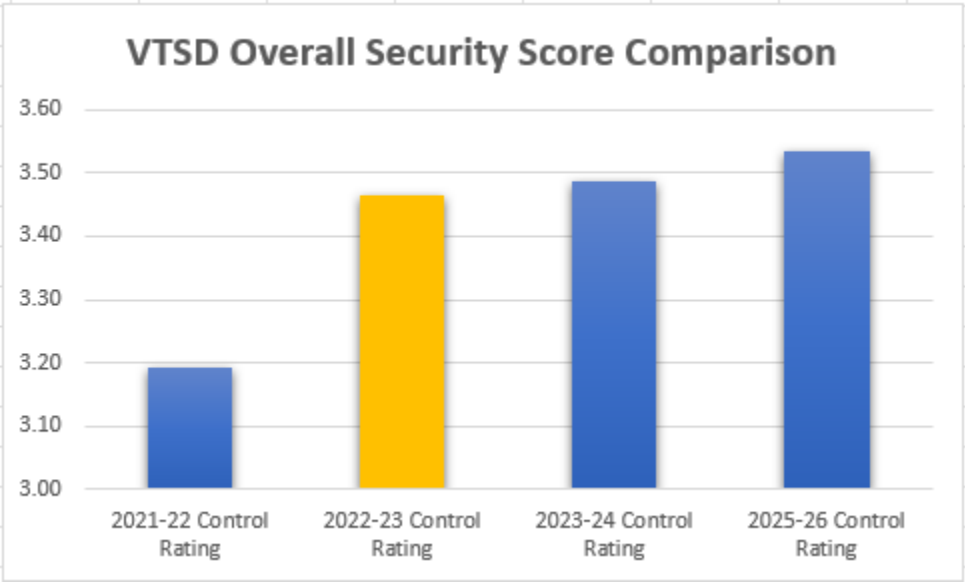
Enhancing (**4 Points**) – Task(s) has been met satisfactorily using current tools and processes, and additional efforts have been made to identify and address other related issues.

Each of the eighteen (18) Critical Security Controls (CSC) is comprised of a varying number of CSC Sub-Controls, with each rated based on the scale above. The rating assigned to each CSC is calculated by taking an average of

the ratings assigned to each of its Sub-Controls. A scoring range has been defined for each CSC for use in determining its consolidated rating:

Poor/Fair (**1.0 -1.49 Points**)
Good (**1.50–2.49 Points**)
Very Good (**2.50–3.49 Points**)
Excellent (**3.50-4.00 Points**)

The **target for minimum acceptance is 3.00** (the median score in the range for "**Very Good**") and the difference represents the gap. Efforts will be made by the district's IT staff going forward to close each gap by pursuing and completing tasks in each of the Sub-Controls. Based on this analysis**,** the district's **Current Overall Critical Security Rating is 3.53 - "Excellent."** This is a 0.34 point improvement from the 2021-22 school year.

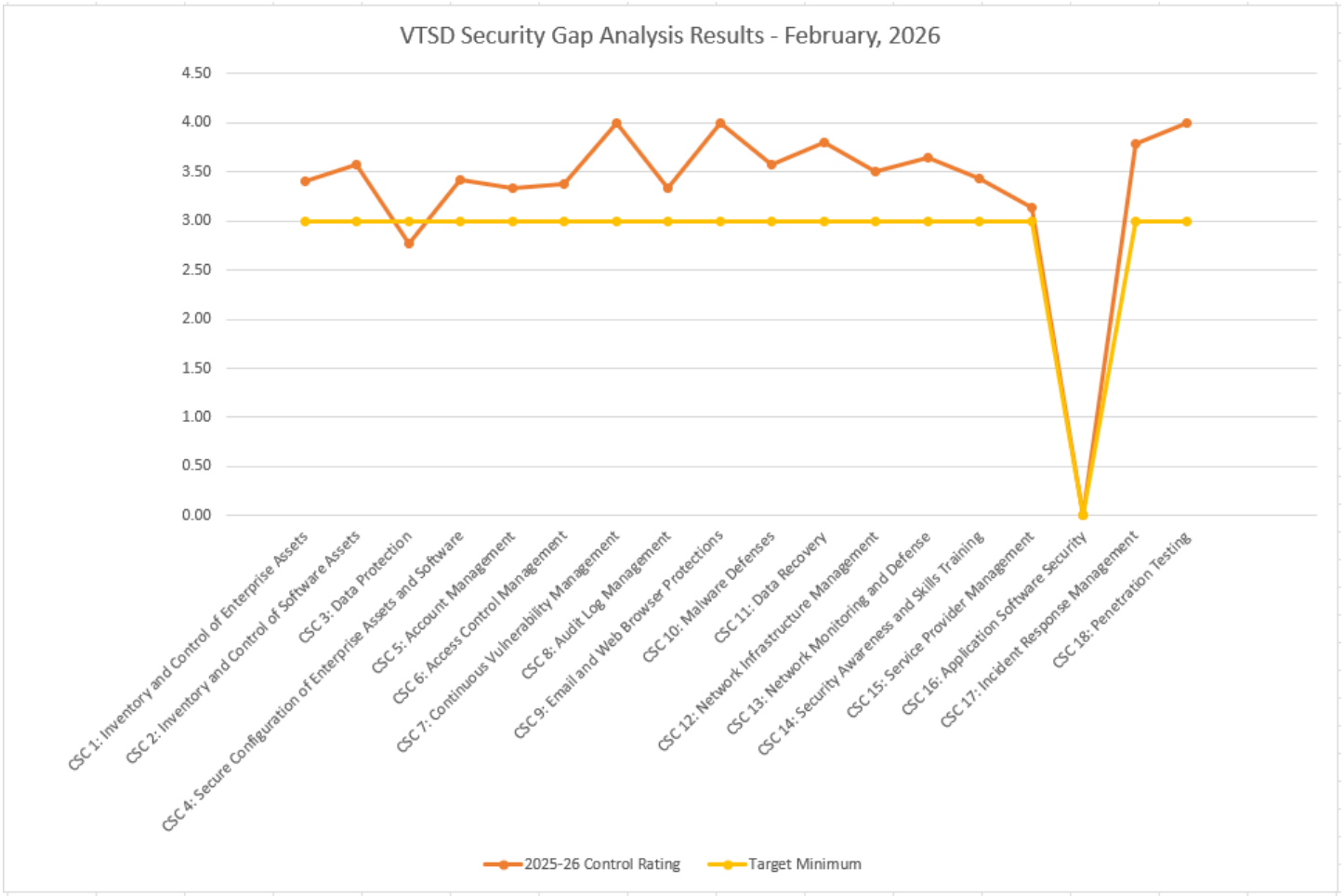


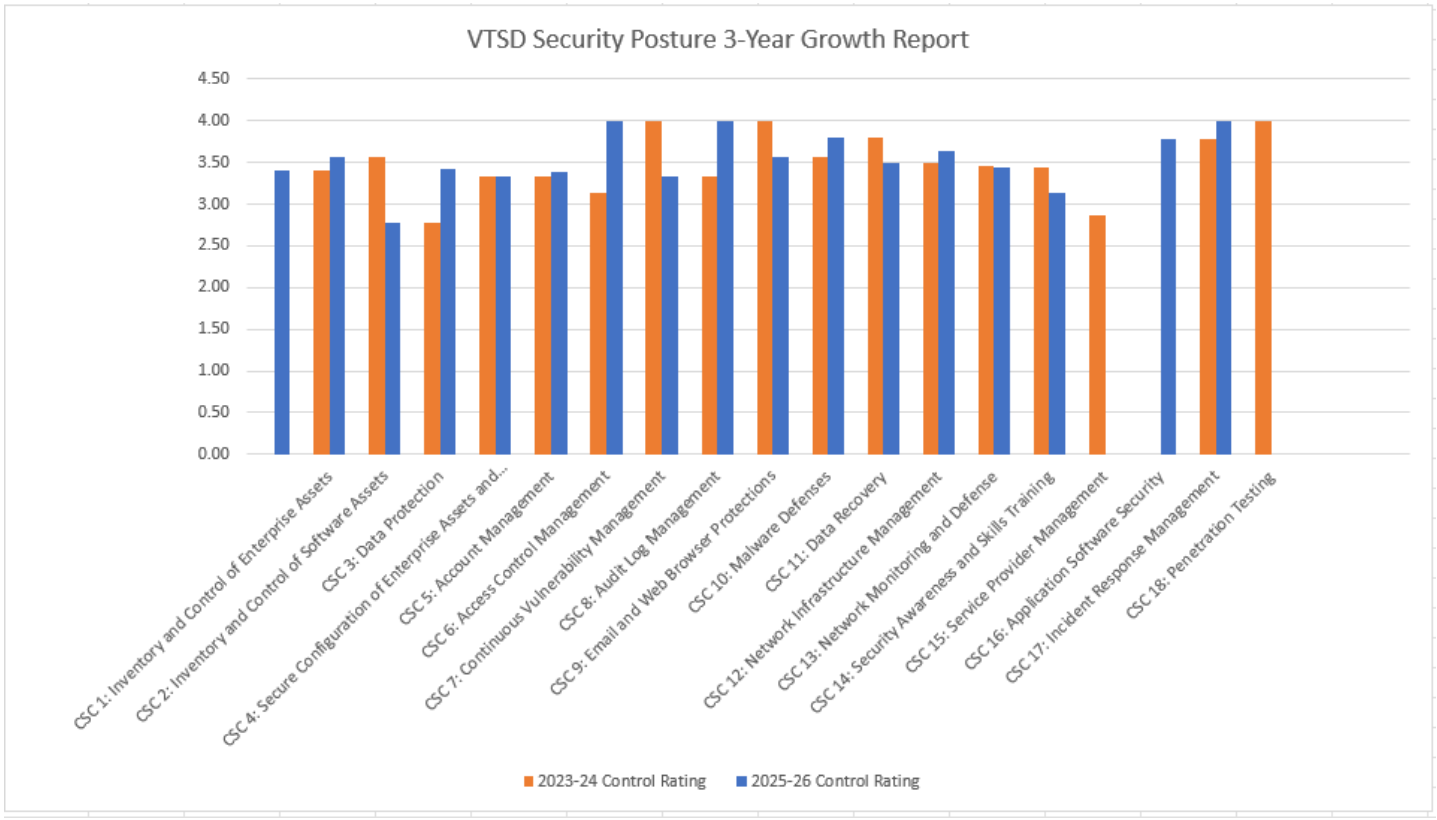
CSC and Sub-Control ratings and may be reviewed individually throughout the body of the document, but a summary of consolidated data is provided on the next page. Although conditions will change in an ongoing fashion as we meet the requirements in this plan, affecting the status of each CSC, we will repeat administration of this Gap Analysis and report changes in revisions to this this plan annually.

2025-26 VTSD Security Gap Analysis Results

Scale:	Aspiring (1.0 - 1.49)	Develping (1.5 - 2.49)	Maintaining (2.5 - 3.49)	Enhancing (3.5 - 4.0)

CIS Critical Security Controls (Version 8.0)	Sub Control Assessment Scores														Control Rating		Target Minimum	Delta
	1	2	3	4	5	6	7	8	9	10	11	12	13	14				
CSC 1: Inventory and Control of Enterprise Assets	3	3	4	3	4										3.40	Very Good	3.00	0.40
CSC 2: Inventory and Control of Software Assets	3	4	4	4	4	3	3								3.57	Excellent	3.00	0.57
CSC 3: Data Protection	3	3	3	2	2	1	3	3	1	4	4	4	3		2.77	Very Good	3.00	(0.23)
CSC 4: Secure Configuration of Enterprise Assets and Software	3	3	4	4	4	3	3	3	4	4	2	4			3.42	Very Good	3.00	0.42
CSC 5: Account Management	3	3	4	3	3	4									3.33	Very Good	3.00	0.33
CSC 6: Access Control Management	4	4	3	3	3	3	4	3							3.38	Very Good	3.00	0.38
CSC 7: Continuous Vulnerability Management	4	4	4	4	4	4	4								4.00	Excellent	3.00	1.00
CSC 8: Audit Log Management	3	4	3	4	3	4	4	3	3	3	3	3			3.33	Very Good	3.00	0.33
CSC 9: Email and Web Browser Protections	4	4	4	4	4	4	4								4.00	Excellent	3.00	1.00
CSC 10: Malware Defenses	4	4	3	3	3	4	4								3.57	Excellent	3.00	0.57
CSC 11: Data Recovery	4	4	4	4	3										3.80	Excellent	3.00	0.80
CSC 12: Network Infrastructure Management	4	3	3	4	4	4	4	2							3.50	Excellent	3.00	0.50
CSC 13: Network Monitoring and Defense	3	4	4	3	4	3	4	4	3	4	4				3.64	Very Good	3.00	0.64
CSC 14: Security Awareness and Skills Training	4	4	4	3	3	3	3	3	4						3.44	Very Good	3.00	0.44
CSC 15: Service Provider Management	3	3	4	3	3	3	3								3.14	Very Good	3.00	0.14
CSC 16: Application Software Security	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CSC 17: Incident Response Management	4	4	4	4	4	4	2	4	4						3.78	Excellent	3.00	0.78
CSC 18: Penetration Testing	4	4	4	4	4										4.00	Excellent	3.00	1.00
Assessment Date: 01-11-2026												Overall Security Score			3.53	Excellent	3.00	0.53


VTSD Security Gap Analysis Results - February, 2026
4.50
4.00
3.50
3.00
2.50
2.00
1.50
1.00
0.50
0.00
CSC 1: Inventory and Control of Enterprise Assets
CSC 2: Inventory and Control of Software Assets
CSC 3: Data Protection
CSC 4: Secure Configuration of Enterprise Assets and Software
CSC 5: Account Management
CSC 6: Access Control Management
CSC 7: Continuous Vulnerability Management
CSC 8: Audit Log Management
CSC 9: Email and Web Browser Protections
CSC 10: Malware Defenses
CSC 11: Data Recovery
CSC 12: Network Infrastructure Management
CSC 13: Network Monitoring and Defense
CSC 14: Security Awareness and Skills Training
CSC 15: Service Provider Management
CSC 16: Application Software Security
CSC 17: Incident Response Management
CSC 18: Penetration Testing
2025-26 Control Rating
Target Minimum


VTSD Security Posture 3-Year Growth Report
4.50
4.00
3.50
3.00
2.50
2.00
1.50
1.00
0.50
0.00
CSC 1: Inventory and Control of Enterprise Assets
CSC 2: Inventory and Control of Software Assets
CSC 3: Data Protection
CSC 4: Secure Configuration of Enterprise Assets and...
CSC 5: Account Management
CSC 6: Access Control Management
CSC 7: Continuous Vulnerability Management
CSC 8: Audit Log Management
CSC 9: Email and Web Browser Protections
CSC 10: Malware Defenses
CSC 11: Data Recovery
CSC 12: Network Infrastructure Management
CSC 13: Network Monitoring and Defense
CSC 14: Security Awareness and Skills Training
CSC 15: Service Provider Management
CSC 16: Application Software Security
CSC 17: Incident Response Management
CSC 18: Penetration Testing
2023-24 Control Rating
2025-26 Control Rating

CSC 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

CSC 1: Inventory and Control of Enterprise Assets				
CSC 1 Rating: 3.20				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Devices	**1.1**	**Establish and Maintain Detailed Enterprise Asset Inventory** Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	IG1 IG2 IG3	**Identify**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Cisco Identity Services Engine (ISE) - BYOD Devices 4. Meraki Dashboard 5. Cisco Secure Endpoint - Wired & Wireless Devices 6. Cisco Umbrella (Windows Roaming Client; iOS Security Connector) 7. Cisco FirePower Management Center (FMC) - Wired & Wireless Devices		

Process		1. Install ZCM agent on all Windows devices (automated in imaging process), registering them each with the primary ZEN Control Center in the ZCM system. 2. Enroll all district-owned iOS devices in JSS inventory, managing all in supervised mode. 3. Permit authorized personally owned devices network access via LDAP-enabled policy on radius server feature of ISE. 4. Capture/monitor all device traffic on all wired and wireless network segments. 5. Gather configuration data for all miscellaneous "Internet of Things" (IoT) devices, identify them in documentation and in FMC and Umbrella, and add them to appropriate device groups.		
Status		**(3) Maintaining:** ZCM and JSS provide device inventories which include data on installed hardware, operating systems, device drivers, applications, deployed configuration policies and assigned users. NCS and Meraki Dashboard provides device inventories and logs for all network switches and access point devices. Loose documentation exists for most IoT devices, but not all. All connected device information is dynamically collected and visible in web traffic monitoring security consoles.		
Devices	**1.2**	**Address Unauthorized Assets** Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	IG1 IG2 IG3	**Respond**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Cisco Cloudlock 4. Microsoft Office 365 Portal 5. Google Workspace Admin Console 6. Cisco Identity Services Engine (ISE) 7. Meraki Dashboard		
Process		1. Establish a detailed list of authorized software 2. Evaluate and select integrity checking tools for implementation 3. Use tools to allow or restrict use of apps based on policy		
Status		**(3) Maintaining:** ZCM, JSS, Cloudlock, O365 Portal, and Google Admin Console provide visibility as to what versions of what applications are installed on district-owned devices, and policy enforcement is possible to restrict which applications/versions can be installed/launched. If licensed appropriately, ISE could be used to identify "Jail Broken" iOS apps. Current software inventory is listed in the district's Technology Plan, but not integrated into policy-based rules.		
Devices	**1.3**	**Utilize an Active Discovery Tool** Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.	IG2 IG3	**Detect**

Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Cisco Identity Services Engine (ISE) - BYOD Devices 4. Cisco Secure Endpoint - Wired & Wireless Devices 5. Cisco Umbrella (Windows Roaming Client; iOS Security Connector) 6. Cisco FirePower Management Center (FMC) - Wired & Wireless Devices 7. Meraki Dashboard		
Process		1. Install ZCM agent on all Windows devices (automated in imaging process), registering them each with the primary ZEN Control Center in the ZCM system. 2. Enroll all district-owned iOS devices in JSS inventory, managing all in supervised mode. 3. Permit authorized personally owned devices network access via LDAP-enabled policy on radius server feature of ISE. 4. Capture/monitor all device traffic on all wired and wireless network segments.		
Status		**(4) Enhancing:** ZCM and JSS provide device inventories which include data on installed hardware, operating systems, device drivers, applications, deployed configuration policies and assigned users. ISE, NCS, Meraki Dashboard, Secure Endpoint, Umbrella and FMC monitor device traffic and record/report visibility on device make/model/OS and their connections including geolocation, initiator and responding IP, connections over time, connections by port, connections by application, connections by DNS, etc.		
Devices	**1.4**	**Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory** Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	IG2 IG3	**Identify**
Tools		1. Micro Focus Open Enterprise (OES) Server DHCP Services 2. Cisco WLAN Controllers DHCP Server Services Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 3. Jamf Pro Mobile Device Management (JSS) - iOS Devices 4. Cisco Identity Services Engine (ISE) - BYOD Devices 5. Meraki Dashboard		

Process		1. Maintain and modify DHCP Scopes as needed on six (6) building-based OES servers, meeting connectivity requirements for specific applications, and performing device identification tasks related to wired PCs and wireless BYOD and Guest devices. 2. Maintain and modify DHCP Scopes as needed in Meraki Dashboard, meeting connectivity requirements for specific applications, and performing device identification tasks related to wireless iOS and laptop PC devices. 3. Configure DHCP servers to provide IP lease allocation information for connected clients 4. Cross check client MAC address from IP lease data with device inventories maintained in ZCM, JSS and ISE environments for identification. 5. Implement "High" Rogue Policy in Meraki Dashboard for Apps and Clients		
Status		**3) Maintaining:** Both known and unknown systems are logged when a connection is made. The status of the device (known vs. unknown) may be investigated, labeled and policy decisions concerning access may be made.		
Devices	**1.5**	**Use a Passive Asset Discovery Tool** Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	**IG3**	**Detect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Cisco Identity Services Engine (ISE) - BYOD Devices 4. Cisco Secure Endpoint - Wired & Wireless Devices 5. Cisco Umbrella (Windows Roaming Client; iOS Security Connector) 6. Cisco FirePower Management Center (FMC) - Wired & Wireless Devices 7. Meraki Dashboard		
Process		1. Install ZCM agent on all Windows devices (automated in imaging process), registering them each with the primary ZEN Control Center in the ZCM system. 2. Enroll all district-owned iOS devices in JSS inventory, managing all in supervised mode. 3. Permit authorized personally owned devices network access via LDAP-enabled policy on radius server feature of ISE. 4. Capture/monitor all device traffic on all wired and wireless network segments.		
Status		**(4) Enhancing:** ZCM and JSS provide device inventories which include data on installed hardware, operating systems, device drivers, applications, deployed configuration policies and assigned users. ISE, NCS, Meraki Dashboard, Secure Endpoint, Umbrella and FMC monitor device traffic and record/report visibility on device make/model/OS and their connections including geolocation, initiator and responding IP, connections over time, connections by port, connections by application, connections by DNS, etc.		

CSC 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

CSC 2: Inventory and Control of Software Assets				
CSC 2 Rating: 3.57				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Applications	**2.1**	**Establish and Maintain a Software Inventory** Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	IG1 IG2 IG3	**Identify**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Cisco Cloudlock 4. Microsoft Office 365 Portal 5. Google Workspace Admin Console 6. Cisco Identity Services Engine (ISE)		
Process		1. Establish a detailed list of authorized software 2. Evaluate and select integrity checking tools for implementation 3. Use tools to allow or restrict use of apps based on policy		
Status		**(3) Maintaining:** ZCM, JSS, Cloudlock, O365 Portal, and Google Admin Console provide visibility as to what versions of what applications are installed on district-owned devices, and policy enforcement is possible to restrict which applications/versions can be installed/launched. If licensed appropriately, ISE could be used to identify "Jail Broken" iOS apps. Current software inventory is listed in the district's Technology Plan, but not integrated into policy-based rules.		

Applications	**2.2**	**<u>Ensure Authorized Software is Currently Supported</u>** Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	**IG1** **IG2** **IG3**	**Identify**
	Tools	1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Cisco Cloudlock 4. Microsoft Office 365 Portal 5. Google Workspace Admin Console 6. Cisco Secure Endpoint - - Wired & Wireless Devices		
	Process	1. Establish a detailed list of authorized software 2. Evaluate and select integrity checking tools for implementation 3. Use tools to allow or restrict use of apps based on policy		
	Status	**<u>(4) Enhancing:</u>** ZCM and JSS provide device inventories which include data on installed hardware, operating systems, device drivers, applications, deployed configuration policies and assigned users. Secure Endpoint shows vulnerabilities where patching is required. Reports may be run on all devices managed in either system, as well as the other systems listed, or individual devices may be queried as needed. There is no list of unsupported software exceptions as we don't run unsupported software.		
Applications	**2.3**	**<u>Address Unauthorized Software</u>** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	**IG1** **IG2** **IG3**	**Respond**

Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Cisco Cloudlock 4. Microsoft Office 365 Portal 5. Google Workspace Admin Console 6. Cisco Secure Endpoint - - Wired & Wireless Devices 7. Meraki Dashboard 8. Cisco Secure Endpoint - Wired & Wireless Devices 9. Cisco Umbrella (Windows Roaming Client; iOS Security Connector) 10. Cisco FirePower Management Center (FMC) - Wired & Wireless Devices 11. Meraki Dashboard		
Process		1. Establish a detailed list of authorized software 2. Evaluate and select integrity checking tools for implementation 3. Use tools to allow or restrict use of apps based on policy		
Status		**(4) Enhancing:** ZCM, JSS, O365 Portal, Google Admin Console, multiple Cisco security products, and Apple School Manager provide visibility as to what versions of what applications are installed on district-owned devices, and policy enforcement is possible to restrict which applications/versions can be installed/launched		
Applications	**2.4**	**Utilize Automated Software Inventory Tools** Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	**IG2** **IG3**	**Detect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Cisco Cloudlock 4. Microsoft Office 365 Portal 5. Google Workspace Admin Console		

Process		1. Install ZCM agent on all Windows devices (automated in imaging process), registering them each with the primary ZEN Control Center in the ZCM system. 2. Enroll all district-owned iOS devices in JSS inventory, managing all in supervised mode. 3. Observe detected iOS Apps that have OAuth connections with Google Workspace, view security ratings and modify classifications/user access permissions 4. Monitor Microsoft application deployments in O365 Portal 5. Monitor Google application deployment and usage data in the Admin Console		
Status		**(4) Enhancing:** ZCM and JSS provide device inventories which include data on installed hardware, operating systems, device drivers, applications, deployed configuration policies and assigned users. Reports may be run on all devices managed in either system, as well as the other systems listed, or individual devices may be queried as needed.		
Applications	**2.5**	**Allowlist Authorized Software** Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	IG2 IG3	**Protect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Cisco Cloudlock 4. Microsoft Office 365 Portal 5. Google Workspace Admin Console		
Process		1. Establish a detailed list of authorized software 2. Evaluate and select integrity checking tools for implementation 3. Use tools to allow or restrict use of apps based on policy		
Status		**(4) Enhancing:** ZCM, JSS, Cloudlock, O365 Portal, and Google Admin Console provide visibility as to what versions of what applications are installed on district-owned devices, and policy enforcement is possible to restrict which applications/versions can be installed/launched		
Applications	**2.6**	**Allowlist Authorized Libraries** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.	IG2 IG3	**Protect**
Tools		1. Cisco Secure Endpoint - Wired & Wireless Devices 2. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers		

Process		1. Create exceptions in Secure Endpoint Management Console, removing specific software libraries from scanning activities to allow for proper functioning of system processes 2. Allow or disallow specific software libraries to load based on Windows Group Policy deployed by ZCM		
Status		**(3) Maintaining:** Several software library exceptions and restrictions have been defined and implemented. Changes are periodically made as needed, however not currently pursued proactively.		
Applications	**2.7**	**Allowlist Authorized Scripts** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	**IG3**	**Protect**
Tools		1. Cisco Secure Endpoint - Wired & Wireless Devices 2. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers		
Process		1. Create exceptions in Secure Endpoint Management Console, whitelisting specific scripts so not detected as executed malware 2. Allow or disallow specific scripts to load based on Windows Group Policy deployed by ZCM		
Status		**(3) Maintaining:** Several whitelisted scripts and restrictions have been defined and implemented. Changes are periodically made as needed, however not currently pursued proactively.		

CSC 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

CSC 3: Data Protection				
CSC 3 Rating: 2.77				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Data	**3.1**	**Establish and Maintain a Data Management Process** Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	IG1 IG2 IG3	**Identify**
Tools		1. VTSD Data Security & Privacy Policy 2. VTSD Data Governance, Security & Privacy Handbook		
Process		1. Maintain VTSD Data Security & Privacy Policy – Build content into user awareness training 2. Maintain VTSD Data Governance, Security & Privacy Handbook – Build content into user awareness training		
Status		**(3) Maintaining:** VTSD is required by law to collect and store student and educator records and takes seriously its obligation to secure information systems and protect the privacy of student data that is collected, used, shared and stored by the District. In addition to the laws that require the VTSD to collect educational data, these data assets are essential to the VTSD's strategic operations, and they must be diligently protected. As a standard operating procedure, the VTSD regularly monitors changes in state and federal regulations that are related to data collection, privacy and security. The VTSD meets all state and federal requirements related to data security and IT infrastructure, as well as the policies and processes encompassed within this data privacy and security policy.		
Data	**3.2**	**Establish and Maintain a Data Inventory** Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	IG1 IG2 IG3	**Identity**

Tools		1. VTSD Data Security & Privacy Policy 2. VTSD Data Governance, Security & Privacy Handbook		
Process		1. Maintain VTSD Data Security & Privacy Policy – Build content into user awareness training 2. Maintain VTSD Data Governance, Security & Privacy Handbook – Build content into user awareness training		
Status		**(3) Maintaining:** VTSD is committed to protecting and safeguarding the data that it collects and recognizes data as a critical asset. A three-tiered governance structure, managed by the Office of Data Management, controls the organization's approach to data and information management through a district-wide infrastructure that ensures appropriate data use, management of change and support for the implementation of security and privacy protocols. This district-wide infrastructure is the mechanism for ensuring appropriate data use, managing change and supporting the implementation of security and privacy protocols.		
Data	**3.3**	**Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	**IG1** **IG2** **IG3**	**Protect**
Tools		1. VTSD Data Security & Privacy Policy 2. VTSD Data Governance, Security & Privacy Handbook		
Process		1. Maintain VTSD Data Security & Privacy Policy – Build content into user awareness training 2. Maintain VTSD Data Governance, Security & Privacy Handbook – Build content into user awareness training		
Status		**(3) Maintaining:** The students' and educators' records that the VTSD collects and stores are used for compliance, audit and evaluation purposes. This information is only available to employees and contract partners who have a responsibility and appropriate need for accessing the information. The VTSD's Technology Department is responsible for developing and implementing the policies and procedures that assure data is properly handled throughout the data lifecycle. As part of these processes, the Technology Department tracks the list of the specific individuals within the District who have access to student and educator data systems, as well as the specific data that are being requested.		

Data	**3.4**	**Enforce Data Retention** Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	IG1 IG2 IG3	**Protect**
Tools		1. VTSD Data Security & Privacy Policy 2. VTSD Data Governance, Security & Privacy Handbook		
Process		1. Modify VTSD Data Security & Privacy Policy to include data retention information – Build content into user awareness training 2. Modify VTSD Data Governance, Security & Privacy Handbook to include data retention information – Build content into user awareness training		
Status		**(2) Developing:** The VTSD Technology Department is responsible for developing and implementing the policies and procedures that assure data is properly handled throughout the data lifecycle, including proper data retention. Although VTSD meets all local, state and federal requirements related to data security and IT infrastructure, specific timelines for data retention do not currently exist in the Data Security Handbook.		
Data	**3.5**	**Securely Dispose of Data** Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	IG1 IG2 IG3	**Protect**
Tools		1. VTSD Data Security & Privacy Policy 2. VTSD Data Governance, Security & Privacy Handbook		
Process		1. Modify VTSD Data Security & Privacy Policy to include data retention information – Build content into user awareness training 2. Modify VTSD Data Governance, Security & Privacy Handbook to include data retention information – Build content into user awareness training		
Status		**(2) Developing:** The VTSD Technology Department is responsible for developing and implementing the policies and procedures that assure data is properly handled throughout the data lifecycle, including proper disposal of data. Although VTSD meets all local, state and federal requirements related to data security and IT infrastructure, specific methods for data disposal do not currently exist in the Data Security Handbook.		
Devices	**3.6**	**Encrypt Data on End-User Devices** Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	IG1 IG2 IG3	**Protect**

Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Microsoft BitLocker Drive Encryption 4. iOS Encryption APP - TBD		
Process		1. Identify mobile devices (laptops & iOS) that are used to hold sensitive data (e.g., child study team members, administrators, etc.). 2. Create "Secure Mobility" device group in ZCM 3. Create and deploy ZCM group policy to "Secure Mobility" group to enable Microsoft Bit Locker. 4. Research and select iOS encryption product for deployment and deploy via JSS. 5. Dispatch Technicians to work with users on encrypting storage and obtaining encryption keys.		
Status		**(1) Aspiring:** Data storage on laptop PCs is currently not encrypted by policy. iOS devices are used to access sensitive data, and although a passcode is required by policy, data encryption tools are not being used.		
Data	**3.7**	**Establish and Maintain a Data Classification Scheme** Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	IG2 IG3	**Identify**
Tools		1. VTSD Data Security & Privacy Policy 2. VTSD Data Governance, Security & Privacy Handbook		
Process		1. Maintain VTSD Data Security & Privacy Policy – Build content into user awareness training 2. Maintain VTSD Data Governance, Security & Privacy Handbook – Build content into user awareness training		
Status		**(3) Maintaining:** Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected in compliance with Board Policy and any applicable laws. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data are classified according to the most sensitive detail they include. Data recorded in several formats (e.g., source document, electronic record, report) have the same classification regardless of format. Data classification and levels are defined in the Security and Risk Management component of the VTSD Data Security Handbook.		

Data	**3.8**	**Document Data Flows** Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	IG2 IG3	**Identify**
Tools		1. VTSD Data Security & Privacy Policy 2. VTSD Data Governance, Security & Privacy Handbook		
Process		1. Maintain VTSD Data Security & Privacy Policy – Build content into user awareness training 2. Maintain VTSD Data Governance, Security & Privacy Handbook – Build content into user awareness training		
Status		**(3) Maintaining:** Data flow policies and procedures for internal use, external use and disclosure are described in the VTSD Data Security & Privacy Policy. Data Transfer/Exchange/Printing are described in the Security Operations section of the VTSD Data Security Handbook. The VTSD Third Party Vendor Contracting Guide ensures the security of student and district data when dealing with external companies or agencies.		
Data	**3.9**	**Encrypt Data on Removable Media** Encrypt data on removable media.	IG2 IG3	**Protect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Microsoft BitLocker Drive Encryption		
Process		1. Identify devices (laptops & desktop PCs) that are used to hold sensitive data (e.g., child study team members, administrators, etc.), and locate user removable media for storing data backups. 2. Create "Secure Mobility" device group in ZCM 3. Create and deploy ZCM group policy to "Secure Mobility" group to enable Microsoft Bit Locker. 4. Dispatch Technicians to work with users on encrypting removable storage and obtaining encryption keys.		
Status		**(1) Aspiring:** Data storage on removable media is currently not encrypted by policy.		

Data	3.10	**Encrypt Sensitive Data in Transit** Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).	IG2 IG3	Protect
Tools		1. SUSE Linux / Open Enterprise Server / Client for Open Enterprise Server 2. Google Drive 3. Microsoft Office 365 4. SysCloud Backup and Recovery 5. On-Prem Database Servers (Genesis, Jamf, Destiny, iManager, ZCM, etc.) 6. Hosted Database Servers (Clever, ASM, Frontline, iObservation, Systems 3000, etc.) 7. Meraki Dashboard 8. Cisco AnyConnect VPN Client / Cisco Firepower Threat Defense 2140 (FTD)		
Process		1. Assess data encryption measures in place on sensitive data in transit between users and core systems 2. Remediate any system with a substandard security posture		

Status	**(4) Enhancing:** 1. Client for Open Enterprise Server supports authentication of NCP and LDAP connections via user authentication into eDirectory. NCP protocol authentication is supported via RSA, and LDAP authentication is supported via SSL and the Simple Bind protocol. Connections to servers are authenticated via user-supplied credentials (via X-Tier's plug-in authentication module architecture). No device authentication is supported directly by the Client. No wire encryption is supplied by this product. Passwords and other authentication materials in temporary storage are encrypted to prevent in-memory scanners. There are no configuration options to enable or disable with the exception of packet signing. Access to resources is protected based on user identity (as stored within eDirectory). The VFS, daemon, and X-Tier work together to compare ACLs for a given file system path or object retrieved from eDirectory to the identity and session scope established for the identity that owns a given connection - the VFS acts as a proxy to the local file system (via redirection of its local mount point) to make such decisions for network-based file system paths or objects. 2. Google Drive encrypts data at rest in the Drive, and data in transit to and from the Drive. Google uses 128-bit and 256-bit AES keys to encrypt data at rest in Google Drive, which helps in protecting the confidentiality of the data stored in Google Drive. 3. With Office 365, data is encrypted at rest and in transit, using several strong encryption protocols, and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES). 4. Google Drive encrypts data at rest in the Drive, and data in transit to and from the Drive. Google uses 128-bit and 256-bit AES keys to encrypt data at rest in Google Drive, which helps in protecting the confidentiality of the data stored in Google Drive. 5. With Office 365, data is encrypted at rest and in transit, using several strong encryption protocols, and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES). 6. SysCloud Backup and Recovery uses 256-bit AES encryption for protecting data when it is at rest and TLS/SSL security for data in motion 7. Wireless network access via WLC devices uses WPA + WPA2 encryption with Pre-Shared Key Authentication 8. Data exchanges between user applications and core local and hosted database servers is encrypted via TLS/SSL 9. Remote access to internal data requires secure VPN access through the firewall by each end user 10. Remote access to hosted accounting/personnel data requires secure VPN access through the firewall by each end user, while access from the local area network is allowed via VPN connection between the two firewalls in play

Data	**3.11**	**Encrypt Sensitive Data at Rest** Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.	**IG2** **IG3**	**Protect**
Tools		1. SUSE Linux / Open Enterprise Server/ Client for Open Enterprise Server 2. Google Drive 3. Microsoft Office 365 4. Microsoft Windows 10 Professional Tools 5. Unitrends Backup and Recovery Appliance 6. SysCloud Backup and Recovery		
Process		1. Assess data encryption measures in place on sensitive data at rest in core systems 2. Remediate any system with a substandard security posture		

Status		**(4) Enhancing:** 1. Microsoft Windows – Users are strongly encouraged not to store data on the local hard drive of their computers, but to use server or cloud storage where data is encrypted. Windows 10 & 11 Pro users who need to store data locally may use Encrypting File System (EFS) encryption technology or BitLocker (a full-disk encryption solution that encrypts an entire volume), but that is not currently required. 2. SUSE Linux / Open Enterprise Server encrypted volume support uses the NICI libraries for all cryptographic support. NICI generates a 128-bit AES key for encryption that persists for the life of the volume. You cannot change the password because it is the key used to encrypt data. NICI uses the password to wrap the key and other volume-specific cryptographic information into a 128-bit package that is persistently stored in two locations on the NSS media: the Volume Data Block and the Volume Locator storage object. After the cryptographic data is wrapped for the activated volume, EVS eliminates the password from memory. 3. Google Drive encrypts data at rest in the Drive, and data in transit to and from the Drive. Google uses 128-bit and 256-bit AES keys to encrypt data at rest in Google Drive, which helps in protecting the confidentiality of the data stored in Google Drive. 4. With Office 365, data is encrypted at rest and in transit, using several strong encryption protocols, and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES). 5. Unitrends Backup and Recovery solutions use AES 256-bit encryption to secure and protect sensitive customer data, but this is not enabled due to our use of deduplication. Deduplication is a one such storage optimization technique that avoids storing duplicate copies of data. Currently, to ensure security, data stored in cloud as well as other large storage areas are in an encrypted format and one problem with that is, the product cannot apply deduplication technique over such an encrypted data. 6. SysCloud Backup and Recovery uses 256-bit AES encryption for protecting data when it is at rest and TLS/SSL security for data in motion.		
Network	**3.12**	**<u>Segment Data Processing and Storage Based on Sensitivity</u>** Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	**IG2** **IG3**	**Protect**
Tools		1. On-Prem Database Servers (Genesis, Jamf, Destiny, iManager, ZCM, etc.) 2. Hosted Database Servers (Clever, ASM, Frontline, iObservation, Systems 3000, etc.)		
Process		1. Use dedicated servers for data storage and processing, with no dual purpose or crossover roles.		

Status		**(4) Enhancing:** On-prem servers and hosted systems all perform only one set of related tasks on the data stored there for that purpose. Servers are not used to process data for purposes other than what is the primary responsibility of each system.		
Data	**3.13**	**Deploy a Data Loss Prevention Solution** Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.	**IG3**	**Protect**
Tools		1. Cisco Cloud E-Mail Security Appliance (ESA) 2. Cisco Cloudlock 3. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 4. Microsoft Office 365 Portal Security & Compliance Policy Center 5. Google Workspace Admin Console		
Process		1. Enable Data Loss Prevention (DLP) features on existing network security and cloud service resources. 2. Implement DLP detection feature in O365 Security & Compliance Center 3. Implement DLP detection rules in Google Workspace 4. Configure automated reports to provide DLP incident notifications when they occur.		
Status		**(4) Enhancing**: DLP tools are in place allowing for monitoring and detection and used for periodic inspection and creating alerts concerning incidents.		
Data	**3.14**	**Log Sensitive Data Access** Log sensitive data access, including modification and disposal.	**IG3**	**Protect**
Tools		1. On-Prem Database Servers (Genesis, Jamf, Destiny, iManager, ZCM, Retain, etc.) 2. Hosted Database Servers (Clever, ASM, Frontline, iObservation, Systems 3000, etc.) 3. Server Operating Environments (SUSE Linux / Open Enterprise Server, Microsoft Windows Server 201X, Google Workspace, Microsoft Office 365, etc.)		
Process		1. Assess data logging/auditing capabilities in place on sensitive data at rest in core systems 2. Enable logging/auditing on any system with that capability available, but disabled		
Status		**(3) Maintaining:** Hardware, software, services and/or procedural mechanisms that record and examine activity in information systems that contain or use PII are reviewed by the Department of Technology staff annually. Department of Technology staff also regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.		

CSC 4: Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

CSC 4: Secure Configuration of Enterprise Assets and Software				
CSC 4 Rating: 3.17				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Applications	**4.1**	**Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	IG1 IG2 IG3	**Protect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Novacoast Desktop Imaging System, Enhancement to Micro Focus ZEN Configuration & Management System (ZCM)		
Process		1. Determine standard device security configurations based on industry best practices. 2. Implement machine learning technology based on network discovery, where available, evaluate and implement recommended modifications. 3. Change default credentials for accessing/managing IoT devices. 4. Archive reports of device configuration settings as a reference when evaluating changes going forward.		
Status		**(3) Maintaining**: Worked with certified vendors when implementing initial device configurations, as well as modifications along the way during upgrades, etc. Standard operating systems, applications, configurations and user restrictions are implemented via established deployment processes using available tools. No organization change control exists, relying solely on process reevaluations conducted by IT department staff in decision-making process.		
Network	**4.2**	**Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	IG1 IG2 IG3	**Protect**

Tools	1. Meraki Dashboard 2. Cisco FirePower Management Center (FMC) - Wired & Wireless Devices
Process	1. Determine standard device security configurations based on industry best practices. 2. Implement machine learning technology based on network discovery, where available, evaluate and implement recommended modifications. 3. Archive reports of device configuration settings as a reference when evaluating changes going forward.
Status	**(3) Maintaining**: Worked with certified vendors when implementing initial device configurations, as well as modifications along the way during upgrades, etc. No organization change control exists, relying solely on research conducted by IT department staff in decision-making process.

Users	**4.3**	**Configure Automatic Session Locking on Enterprise Assets** Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	IG1 IG2 IG3	**Protect**

Tools	1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices
Process	1. Create, assign by device or user (group), and deploy system policies to desktop and laptop computers that lock screens with re-authentication required after a defined period of inactivity (ZCM). 2. Create a passcode requirement policy, assign by device or user (group), and deploy configuration profiles to iOS devices (JSS).
Status	**(4) Enhancing:** Policy/Profile management features continue to be a valuable component within each of our existing device management platforms. Leveraging device management systems to enforce device access security is enabled in this environment.

Devices	**4.4**	**Implement and Manage a Firewall on Servers** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	IG1 IG2 IG3	**Protect**

Tools		1. Cisco Secure Endpoint connector/console.		
Process		1. Implement Secure Endpoint Connector to perform vulnerability scanning on local systems, perform cloud lookup to check file disposition for files executed, moved or copied, and identify all vulnerable computers and their vulnerable applications. 2. Schedule period scans of all systems to gather vulnerability data Leverage OS and server-based firewall products on critical hosts. 3. Configure alerts/automated actions when anomalies are discovered. 4. Place clients with malware detections or known vulnerabilities into "Triage" mode via Secure Endpoint Management Console, removing network access during remediation activities.		
Status		**(4) Enhancing:** Current tools in place can track changes in system and application files and show the number of vulnerable applications that have been executed, moved, or copied, together with the number of vulnerable computers. Whenever an executable file is moved, copied, or executed, the Secure Endpoint Connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database, that information is displayed. District's end-point security resources provide best-in-class protection. All Cisco products are licensed with Advanced Malware Protection (AMP), which is integrated with the Cisco Talos Security Intelligence and Research Group for detection, analysis and protection against known and emerging treats. Agent status for Secure Endpoint and Security Connector may be monitored via cloud-based AMP console, and leveraging automation in reporting and remediation to reduce administrative efforts is desirable.		
Devices	**4.5**	**Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	**IG1** **IG2** **IG3**	**Protect**
Tools		1. Cisco Secure Endpoint connector/console. 2. Windows Defender 3. Cisco Umbrella Windows Roaming Client and iOS Security Connecter		
Process		1. Implement Secure Endpoint Connector to perform vulnerability scanning on local systems, perform cloud lookup to check file disposition for files executed, moved or copied, and identify all vulnerable computers and their vulnerable applications. 2. Schedule period scans of all systems to gather vulnerability data Leverage OS and server-based firewall products on critical hosts. 3. Configure alerts/automated actions when anomalies are discovered. 4. Place clients with malware detections or known vulnerabilities into "Triage" mode via Secure Endpoint Management Console, removing network access during remediation activities		

Status		**(4) Enhancing:** Current tools in place can track changes in system and application files and show the number of vulnerable applications that have been executed, moved, or copied, together with the number of vulnerable computers. Whenever an executable file is moved, copied, or executed, the Secure Endpoint Connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database, that information is displayed. District's end-point security resources provide best-in-class protection. All Cisco products are licensed with Advanced Malware Protection (AMP), which is integrated with the Cisco Talos Security Intelligence and Research Group for detection, analysis and protection against known and emerging treats. Agent status for Secure Endpoint and Security Connector may be monitored via cloud-based AMP console, and leveraging automation in reporting and remediation to reduce administrative efforts is desirable.		
Network	**4.6**	**Securely Manage Enterprise Assets and Software** Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	**IG1** **IG2** **IG3**	**Protect**
Tools		1. PuTTY (SSH) Client 2. Device(s) Secure Web UI w/SSL encryption 3. Cisco AnyConnect VPN Client 4. Device/Service Built-In Two-Factor Authentication Feature 5. Third-Party Multi-Factor Authentication Service Provided (Google Authenticator & Cisco's Duo)		
Process		1. Implement encrypted SSH client for CLI management 2. Leverage appliance self-signed or commercial trusted root certificates to encrypt web page transmissions where possible. 3. Leverage secure VPN tunnel for remote management sessions. 4. Leverage built-in two-factor authentication on supported systems when feasible. 5. Investigate and select third-party two-factor authentication service to make authentication all-inclusive and standardize the process.		
Status		**(3) Maintaining**: Most device management CLI or WebUI approaches in use implement 128-bit or 256-bit encryption via self-signed certificates, however a few data systems currently use a commercially verified trusted root certificate. Telnet and HTTP may be used, but only while operating inside the network, including via a secure VPN session		

Users	**4.7**	**<u>Manage Default Accounts on Enterprise Assets and Software</u>** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	**IG1** **IG2** **IG3**	**Protect**
Tools		1. All asset management tools		
Process		1. Change default admin account passwords 2. Create backup (backdoor) admin account on each asset where possible 3. Delete default admin account on each asset where possible		
Status		**<u>(3) Maintaining</u>**: Default admin account passwords changed when new products are introduced. A backup (backdoor) account is created, often by the installing vendor, when a new product is rolled out – that password is changed once we are no longer engaging that vendor. Seldom do we delete a built-in admin account, as that is usually not possible.		
Devices	**4.8**	**<u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u>** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	**IG2** **IG3**	**Protect**
Tools		1. CISA Web Application Scanning Reports		
Process		1. Identify available features or services not needed for meeting the desired function for each asset, and assess vulnerability status 2. Disable each unused feature in management portal wherever possible		
Status		**<u>(3) Maintaining</u>**: Heightened efforts made to disable Internet facing applications based on Cyber Hygiene Web Application Scanning and other Vulnerability scanning conducted on our behalf by CISA. Product End-of-Life thresholds are considered as well.		

Devices	4.9	**Configure Trusted DNS Servers on Enterprise Assets** Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.	IG2 IG3	Protect
Tools		1. **Domain-Based Security** - Umbrella Virtual Appliances (VAs). VAs are lightweight virtual machines that are compatible with the district's VMWare ESX/ESXi environment. When utilized as conditional DNS forwarders on the network, Umbrella VAs record the internal IP address information of DNS requests for usage in reports, security enforcement, and category filtering policies. Additionally, VAs encrypt and authenticate DNS data for enhanced security. 2. **Internal DNS Servers** - The DNS software in Open Enterprise Server integrates DNS information into eDirectory, our network object management environment. Integrating DNS with eDirectory greatly simplifies network administration by enabling us to enter all configuration information into one distributed database. The DNS configuration information is replicated just like any other data in eDirectory. The concept of a primary or secondary has been shifted away from the server to the zone itself. After you have configured the zone, the data is available to any of the OES DNS servers you select to make authoritative for the zone. The OES DNS server takes advantage of the peer-to-peer nature of eDirectory by replicating the DNS data. 3. **DNS Forwarding** - Our internal DNS environment uses OpenDNS servers as DNS Forwarders, rather than our ISP's DNS servers. OpenDNS offers DNS services that are faster and more reliable than any other DNS service. With OpenDNS we more quickly reach our intended website and never experience the outages that occur with the DNS services provided by an ISP. In terms of security, OpenDNS has solid security capabilities and will block malicious websites, or allow blacklists of certain websites.		
Process		1. Umbrella VA addresses are dynamically assigned as DNS servers in the TCPIP configuration to all devices via DHCP. 2. Umbrella VAs determine whether the host being contacted by a device is internal or external. 3. If internal, DNS resolution is handled via OES DNS servers integrated with eDirectory. If external, OpenDNS server forwarding addresses are used to resolve hosts outside the network, with domain level security based on security intelligence.		
Status		**(4) Enhancing:** Current tools in place provide fast name resolution for internal and external hosts, and they contribute to our multi-layered network security architecture.		

Devices	**4.10**	**Enforce Automatic Device Lockout on Portable End-User Devices** Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.	IG2 IG3	**Respond**
Tools		1. NetIQ eDirectory - User Intruder Lockout Feature 2. Micro Focus ZEN Configuration & Management System (ZCM) – Laptop Group Policy Configuration 3. Jamf Pro Mobile Device Management (JSS) - iOS Device Restrictions		
Process		1. eDirectory authentication is limited to 5 failed attempts before account lockout is triggered and specifies the last network address (workstation) that login was attempted from by this object if login was disabled because of intruder detection. 2. Windows Group Policy (applied via ZCM) - An Account Lockout security policy is enabled for all staff local Windows user accounts. The account lockout threshold (determines the number of failed sign-in attempts that will cause a user account to be locked) is set to 10 invalid login attempts, the account lockout duration (determines the number of minutes that a locked-out account remains locked out before automatically becoming unlocked) is set to 30 minutes, and the reset account lockout counter (determines the number of minutes that must elapse from the time a user fails to log on before the failed logon attempt counter is reset to 0) is set for 30 minutes. 3. iPadOS configuration profile will disable managed iPad for 1 minute after six failed passcode attempts in a row. The seventh incorrect passcode attempt will lock the user out for 5 minutes, the eighth attempt for 15, and the tenth for an hour.		
Status		**(4) Enhancing:** Current tools in place provide satisfactory implementation of device lockout following failed authentication attempts across several device platforms.		
Devices	**4.11**	**Enforce Remote Wipe Capability on Portable End-User Devices** Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.	IG2 IG3	**Protect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) – Laptop Group Policy Configuration 2. Jamf Pro Mobile Device Management (JSS) - iOS Device Restrictions		

Process	1. ZEN Configuration & Management System (ZCM) allows for an administrator to wipe and reset a device to factory settings via the Quick Task menu in the device's properties page, so long as the device supports that action. A limitation is that the device must be connected to the local area network, either on-prem or via a VPN connection. There is no ability for an administrator to manage a device that is connected to a different network or simply on the Internet. 2. Jamf Pro Mobile Device Management allows for Enable Lost Mode (this locks the device and provides a phone number on the lock screen to report the device missing), Set Activation Lock (Apple securely stores the the Apple ID on its activation servers and links it to the device - the Apple ID password or device passcode is required before anyone can erase the device or reactivate and use the device) and Wipe Device (permanently erases data and settings on the device) options, each more extreme than the next.			
Status	**(2) Developing**: Although most of our managed devices may be wiped remotely by an administrator via the respective management system, laptops may only be wiped if present on the district's network.			
Devices	**4.12**	**Separate Enterprise Workspaces on Mobile End-User Devices** Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.	**IG3**	**Protect**
Tools	1. NetIQ eDirectory - Client for Open Enterprise Server 2. Micro Focus ZEN Configuration & Management System (ZCM) – ZCM Agent 3. Jamf Pro Mobile Device Management (JSS) – Apple Configuration Profiles			
Process	1. Desktop and Laptop computers are deployed via an imaging process that installs the Client for Open Enterprise Server and ZCM Agent software. The Windows local user account is created dynamically based on a ZCM policy which successful authentication in eDirectory. User group membership determines the GPOs and applications assigned to the user on the device with the ZCM agent constantly polling eDirectory as a user source. Users are restricted and cannot create personal accounts. 2. iPads are deployed via an enrollment process that implements a specific configuration profile that engages following an LDAP lookup with eDirectory (based on group membership). The managed Apple ID linked to the device is restricted based on the assigned configuration profile and apps are deployed based on user properties found in eDirectory.			
Status	**(4) Enhancing:** Current tools in place provide satisfactory implementation of device deployment and use of applications and access to data across several device platforms.			

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

CSC 5: Account Management				
CSC 5 Rating: 3.33				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Users	**5.1**	**Establish and Maintain an Inventory of Accounts** Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	IG1 IG2 IG3	**Identify**
Tools		1. Blackboard Web Community Manager – Forms & Surveys 2. Server/platform management As-Built Documentation 3. Service accounts list documentation 4. All platform user directories		
Process		1. New account provisioning, decommissioning, assignment transfers, etc., all begin with the submission of an online form by a secretary after all required personnel data has been gathered, and while the information is sent forward for processing through automation or manual attention, a copy of the request record is written to a database in the Blackboard Web Community Manager environment. 2. Resource administrator account credentials are recorded within the as-built documentation stored by the director of technology for each resource. 3. Service account credentials are also stored in a master list, managed by the director of technology. 4. All resources have a user directory built into the management portal that may be viewed by the resource administrator.		
Status		**(3) Maintaining**: Although multiple account inventories exist and are accessible by authorized staff, there is not one single master inventory.		
Users	**5.2**	**Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	IG1 IG2 IG3	**Protect**

Tools		1. iManager (eDirectory) – Password Policy for network storage, printing, web content, miscellaneous database applications, local Windows Dynamic User access via LDAP integration. 2. Google Workspace – Password Policy in place for Gmail, Docs, Drive, etc., as well as OAuth linkage with third party resources, with mandatory MFA requirement for staff 3. Microsoft Office 365 – Password Policy in place for Web Apps, OneDrive, Teams, etc.		
Process		1. Establish and implement complex password requirements in mandatory password policy.		
Status		**(3) Maintaining**: We adopt this practice whenever possible, however currently require 8 characters minimum (24 maximum) in user passwords. Other requirements include: 1 capital letter, 1 lower case letter, 1 number, 1 non-alphanumeric character, 180 day expiration, 365 day non-reusability, and intruder detection lock out after 5 bad attempts within a 15 minute period.		
Users	**5.3**	**Disable Dormant Accounts** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	IG1 IG2 IG3	**Respond**
Tools		1. Genesis SIS (Data Exchange Source for Multi-System User Provisioning) 2. NetIQ eDirectory – Multi-System LDAP Authentication Provider 3. On-Prem Active Directory (AD) 4. Micro Focus Identity Manager (eDirectory & Active Directory Bi-Directional Drivers) 5. Google Cloud Directory Services (GCDS) 6. Microsoft School Directory Sync - SDS (Azure AD/O365 Provisioning) 7. Apple School Manager - ASM (Managed Apple ID Provisioning) 8. Clever SSO		
Process		1. Implementation of account provisioning and decommissioning via automated tools. 2. Implementation of manual account decommissioning based on user status monitoring and periodic task completion.		
Status		**(4) Enhancing:** Student and staff records entered into Genesis SIS are used to provision user accounts in multiple external systems via automation. Integration with eDirectory via Identity Manager determines account provisioning and decommission in many applications via LDAP, On-Prem AD, and Google via GCDS. Genesis SIS integration is used for account provisioning and decommission in Azure AD (Office 365) via Microsoft SDS, in Apple via ASM, and in Clever SSO (Single Sign On provider for many applications). Other applications, whether accounts were provisioned via automation or manual setup, must have dormant accounts decommissioned manually by IT staff either as needed (by using Genesis WebDesk for monitoring student and staff record status changes) or via our Network Resource Account Provisioning Notification process, or regularly at the conclusion of every school year.		

Users	**5.4**	**<u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u>** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	**IG1** **IG2** **IG3**	**Protect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) – Laptop Group Policy Configuration 2. Jamf Pro Mobile Device Management (JSS) - iOS Device Restrictions		
Process		1. Desktop and Laptop computers are deployed via an imaging process that installs the Client for Open Enterprise Server and ZCM Agent software. The Windows local user account is created dynamically based on a ZCM policy which successful authentication in eDirectory. User group membership determines the GPOs and applications assigned to the user on the device with the ZCM agent constantly polling eDirectory as a user source. Users accounts are Standard Windows accounts, without elevated privileges, which supports the principle of least privilege (PoLP). 2. iPads are deployed via an enrollment process that implements a specific configuration profile that engages following an LDAP lookup with eDirectory (based on group membership). The managed Apple ID linked to the device is restricted based on the assigned configuration profile and apps are deployed based on user properties found in eDirectory.		
Status		**<u>(3) Maintaining</u>**: Although user accounts on a device may be restricted, in some other resource management portals, the administrator account may be the regular eDirectory user account via LDAP authentication. In many of these cases when a separate and dedicated administrative account is not being used, multi-factor authentication is enforced, however that is not always the case.		
Users	**5.5**	**<u>Establish and Maintain an Inventory of Service Accounts</u>** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	**IG2** **IG3**	**Identify**
Tools		1. Server/platform management As-Built Documentation 2. Service accounts list documentation		
Process		1. Resource service account credentials are recorded within the as-built documentation stored by the director of technology for each resource. 2. Additional service account credentials are also stored in a master list, managed by the director of technology. 3. All resources have a user directory built into the management portal that may be viewed by the resource administrator.		

Status		**(3) Maintaining**: Although service account inventories exist and are accessible by authorized staff, there is not one single master inventory and no regularly scheduled reviews.		
Users	**5.6**	**Centralize Account Management** Centralize account management through a directory or identity service.	IG2 IG3	**Protect**
Tools		1. Genesis SIS (Data Exchange Source for Multi-System User Provisioning) 2. NetIQ eDirectory – Multi-System LDAP Authentication Provider 3. On-Prem Active Directory (AD) 4. Micro Focus Identity Manager (eDirectory & Active Directory Bi-Directional Drivers) 5. Google Cloud Directory Services (GCDS) 6. Microsoft School Directory Sync - SDS (Azure AD/O365 Provisioning) 7. Apple School Manager - ASM (Managed Apple ID Provisioning) 8. Clever SSO		
Process		1. Implementation of account provisioning and decommissioning via automated tools. 2. Implementation of manual account decommissioning based on user status monitoring and periodic task completion.		
Status		**(4) Enhancing:** Student and staff records entered into Genesis SIS are used to provision user accounts in multiple external systems via automation. Integration with eDirectory via Identity Manager determines account provisioning and decommission in many applications via LDAP, On-Prem AD, and Google via GCDS. Genesis SIS integration is used for account provisioning and decommission in Azure AD (Office 365) via Microsoft SDS, in Apple via ASM, and in Clever SSO (Single Sign On provider for many applications). Other applications, whether accounts were provisioned via automation or manual setup, must have dormant accounts decommissioned manually by IT staff either as needed (by using Genesis WebDesk for monitoring student and staff record status changes) or via our Network Resource Account Provisioning Notification process, or regularly at the conclusion of every school year.		

CSC 6: Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

CSC 6: Access Control Management				
CSC 6 Rating: 3.13				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Users	**6.1**	**Establish an Access Granting Process** Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	IG1 IG2 IG3	**Protect**
Tools		1. Genesis SIS (Data Exchange Source for Multi-System User Provisioning) 2. NetIQ eDirectory – Multi-System LDAP Authentication Provider 3. On-Prem Active Directory (AD) 4. Micro Focus Identity Manager (eDirectory & Active Directory Bi-Directional Drivers) 5. Google Cloud Directory Services (GCDS) 6. Microsoft School Directory Sync - SDS (Azure AD/O365 Provisioning) 7. Apple School Manager - ASM (Managed Apple ID Provisioning) 8. Clever SSO 9. Meraki Dashboard Lobby Ambassador – Wireless Guest Account Provisioning		
Process		1. Implementation of account provisioning and decommissioning via automated tools. 2. Maintain “network resource provisioning” process to establish communications between human resources, department leaders and technology/data security managers so that changes in employment status for staff members are communicated to all with relevant data elements. 3. Data managers are to respond to reported “end of employment,” or “leave of absence” notifications and disable authentication privileges or otherwise decommission access to any/all data systems where access was previously allowed. 4. Consultant or contractor remote access via VPN resources or on-prem access via wireless guest account must have a finite duration based on project scope and timeframe.		

Status		**(4) Enhancing:** Current process for "resource provisioning" is effective so long as HR staff reports changes in a timely manner and technology/data managers perform the desired task for removing access from users whose employment terminates, embarks on approved leave of absence, or whose contracted service engagement completes. Advanced notifications allow an expiration date and time to be set in for a user in eDirectory in advance, which disables the account once that benchmark is reached. LDAP integration with eDirectory is used across several systems, so centralized account management is automated to some extent. Other systems are managed independently, and account expiration is handled by associated technology/data managers based on workflow preferences. The implementation of Micro Focus Identity Manager service interfaces between our student information system (Genesis) and several other key systems has been completed so that employment or student enrollment status changes lead to network resource access changes in an automated way.		
Users	**6.2**	**Establish an Access Revoking Process** Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	**IG1** **IG2** **IG3**	**Protect**
Tools		1. Genesis SIS (Data Exchange Source for Multi-System User Provisioning) 2. NetIQ eDirectory – Multi-System LDAP Authentication Provider 3. On-Prem Active Directory (AD) 4. Micro Focus Identity Manager (eDirectory & Active Directory Bi-Directional Drivers) 5. Google Cloud Directory Services (GCDS) 6. Microsoft School Directory Sync - SDS (Azure AD/O365 Provisioning) 7. Apple School Manager - ASM (Managed Apple ID Provisioning) 8. Clever SSO		
Process		1. Implementation of account provisioning and decommissioning via automated tools. 2. Maintain "network resource provisioning" process to establish communications between human resources, department leaders and technology/data security managers so that changes in employment status for staff members are communicated to all with relevant data elements. 3. Data managers are to respond to reported "end of employment," or "leave of absence" notifications and disable authentication privileges or otherwise decommission access to any/all data systems where access was previously allowed. 4. Consultant or contractor remote access via VPN resources must have a finite duration based on project scope and timeframe.		

Status		**(4) Enhancing:** Current process for "resource provisioning" is effective so long as HR staff reports changes in a timely manner and technology/data managers perform the desired task for removing access from users whose employment terminates, embarks on approved leave of absence, or whose contracted service engagement completes. Advanced notifications allow an expiration date and time to be set in for a user in eDirectory in advance, which disables the account once that benchmark is reached. LDAP integration with eDirectory is used across several systems, so centralized account management is automated to some extent. Other systems are managed independently, and account expiration is handled by associated technology/data managers based on workflow preferences. The implementation of Micro Focus Identity Manager service interfaces between our student information system (Genesis) and several other key systems has been completed so that employment or student enrollment status changes lead to network resource access changes in an automated way.		
Users	**6.3**	**Require MFA for Externally-Exposed Applications** Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	IG1 IG2 IG3	**Protect**
Tools		1. Biometrics 2. Hardware Tokens 3. SMS Text Messaging 4. Time-Based One Time Password (TOTP) with Authentication App 5. Push Notification		
Process		1. Implement multi-factor authentication for all user accounts on existing systems that hold sensitive data. 2. Subscribe to a third-party authentication provider service (e.g., Duo) to implement multi-factor authentication for user accounts on existing systems that do not support it natively.		
Status		**(3) Maintaining**: Multi-factor authentication now enforced in the Google Workspace application, Genesis SIS, Cisco AnyConnect VPN, and Systems 3000 Accounting/Payroll for all staff users, and administrator-level accounts on specific third-party cloud-based systems, with some requiring it in corporate policy terms and conditions.		
Network	**6.4**	**Require MFA for Remote Network Access** Require MFA for remote network access.	IG1 IG2 IG3	**Protect**
Tools		1. Biometrics 2. Hardware Tokens 3. SMS Text Messaging 4. Time-Based One Time Password (TOTP) with Authentication App 5. Push Notification		
Process		1. Implement multi-factor authentication for all user accounts on existing systems that hold sensitive data. 2. Subscribe to a third-party authentication provider service (e.g., Duo) to implement		

Status		**(3) Maintaining**: Multi-factor authentication now enforced in the Google Workspace application, Genesis SIS, Cisco AnyConnect VPN, and Systems 3000 Accounting/Payroll for all staff users, and administrator-level accounts on specific third-party cloud-based systems, with some requiring it in corporate policy terms and conditions.		
Users	**6.5**	**Require MFA for Administrative Access** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	IG1 IG2 IG3	**Protect**
Tools		1. Biometrics 2. Hardware Tokens 3. SMS Text Messaging 4. Time-Based One Time Password (TOTP) with Authentication App 5. Push Notification		
Process		1. Implement multi-factor authentication for administrator-level accounts on existing systems that support it. 2. Subscribe to a third-party authentication provider service (e.g., Duo) to implement multi-factor authentication for administrator-level accounts on existing systems that do not support it natively.		
Status		**(3) Maintaining**: Multi-factor authentication is currently enforced on most administrator-level accounts on specific third-party cloud-based systems, with some requiring it in corporate policy terms and conditions.		
Users	**6.6**	**Establish and Maintain an Inventory of Authentication and Authorization Systems** Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.	IG2 IG3	**Identify**
Tools		1. Voorhees Technology for Digital Learning Plan 2023-26, Appendix C: Software Resources – Operations, Communications, Security & Management		
Process		1. Publish inventory in district technology plan during the revision process every 3 years 2. Edit working revision of the technology plan in an ongoing basis as new products or services come online.		
Status		**(3) Maintaining**: Inventory is available in district's technology plan and is revised periodically.		

Users	**6.7**	**Centralize Access Control** Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.	IG2 IG3	**Protect**
Tools		1. Genesis SIS (Data Exchange Source for Multi-System User Provisioning) 2. NetIQ eDirectory – Multi-System LDAP Authentication Provider 3. On-Prem Active Directory (AD) 4. Micro Focus Identity Manager (eDirectory & Active Directory Bi-Directional Drivers) 5. Google Cloud Directory Services (GCDS) 6. Microsoft School Directory Sync - SDS (Azure AD/O365 Provisioning) 7. Apple School Manager - ASM (Managed Apple ID Provisioning) 8. Clever SSO 9. Meraki Dashboard Lobby Ambassador – Wireless Guest Account Provisioning 10. Cisco Identity Services Engine (ISE) - BYOD Devices		
Process		1. Use iManager (eDirectory) to establish user account management for network storage, printing, web content, miscellaneous database applications, local Windows Dynamic User Policy, staff & student BYOD wireless network. 2. Leverage LDAP integration feature where available in current applications, network and security devices to centralize access policies linked to eDirectory. 3. Use Genesis SIS file transfers to provision access for students and staff via: a) Google Cloud Directory Services (GCDS) b) Microsoft School Directory Sync - SDS (Azure AD/O365 Provisioning) c) Apple School Manager - ASM (Managed Apple ID Provisioning) d) Clever SSO		
Status		**(4) Enhancing**: eDirectory (domain), local server, appliance and PC security policies are managed centrally by the Director of Technology to minimize risk. Explicit group membership (security) assignments are either made directly or propagated via LDAP (linked to eDirectory security assignments). Several applications support Active Directory integration over LDAP, so this creates some limitations. We are now running a local AD environment synchronized with eDirectory to resolve that issue. Other systems only provide localized user management, however not many. Other provisioning is conducted through file transfer between our SIS and identity management and SSO platforms.		
Data	**6.8**	**Define and Maintain Role-Based Access Control** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.	IG3	**Protect**
Tools		1. All data and systems management assets, both on-prem and cloud-based 2. Automated user provisioning data exchange rules for LDAP, IDM, and direct mapping configurations 3. Voorhees Technology for Digital Learning Plan 2023-26, Action Plan 4: Data & Privacy		

Process	1. Determine correlation between users and/or groups with the level of access required in each asset based on the built-in roles available. 2. Adhere to relevant action items in the district's technology plan, specifically 4.2 Data Policies, Procedures and Practices.
Status	**(3) Maintaining**: Action items related to data policies, procedures and practices are available in district's technology plan, which is modified continuously and revised every three years.

CSC 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

CSC 7: Continuous Vulnerability Management				
CSC 7 Rating: 4.00				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Applications	**7.1**	**Establish and Maintain a Vulnerability Management Process** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	IG1 IG2 IG3	**Protect**
Tools		1. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 2. Center for Internet Security (CIS) Configuration Assessment Tool 3. Micro Focus ZCM Patch Management System (ZPM)		
Process		1. Implement Secure Endpoint Connector to perform vulnerability scanning on local systems, perform cloud lookup to check file disposition for files executed, moved or copied, and identify all vulnerable computers and their vulnerable applications. 2. Schedule period scans of all systems to gather vulnerability data for analysis. 3. Remediate with patch management process.		
Status		**(4) Enhancing:** Current tools in place can track changes in system and application files and show the number of vulnerable applications that have been executed, moved, or copied, together with the number of vulnerable computers. Whenever an executable file is moved, copied, or executed, the Secure Endpoint Connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database, that information is displayed.		
Applications	**7.2**	**Establish and Maintain a Remediation Process** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	IG1 IG2 IG3	**Respond**

Tools		1. Center for Internet Security (CIS) Configuration Assessment Tool 2. Micro Focus ZCM Patch Management System (ZPM) 3. Automatic Updates Enabled		
Process		1. Compare vulnerability scan logs to detect anomalies and prioritize action. 2. Acquire patches to resolve discovered vulnerabilities based on prioritization. 3. Schedule patch rollout based on level of associated risk.		
Status		**(4) Enhancing:** Current tools in place provides "The Top Vulnerable Applications" table which displays the top vulnerable applications in order of severity, the version number, the number of executions, the number of CVEs, and their severity. The Top Vulnerable Computers table displays the top vulnerable computers and the number of vulnerable applications on the computers, which are targeted by ZCM Patch Management for remediation.		
Applications	**7.3**	**Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	IG1 IG2 IG3	**Protect**
Tools		1. Micro Focus ZCM Patch Management System (ZPM) 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Automatic Updates Enabled		
Process		1. Implement combination of automatic updates along with targeted patch deployments or updates based on available intelligence data as necessary. 2. Periodically perform manual patch checks and deployments, engaging end users to perform these actions on resources they use on a regular basis, where applicable.		
Status		**(4) Enhancing:** Patch management practices continue to be a deliberate pursuit, using features available each of our existing device management platforms, device operating systems and the applications themselves. Efforts to coordinate patch deployments with published OS and application vulnerabilities are made.		
Applications	**7.4**	**Perform Automated Application Patch Management** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	IG1 IG2 IG3	**Protect**
Tools		1. Micro Focus ZCM Patch Management System (ZPM) 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Automatic Updates Enabled		
Process		1. Implement combination of automatic updates along with targeted patch deployments or updates based on available intelligence data as necessary. 2. Periodically perform manual patch checks and deployments, engaging end users to perform these actions on resources they use on a regular basis, where applicable.		

Status		**(4) Enhancing:** Patch management practices continue to be a deliberate pursuit, using features available each of our existing device management platforms, device operating systems and the applications themselves. Efforts to coordinate patch deployments with published OS and application vulnerabilities are made.		
Applications	**7.5**	**Perform Automated Vulnerability Scans of Internal Enterprise Assets** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.	IG2 IG3	**Identify**
Tools		1. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 2. Center for Internet Security (CIS) Configuration Assessment Tool 3. Cybersecurity and Infrastructure Security Agency (CISA) Cyber Health Assessment		
Process		1. Implement Secure Endpoint Connector to perform vulnerability scanning on local systems, perform cloud lookup to check file disposition for files executed, moved or copied, and identify all vulnerable computers and their vulnerable applications. 2. Schedule period scans of all systems to gather vulnerability data for analysis. 3. Perform continuous weekly CISA vulnerability scans (Nessus) of Internet-facing		
Status		**(4) Enhancing:** Current tools in place can track changes in system and application files and show the number of vulnerable applications that have been executed, moved, or copied, together with the number of vulnerable computers. Whenever an executable file is moved, copied, or executed, the Secure Endpoint Connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database, that information is displayed.		
Applications	**7.6**	**Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.	IG2 IG3	**Identify**
Tools		1. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 2. Center for Internet Security (CIS) Configuration Assessment Tool 3. Cybersecurity and Infrastructure Security Agency (CISA) Cyber Health Assessment		
Process		1. Implement Secure Endpoint Connector to perform vulnerability scanning on local systems, perform cloud lookup to check file disposition for files executed, moved or copied, and identify all vulnerable computers and their vulnerable applications. 2. Schedule period scans of all systems to gather vulnerability data for analysis. 3. Perform continuous weekly CISA vulnerability scans (Nessus) of Internet-facing resources.		

Status		**(4) Enhancing:** Current tools in place can track changes in system and application files and show the number of vulnerable applications that have been executed, moved, or copied, together with the number of vulnerable computers. Whenever an executable file is moved, copied, or executed, the Secure Endpoint Connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database, that information is displayed.		
Application	**7.7**	**Remediate Detected Vulnerabilities** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	**IG2** **IG3**	**Respond**
Tools		1. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 2. Center for Internet Security (CIS) Configuration Assessment Tool 3. Multi-State Information Sharing and Analysis Center (MS-ISAC) – Advisories 4. Center for Internet Security, Inc. (CIS) – Controls, Benchmarks & Tools 5. Homeland Security Information Network (HSIN) 6. NJ Cybersecurity & Communications Integration Cell – Bulletins 7. Deloite Cyber Detect & Respond Team – Cyber Threat Briefings 8. Cybersecurity and Infrastructure Security Agency (CISA) Cyber Health Assessment		
Process		1. Capture vulnerability scan logs to detect new events targeting intelligence data provided as a service by multiple cybersecurity resources (subscription services). 2. Review weekly CISA Cyber Hygiene reports from vulnerability scans and act to remediate identified threats.		
Status		**(4) Enhancing:** Current tools in place provides “The Top Vulnerable Applications” table which displays the top vulnerable applications in order of severity, the version number, the number of executions, the number of CVEs, and their severity. The Top Vulnerable Computers table displays the top vulnerable computers and the number of vulnerable applications on the computers.		

CSC 8: Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

CSC 8: Audit Log Management				
CSC 8 Rating: 3.25				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Network	**8.1**	**Establish and Maintain an Audit Log Management Process** Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	IG1 IG2 IG3	**Protect**
Tools		1. All network equipment and installed OS and installed applications. 2. Cisco SecureX		
Process		1. Implement standardized logging on each device, OS and installed applications. 2. Identify storage location for log data. 3. Identify procedures for accessing and reviewing log data. 4. Monitor storage status and maintain satisfactory available size for log repositories. 5. Configure log rotation/retention configuration to ensure availability of both the data and the available storage for future data gathering. 6. Implement Cisco SecureX on infrastructure to unify visibility, enable automation, and strengthen security across network, endpoints, cloud, and applications.		
Status		**(3) Maintaining:** Most installed equipment has log collecting capability and network administrators practice auditing the logs regularly.		
Network	**8.2**	**Collect Audit Logs** Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	IG1 IG2 IG3	**Detect**

Tools	1. Cisco Firepower Threat Defense 2140 (FTD) 2. Cisco Identity Services Engine (ISE) - BYOD Devices 3. Meraki Dashboard 4. Cisco FirePower Management Center (FMC) - Wired & Wireless Devices 5. Cisco Umbrella (OpenDNS) - Wired & Wireless Devices 6. Cisco SecureX
Process	1. Implement standardized logging on each device. 2. Identify procedures for accessing and reviewing log data. 3. Review log data periodically on a regular schedule. 4. Implement Cisco SecureX on infrastructure to unify visibility, enable automation, and strengthen security across network, endpoints, cloud, and applications.
Status	**(4) Enhancing**: Logs are reviewed periodically to monitor for unauthorized attached devices, file exchanges, and network traffic. Logs are also used for problem identification and resolution tasks. Log review frequency should be generally increased.

Network	**8.3**	**Ensure Adequate Audit Log Storage** Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	IG1 IG2 IG3	**Protect**
Tools		1. All network equipment and installed OS and installed applications. 2. Cisco SecureX		
Process		1. Implement standardized logging on each device, OS and installed applications. 2. Identify storage location for log data. 3. Monitor storage status and maintain satisfactory available size for log repositories. 4. Configure log rotation/retention configuration to ensure availability of both the data and the available storage for future data gathering. 5. Implement Cisco SecureX on infrastructure to unify visibility, enable automation, and strengthen security across network, endpoints, cloud, and applications. 6.		
Status		**(3) Maintaining:** Most installed equipment has log collecting capability. Network administrators maintain available storage by managing log rotation/retention configuration when possible, otherwise old logs are removed whenever storage capacity is reached.		
Network	**8.4**	**Standardize Time Synchronization** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.	IG2 IG3	**Protect**

Tools		Network Time Servers: 1. VTSERV2 2. VMSSERV2 3. VMS4510R		
Process		1. Configure internal network time provider to obtain their time via Internet-based NTP server pools. 2. Check all network equipment to make sure one or more of these listed network time servers are configured and used. 3. Reconfigure time provider(s) on any equipment that uses a different time provider.		
Status		**(4) Enhancing**: All devices are using the listed time provider(s), with these configured to use established Internet-based NTP server pools.		
Network	**8.5**	**Collect Detailed Audit Logs** Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.	IG2 IG3	**Detect**
Tools		1. All network equipment and installed OS and installed applications.		
Process		1. Implement standardized logging on each device, OS and installed applications. 2. Identify procedures for accessing and reviewing log data. 3. Review log data periodically on a regular schedule.		
Status		**(3) Maintaining:** Most installed equipment has log collecting capability and network administrators practice auditing the logs regularly.		
Network	**8.6**	**Collect DNS Query Audit Logs** Collect DNS query audit logs on enterprise assets, where appropriate and supported.	IG2 IG3	**Detect**
Tools		1. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 2. Cisco Cloud E-Mail Security Appliance (ESA)		
Process		1. Implement Umbrella (OpenDNS) secure internet gateway platform to secure network and roaming clients through threat intelligence. 2. Review/analyze threat data supplied weekly by Multi-State Information Sharing and Analysis Center (MS-ISAC) for lists of reported malware propagating IP addresses and domains for manual firewall blacklist maintenance. 3. Implement ESA with AMP threat intelligence and reputation filtering features		

Status		**(4) Enhancing**: District's security appliances and end-point security resources provide best-in-class protection. All Cisco products are licensed with AMP, which is integrated with the Cisco Talos Security Intelligence and Research Group for detection, analysis and protection against known and emerging treats.		
Network	**8.7**	**Collect URL Request Audit Logs** Collect URL request audit logs on enterprise assets, where appropriate and supported.	IG2 IG3	**Detect**
Tools		1. Cisco Firepower Threat Defense 2140 (FTD) 2. Cisco Identity Services Engine (ISE) - BYOD Devices 3. Cisco FirePower Management Center (FMC) - Wired & Wireless Devices 4. Cisco Umbrella (OpenDNS) - Wired & Wireless Devices 5. Meraki Dashboard		
Process		1. Enable URL logging on each resource listed 2. Configure specific periodic reports to be generated and sent based on set criteria 3. Use data to investigate user behavior or to troubleshoot connectivity issues as needed.		
Status		**(4) Enhancing**: All devices are capable of logging URL requests, and several tools are available for monitoring or incident investigation.		
Devices	**8.8**	**Collect Command-Line Audit Logs** Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.	IG2 IG3	**Detect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) – Group Policy Configuration		
Process		1. Desktop and Laptop computers are deployed via an imaging process and the Windows local user account is created dynamically based on a ZCM policy which successful authentication in eDirectory. User group membership determines the GPOs and applications assigned to the user on the device with the ZCM agent constantly polling eDirectory as a user source. 2. Audit Process Creation policy is enabled on every Windows device, and the command line information for every process will be logged in plain text in the security event log as part of the Audit Process Creation event 4688 3. View logs as necessary in Event Viewer		
Status		**(3) Maintaining:** All Windows devices have log collecting capability. Network administrators must practice auditing the logs regularly, or in the investigation of an incident.		

Network	**8.9**	**Centralize Audit Logs** Centralize, to the extent possible, audit log collection and retention across enterprise assets.	IG2 IG3	**Detect**
Tools		1. All network equipment and installed OS and installed applications. 2. Cisco SecureX		
Process		1. Implement standardized logging on each device, OS and installed applications. 2. Learn procedures for accessing and reviewing log data. 3. Review log data periodically on a regular schedule. 4. Implement Cisco SecureX on infrastructure to unify visibility, enable automation, and strengthen security across network, endpoints, cloud, and applications.		
Status		**(3) Maintaining:** Although most installed equipment has log collecting capability, although some logs are currently not centrally located and network administrators must practice auditing the independent logs regularly, SecureX integrates Cisco's security product data within a single pane of glass.		
Network	**8.10**	**Retain Audit Logs** Retain audit logs across enterprise assets for a minimum of 90 days.	IG2 IG3	**Protect**
Tools		1. All network equipment and installed OS and installed applications.		
Process		1. Implement standardized logging on each device, OS and installed applications. 2. Identify storage location for log data. 3. Monitor storage status and maintain satisfactory available size for log repositories. 4. Configure log rotation/retention configuration to ensure availability of both the data and the available storage for future data gathering.		
Status		**(3) Maintaining:** Most installed equipment has log collecting capability. Network administrators maintain available storage by managing log rotation/retention configuration when possible, otherwise the default retention durations is used. Old logs are removed whenever storage capacity is reached.		
Network	**8.11**	**Conduct Audit Log Reviews** Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.	IG2 IG3	**Detect**
Tools		1. All network equipment and installed OS and installed applications.		
Process		1. Implement standardized logging on each device, OS and installed applications. 2. Learn procedures for accessing and reviewing log data. 3. Review log data periodically on a regular schedule.		

Status		**(3) Maintaining:** Most installed equipment has log collecting capability. Network administrators must practice auditing the logs regularly, or in the investigation of an incident.		
Data	**8.12**	**Collect Service Provider Logs** Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.	**IG3**	**Detect**
Tools		1. Hosted Database Servers (Google Workspace, Microsoft Office 365Clever, Apple School Manager, Frontline, iObservation, Systems 3000, etc.)		
Process		1. Implement standardized logging in each environment, hosted OS and installed applications. 2. Learn procedures for accessing and reviewing log data. 3. Review log data periodically on a regular schedule.		
Status		**(3) Maintaining:** Most hosted environments have log collecting capability. Network administrators must practice auditing the logs regularly, or in the investigation of an incident.		

CSC 9: Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

CSC 9: Email and Web Browser Protections				
CSC 9 Rating: 4.00				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Applications	**9.1**	**Ensure Use of Only Fully Supported Browsers and Email Clients** Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	IG1 IG2 IG3	**Protect**
Tools		1. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 2. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 3. Jamf Pro Mobile Device Management (JSS) - iOS Devices 4. Micro Focus ZCM Patch Management System (ZPM)		
Process		1. Monitor vendor browser update/upgrade availability and initiate update process or push new installation via device management resources. 2. Identify needed browser updates by performing regular vulnerability scanning 3. Configure browser products to auto-update whenever new versions become available. 4. Direct end users to initiate browser version updates, whenever it is determined that other approaches were not successful.		
Status		**(4) Enhancing**: Browsers generally auto-update, users manually update when reminded to do so, and periodic manual push installs are scheduled annually. Heightened efforts to increase frequency of push installs since implementation of vulnerability scanning and subsequent report data.		
Network	**9.2**	**Use DNS Filtering Services** Use DNS filtering services on all enterprise assets to block access to known malicious domains.	IG1 IG2 IG3	**Protect**

Tools		1. **Domain-Based Security** - Umbrella Virtual Appliances (VAs). VAs are lightweight virtual machines that are compatible with the district's VMWare ESX/ESXi environment. When utilized as conditional DNS forwarders on the network, Umbrella VAs record the internal IP address information of DNS requests for usage in reports, security enforcement, and category filtering policies. Additionally, VAs encrypt and authenticate DNS data for enhanced security. 2. **Internal DNS Servers** - The DNS software in Open Enterprise Server integrates DNS information into eDirectory, our network object management environment. Integrating DNS with eDirectory greatly simplifies network administration by enabling us to enter all configuration information into one distributed database. The DNS configuration information is replicated just like any other data in eDirectory. The concept of a primary or secondary has been shifted away from the server to the zone itself. After you have configured the zone, the data is available to any of the OES DNS servers you select to make authoritative for the zone. The OES DNS server takes advantage of the peer-to-peer nature of eDirectory by replicating the DNS data. 3. **DNS Forwarding** - Our internal DNS environment uses OpenDNS servers as DNS Forwarders, rather than our ISP's DNS servers. OpenDNS offers DNS services that are faster and more reliable than any other DNS service. With OpenDNS we more quickly reach our intended website and never experience the outages that occur with the DNS services provided by an ISP. In terms of security, OpenDNS has solid security capabilities and will block malicious websites, or allow blacklists of certain websites.		
Process		1. Umbrella VA addresses are dynamically assigned as DNS servers in the TCPIP configuration to all devices via DHCP. 2. Umbrella VAs determines whether the host being contacted by a device is internal or external. **3.** If internal, DNS resolution is handled via OES DNS servers integrated with eDirectory. If external, OpenDNS server forwarding addresses are used to resolve hosts outside the network, with domain level security based on security intelligence.		
Status		**(4) Enhancing:** Current tools in place provide fast name resolution for internal and external hosts, and they contribute to our multi-layered network security architecture.		
Network	**9.3**	**Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.	IG2 IG3	**Protect**
Tools		1. Cisco FirePower Management Center (FMC) - Wired & Wireless Devices 2. Cisco Umbrella (OpenDNS) - Wired & Wireless Devices 3. Cisco Umbrella Windows Roaming Client and iOS Security Connecter 4. Meraki Dashboard		

Process		1. Implement URL request logging to filter traffic for all district-owned or personally-owned devices connected to the district's network either locally or via remote VPN access. 2. Select, acquire and implement security solution for district-owned mobile devices so that URL requests may be filtered regardless of the network on which connected.		
Status		**(4) Enhancing**: Multiple resources available for monitoring, allowing and restricting the URL traffic of all devices attached to the district's network as well as when attached to remote networks.		
Applications	**9.4**	**Restrict Unnecessary or Unauthorized Browser and Email Client Extensions** Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.	IG2 IG3	**Protect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Jamf Pro Mobile Device Management (JSS) - iOS Devices 3. Cisco FirePower Management Center (FMC) - Wired & Wireless Devices 4. Cisco Umbrella (OpenDNS) - Wired & Wireless Devices 5. Cisco Cloudlock – Cloud Content Management 6. Meraki Dashboard		
Process		1. Continue push installations of approved e-mail client software and version upgrades via ZCM. 2. Disable unwanted PC applications via Windows Group Policy deployment tools in ZCM. 3. Disable unwanted iOS applications via Smart Group identification in JSS, as well as in Cisco Umbrella and Cloudlock portals 4. Configure and push install desired student and staff e-mail configuration policy via JSS. 5. Disable access to personal web-based e-mail using content filtering via policies in FMC, JSS & Umbrella		
Status		**(4) Enhancing**: Organization approved e-mail client/version/ is pushed out to all devices via device management systems. Application blacklisting is performed as needed using device management systems and personal web-based e-mail portal access is blocked for all users via content filtering resources.		
Network	**9.5**	**Implement DMARC** To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.	IG2 IG3	**Protect**
Tools		1. Comcast Business Class Internet Support 2. Cisco Cloud E-Mail Security Appliance (ESA) 3. Google Admin Console - Advanced Settings for Gmail		

Process		1. Open support ticket with ISP to modify DNS MX record to include proper SFP record for mail domain, then test. 2. Turn on SPF Verification feature in ESA Mail Flow Policy security features options. 3. Maintain enabled Sender DNS Verification feature in ESA Mail Flow Policy.		
Status		**(4) Enhancing**: Multiple resources available for monitoring, allowing and restricting the flow of inbound e-mail message traffic. Additional security enhancements with SPF and DKIM standards are currently in place.		
Network	**9.6**	**Block Unnecessary File Types** Block unnecessary file types attempting to enter the enterprise's email gateway.	IG2 IG3	**Protect**
Tools		1. Cisco Cloud E-Mail Security Appliance (ESA)		
Process		1. Continue to implement File Reputation and File Analysis security features via ESA Advance Malware Protection (AMP) feature. 2. Continue to implement ESA Content Scanner Tools with Anti-Virus subscription-based security. 3. Continue to implement URL Filtering and Web Interaction Tracking features via ESA security.		
Status		**(4) Enhancing**: District's e-mail security appliance is configured as a mail relay between the district's e-mail system and the Internet. E-mail attachments are scanned in all inbound and outbound message. A multi-layered approach exists, including file reputation, file analysis and anti-virus scanning.		
Network	**9.7**	**Deploy and Maintain Email Server Anti-Malware Protections** Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	IG3	**Protect**
Tools		1. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 2. Cisco Cloud E-Mail Security Appliance (ESA) w/ Advanced Malware Prevention (AMP) 3. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 4. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 5. Google Admin Console		
Process		1. Continue implementation of listed security products on devices to include PCs, Windows servers and iOS devices. 2. Monitor FMC, ESA, and Secure Endpoint detection and remediation activity based on AMP Threat Grid intelligence via available system reporting tools. 3. Explore options for consolidation of all resource logs and reports.		

Status	**<u>(4) Enhancing</u>**: District's security appliances and end-point security resources provide best-in-class protection. All Cisco products are licensed with AMP, which is integrated with the Cisco Talos Security Intelligence and Research Group for detection, analysis and protection against known and emerging treats. Agent status for Secure Endpoint and Security Connector may be monitored via AMP portal. Google Enterprise for Education licensing provided enhanced security tools (e.g., Investigate, etc.) for protecting the e-mail environment in Google workspace for Education.

CSC 10: Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

CSC 10: Malware Defenses				
		CSC 10 Rating: 3.57		
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Devices	**10.1**	**Deploy and Maintain Anti-Malware Software** Deploy and maintain anti-malware software on all enterprise assets.	IG1 IG2 IG3	**Protect**
Tools		1. Cisco Cloud E-Mail Security Appliance (ESA) w/ Advanced Malware Prevention (AMP) 2. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 3. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 4. Cisco Identity Services Engine (ISE) 5. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 6. Cisco Secure Endpoint Connector 7. Cisco Umbrella Windows Roaming Client and iOS Security Connecter 8. Cisco SecureX		
Process		1. Continue implementation of listed security products on devices to include PCs, Windows servers and iOS devices. 2. Select and implement anti-malware solution for Linux servers. 3. Monitor FMC, ESA, Umbrella, and Secure Endpoint detection and remediation activity via available system reporting tools. 4. Explore options for consolidation of all resource logs and reports. 5. Implement Cisco SecureX on infrastructure to unify visibility, enable automation, and strengthen security across network, endpoints, cloud, and applications.		
Status		**(4) Enhancing**: District's security appliances and end-point security resources provide best-in-class protection. Leveraging automation in reporting and remediation to reduce administrative efforts is desirable, and SecureX integrates Cisco's security product data within a single pane of glass.		
Devices	**10.2**	**Configure Automatic Anti-Malware Signature Updates** Configure automatic updates for anti-malware signature files on all enterprise assets.	IG1 IG2 IG3	**Protect**

Tools		1. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 2. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 3. Cisco Identity Services Engine (ISE) 4. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 5. Cisco Secure Endpoint Connector 6. Cisco Umbrella Windows Roaming Client and iOS Security Connecter		
Process		1. Continue implementation of listed security products on devices to include PCs, Windows servers and iOS devices. 2. Select and implement anti-malware solution for Linux servers. 3. Monitor FMC, ESA, Umbrella, and Secure Endpoint detection and remediation activity via available system reporting tools. 4. Explore options for consolidation of all resource logs and reports.		
Status		**(4) Enhancing**: District's security appliances and end-point security resources provide best-in-class protection. All Cisco products are licensed with AMP, which is integrated with the Cisco Talos Security Intelligence and Research Group for detection, analysis and protection against known and emerging treats. Agent status for Secure Endpoint and Security Connector may be monitored via AMP portal.		
Devices	**10.3**	**Disable Autorun and Autoplay for Removable Media** Disable autorun and autoplay auto-execute functionality for removable media.	IG1 IG2 IG3	**Protect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 3. Cisco Identity Services Engine (ISE) 4. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP)		
Process		1. Enable building administrator to grant guest wireless network access as needed by providing access to a periodically changing pre-shared key for distribution. 2. Apply ACLs are to this network preventing guest user access to internal resources. 3. Make BYOD wireless network access available to all staff and to students with parental permission for academic use. 4. Leverage ISE to perform LDAP lookup to grant or deny access based on group membership in eDirectory. 5. Implement ISE to allow for device Posturing and Profiling conditional access rules for both wired and wireless networks. 6. Configure integration between ISE and FMC to perform identity-based device threat detection. 7. Disable auto-run on removable devices is possible via Windows Group Policy deployment tools in ZCM. 8. Configure anti-virus agent to conduct automatic scan of removable devices at time of insertion.		

Status		**(3) Maintaining**: Multiple resources available for managing endpoint security. Wireless network threat prevention measures in place surpass wired network measures, which must be enhanced. Identity based access and activity monitoring features must be leveraged more so than they are now. Capabilities exist for managing automated behaviors associated with removable storage devices, and policies in ZCM and Secure Endpoint have been enabled.		
Devices	**10.4**	**Configure Automatic Anti-Malware Scanning of Removable Media** Configure anti-malware software to automatically scan removable media.	**IG2** **IG3**	**Detect**
Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 3. Cisco Identity Services Engine (ISE) 4. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP)		
Process		1. Enable building administrator to grant guest wireless network access as needed by providing access to a periodically changing pre-shared key for distribution. 2. Apply ACLs are to this network preventing guest user access to internal resources. 3. Make BYOD wireless network access available to all staff and to students with parental permission for academic use. 4. Leverage ISE to perform LDAP lookup to grant or deny access based on group membership in eDirectory. 5. Implement ISE to allow for device Posturing and Profiling conditional access rules for both wired and wireless networks. 6. Configure integration between ISE and FMC to perform identity-based device threat detection. 7. Disable auto-run on removable devices is possible via Windows Group Policy deployment tools in ZCM. 8. Configure anti-virus agent to conduct automatic scan of removable devices at time of insertion.		
Status		**(3) Maintaining**: Multiple resources available for managing endpoint security. Wireless network threat prevention measures in place surpass wired network measures, which must be enhanced. Identity based access and activity monitoring features must be leveraged more so than they are now. Capabilities exist for managing automated behaviors associated with removable storage devices, and policies in ZCM and Secure Endpoint have been enabled.		
Devices	**10.5**	**Enable Anti-Exploitation Features** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.	**IG2** **IG3**	**Protect**

Tools		1. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 2. Enhanced Mitigation Experience Toolkit (EMET)		
Process		1. Use Windows Group Policy deployment tools in ZCM to enable DEP for "all essential Windows programs and services only" on all Windows PCs. 2. Use Windows Group Policy deployment tools in ZCM to ensure that ASLR is enabled on all Windows PCs. 3. Consider implementation of EMET and/or successor products on all PCs to fine-tune Windows security features.		
Status		**(3) Maintaining**: DEP and ASLR are enabled by default on all Windows PCs, and ASLR is enabled on all iOS devices. Future experimentation with EMET will determine relevance in our environment.		
Devices	**10.6**	**Centrally Manage Anti-Malware Software** Centrally manage anti-malware software.	IG2 IG3	**Protect**
Tools		1. Cisco Cloud E-Mail Security Appliance (ESA) w/ Advanced Malware Prevention (AMP) 2. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 3. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 4. Cisco Identity Services Engine (ISE) 5. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 6. Cisco Secure Endpoint Connector 5. Cisco Umbrella Windows Roaming Client and iOS Security Connecter 6. Cisco SecureX		
Process		1. Continue implementation of listed security products on devices to include PCs, Windows servers and iOS devices. 2. Select and implement anti-malware solution for Linux servers. 3. Monitor FMC, ESA, Umbrella, and Secure Endpoint detection and remediation activity via available system reporting tools. 4. Explore options for consolidation of all resource logs and reports. 5. Implement Cisco SecureX on infrastructure to unify visibility, enable automation, and strengthen security across network, endpoints, cloud, and applications.		
Status		**(4) Enhancing**: District's security appliances and end-point security resources provide best-in-class protection. All Cisco products are licensed with AMP, which is integrated with the Cisco Talos Security Intelligence and Research Group for detection, analysis and protection against known and emerging treats. Talos shares intelligence data across all products, so leveraging automation in reporting and remediation to reduce administrative efforts is possible. SecureX integrates Cisco's security product data within a single pane of glass.		
Devices	**10.7**	**Use Behavior-Based Anti-Malware Software** Use behavior-based anti-malware software.	IG2 IG3	**Detect**

Tools	1. Cisco Cloud E-Mail Security Appliance (ESA) w/ Advanced Malware Prevention (AMP) 2. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 3. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 4. Cisco Identity Services Engine (ISE) 5. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 6. Cisco Secure Endpoint Connector 7. Cisco Umbrella Windows Roaming Client and iOS Security Connecter
Process	1. Implement endpoint security that employs advanced malware protection blocks known malware exploits accurately and efficiently without being solely dependent on signatures. 2. Implement endpoint security that employs continuous monitoring of all file activity results in faster detection of new threats. 3. Implement endpoint security that detects and mitigates zero-day attacks and other, more sophisticated malware. 4. Implement endpoint security with next-generation capabilities that include: a. Behavior-based malware detection, which builds a full context around every process execution path in real time b. Machine learning models, which identify patterns that match known malware characteristics and other various forms of artificial intelligence
Status	**(4) Enhancing**: The district deploys Cisco products with Advanced malware protection that provides prevention, detection, and response all in one solution and are generally highly automated. Their built-in, open platforms enable much simpler and more efficient workflows. All Cisco products are licensed with AMP, which is integrated with the Cisco Talos Security Intelligence and Research Group for detection, analysis and protection against known and emerging treats. Talos shares intelligence data across all products, so leveraging automation in reporting and remediation to reduce administrative efforts is possible.

CSC 11: Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

CSC 11: Data Recovery				
CSC 11 Rating: 3.60				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Data	**11.1**	**Establish and Maintain a Data Recovery Process** Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	IG1 IG2 IG3	**Recover**
Tools		1. VTSE Technology Disaster Recovery Plan (document)		
Process		1. Maintain documentation that includes: a. A prioritized list of critical services, data and contacts. b. A process enabling the district to restore any loss of data in the event of fire, vandalism, natural disaster or system failure. c. A process enabling the district to continue to operate in the event of fire, vandalism, natural disaster or system failure. d. Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary. 2. Publish for access by key personnel on district website		
Status		**(4) Enhancing**: Technology staff maintains a technology disaster recovery plan delineating the district's procedures for recovery from an unforeseen disaster or emergency. This plan contains process level procedures for recovering critical technology platforms, telecommunications infrastructure and ensuring data security. Controls ensure that the district can recover from any damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the Department of Technology for response to a system emergency or other occurrence (e.g., fire, vandalism, system failure and natural disaster) that damages data or systems.		

Data	**11.2**	**<u>Perform Automated Backups</u>** Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	**IG1** **IG2** **IG3**	**Recover**
Tools		1. Unitrends Recovery Series Backup Appliance, Removable Archive Drives & Cloud Storage for On-Prem Systems 2. Apple iCloud for Apple Devices 3. Google Vault & SysCloud Solutions for Google Workspace for Education Platform		
Process		1. Unitrends a. Maintain weekly Full (Master) Backup Job on all Windows and Linux server system, applications, and data file storage partitions. b. Maintain weekly Full (Master) Backup Job on all SQL database instances. c. Maintain daily Incremental Backup Job on all Windows and Linux server system, applications, and data file storage partitions. d. Maintain daily Backup Copy Hot Target uploads to Unitrends Cloud storage for offsite 90-day storage retention. e. Maintain weekly Backup Copy Cold Target uploads to removable Archive Drive (air gapped) storage for offsite 14-day storage retention. f. Leverage Unitrends backup appliance predictive analytics engine to detect anomalies consistent with malware, such as ransomware. g. Monitor daily backup logs to confirm success or identify/resolve any points of failure. 2. iCloud – Schedule nightly device backups for iOS devices 3. Google Vault & SyCloud – Continuous backup of Google Applications, such as Drive & Gmail		
Status		**<u>(4) Enhancing</u>**: High frequency of backup jobs with diversity of targets and types are conducted. Predictive analytics feature offers possibility for preemptive measures to reduce risking integrity of backup data, as well as providing actionable intelligence for addressing risks in live data stores. Multiple offsite backup copy solutions provide redundancy and promote success in disaster recovery measures, if needed.		
Data	**11.3**	**<u>Protect Recovery Data</u>** Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	**IG1** **IG2** **IG3**	**Protect**
Tools		1. Unitrends Recovery Series Backup Appliance, Removable Archive Drives & Cloud Storage		

Process		1. Ensure data center (location of backup appliance) doors are secured with keys/access provided only to authorized personnel. 2. Ensure offsite Archive Drive set (air gapped) is secured in locked quarters with keys/access provided only to authorized personnel. 3. Ensure Unitrends Cloud storage is secured with connection method and access credentials shared only with authorized personnel. 4. Enable backup appliance encryption feature to protect backup sets in storage. 5. Encrypt backups for specific protected assets when deemed necessary.		
Status		**(4) Enhancing**: Physical storage security measures have been taken and executed continuously. Backup appliance encryption feature is available and utilized. Backup copies stored offsite in cloud-based and air gapped media.		
Data	**11.4**	**Establish and Maintain an Isolated Instance of Recovery Data** Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.	IG1 IG2 IG3	**Recover**
Tools		1. Unitrends Recovery Series Backup Appliance, Removable Archive Drives & Cloud Storage		
Process		1. Maintain daily Backup Copy Hot Target uploads to Unitrends Cloud storage for offsite 90-day storage retention. 2. Maintain weekly Backup Copy Cold Target uploads to removable Archive Drive (air gapped) storage for offsite 14-day storage retention.		
Status		**(4) Enhancing**: Unitrends Recovery Series Backup Appliance uses agent-based or VM-based communications that do not provide addressable data shares, not continuously addressable in any way. Relocation of physical removable drives containing backup copies, as well as cloud backup copies provides desired data isolation.		
Data	**11.5**	**Test Data Recovery** Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.	IG2 IG3	**Recover**
Tools		1. Unitrends Recovery Series Backup Appliance, Removable Archive Drives & Cloud Storage 2. Apple iCloud for Apple Devices 3. Google Vault & SysCloud Solutions for Google Workspace for Education Platform		

Process	1. Conduct periodic restore jobs from backup appliance storage, cloud storage and archive job storage targeting original server storage path as restore target in order to assess data integrity. 2. Conduct periodic restore jobs from backup appliance storage, cloud storage and archive job storage targeting new server storage path as restore target in order to assess data integrity.
Status	**(3) Maintaining**: Period test restore jobs are conducted, but usually are actual needed restore incidents. Efforts should be made to conduct test restores during non-critical situations.

CSC 12: Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

CSC 12: Network Infrastructure Management				
CSC 12 Rating: 3.25				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Network	**12.1**	**Ensure Network Infrastructure is Up to Date** Ensure network infrastructure is kept up to date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	IG1 IG2 IG3	**Protect**
Tools		1. Cisco Catalyst Switching & InterVLAN Routing 2. Cisco HyperFlex HX Data Platform / VMware vSphere 3. Meraki Dashboard 4. Cisco Duo 5. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 6. Cisco Secure Endpoint Connector 7. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 8. Jamf Pro Mobile Device Management (JSS) - iOS Devices 9. Micro Focus ZCM Patch Management System (ZPM)		
Process		1. Maintain licensing and support contracts with device vendors so that software updates are available and accessible for deployment. 2. Make periodic evaluations of software version levels and patch status and engage in manual updates as needed. 3. Review published software benchmark data for vulnerability checks. 4. Review vendor or security organization provided software vulnerability alerts and take appropriate action. 5. Utilize automated software update processes where available.		
Status		**(4) Enhancing**: Access to support updates is available via annual support contract and licensing renewals. Beyond automated update and patch deployments, efforts to review security feature status in software version levels and react to changing software vulnerability conditions are now enhanced in terms of dedicated focus and response.		

Network	**12.2**	**Establish and Maintain a Secure Network Architecture** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.	IG2 IG3	**Protect**
Tools		1. Cisco Catalyst Switch InterVLAN Routing Configurations 2. Cisco HyperFlex HX Data Platform / VMware vSphere 3. Meraki Dashboard 4. iManager (eDirectory) – Password Policy for network storage, printing, web content, miscellaneous database applications, local Windows Dynamic User access via LDAP integration. 5. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 6. Jamf Pro Mobile Device Management (JSS) - iOS Devices		
Process		1. Create VLANs on network switches and associated interVLAN routing configurations. 2. Create VLANs in virtual network infrastructure associated interVLAN routing configurations. 3. Create separated wireless interfaces with independent IP subnet configurations and link them to associated SSIDs. 4. Establish and implement mandatory access policy for network/device administrators.		
Status		**(3) Maintaining**: Network segmentation exists as recommended, preventing non-routable layer 2 traffic from moving laterally across subnets. Workstations and other user devices reside on VLANs that do not contain servers or other critical resources, however no ACLs or firewall filtering resources are currently in use. Mandatory access policy for network/device administrators is in place, however there are no current means for monitoring adherence to the policy.		
Network	**12.3**	**Securely Manage Network Infrastructure** Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.	IG2 IG3	**Protect**
Tools		1. PuTTY (SSH) Client 2. Device(s) Secure Web UI w/SSL encryption 3. Cisco AnyConnect VPN Client 4. Device/Service Built-In Two-Factor Authentication Feature 5. Third-Party Multi-Factor Authentication Service Provided (e.g. DUO)		

Process	1. Implement encrypted SSH client for CLI management 2. Leverage appliance self-signed or commercial trusted root certificates to encrypt web page transmissions where possible. 3. Leverage secure VPN tunnel for remote management sessions. 4. Leverage built-in two-factor authentication on supported systems when feasible. 5. Investigate and select third-party two-factor authentication service to make authentication all-inclusive and standardize the process.			
Status	**(3) Maintaining:** Most device management CLI or WebUI approaches in use implement 128-bit or 256-bit encryption via self-signed certificates, however a few data systems currently use a commercially verified trusted root certificate. Some data systems provide two-factor authentication for either administration or user access. Enforcement of the use of two-factor authentication is being expanded in a global approach using a third-party authentication service provider (Cisco Duo).			
Network	**12.4**	**Establish and Maintain Architecture Diagram(s)** Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	IG2 IG3	**Identify**
Tools		1. Voorhees Technology for Digital Learning Plan 2023-26 (document) 2. Server/platform management As-Built Documentation		
Process		1. Network diagrams are included in Appendix B of the district's technology plan. 2. Resource configurations are recorded within the as-built documentation stored by the director of technology for each resource.		
Status		**(4) Enhancing**: Network architecture documentation is maintained and revised sufficiently as changes are made.		
Network	**12.5**	**Centralize Network Authentication, Authorization, and Auditing (AAA)** Centralize network AAA.	IG2 IG3	**Protect**
Tools		1. Cisco Firepower Threat Defense 2140 (FTD) 2. Cisco Identity Services Engine (ISE) 3. Cisco AnyConnect VPN Client		
Process		1. Review current status of public facing servers to assess business relevance. 2. Utilize secure LDAP integration via ISE for VPN and WLAN authentication. 3. Make modifications if needed by removing static IP mapping in FTD configuration.		
Status		**(4) Enhancing**: Periodic review of access rules are performed and changes are made as appropriate.		

Network	**12.6**	**Use of Secure Network Management and Communication Protocols** Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).	IG2 IG3	**Protect**
Tools		1. Meraki Dashboard		
Process		1. Configure WPA2 security on SSIDs for use by district-owned devices. 2. Configure 802.1X for personally-owned devices to authenticate via local Radius Servers - Cisco Identity Services Engine (ISE) 3. Configure open guest network using Meraki Cloud Authentication, with "Walled-Garden" configuration (Internet only) – clients unable to connect with other internal LAN resources.		
Status		**(4) Enhancing**: Best practices implemented for management of district-owned, personally-owned (staff & student BYOD), and controlled guest user device network access. AAA security is also provided via configuration of RADIUS server authentication (ISE).		
Devices	**12.7**	**Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure** Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.	IG2 IG3	**Protect**
Tools		1. Telnet, SSH, VNC, RDP 2. VMware vCenter 3. Micro Focus ZEN Configuration & Management System (ZCM) 4. Cisco AnyConnect VPN Client / Cisco Firepower Threat Defense 2140 (FTD)		
Process		1. Choose remote access applications for device administration that utilize encryption protocols. 2. Require secondary encryption channel (VPN) for performing off-site device administration tasks.		
Status		**(4) Enhancing:** Remote access applications for use in device administration utilize encryption protocols, and are used when management tasks are performed while directly connected to the district network on premises. Secure VPN connection is used when management tasks are performed while connected to the district network from a remote location.		
Network	**12.8**	**Establish and Maintain Dedicated Computing Resources for All Administrative Work** Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.	IG3	**Protect**

Tools	1. Additional Network Management Device(s), e.g., PC, Tablet, etc.) 2. Micro Focus ZEN Configuration & Management System (ZCM) - PC Desktops/Servers 3. Jamf Pro Mobile Device Management (JSS) - iOS Devices 4. Cisco Catalyst Switch(s) – Configured Wired VLAN Segmentation 5. Meraki Dashboard
Process	1. Provide each network administrator with an additional device for dedicated network management activities. 2. Limit device application access by policy via device management. 3. Create wired and wireless network segmentation for management device connections that provide access only to devices to be managed. 4. Implement use of dedicated device management port wherever available, rather than using the configured device implementation port(s). 5. Attach device management port to segmented, isolated VLAN for dedicated management purposes.
Status	**(2) Developing:** Devices that provide dedicated management ports are only being used when mandated in or to conserve available device switch ports, however their use should be considered in order to reduce unnecessary risk. Network segmentation is in place and used to separate resources, but not to isolate resource management from normal use.

CSC 13: Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

CSC 13: Network Monitoring and Defense				
CSC 13 Rating: 2.91				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Network	**13.1**	**Centralize Security Event Alerting** Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.	IG2 IG3	Detect
Tools		1. All network equipment and installed OS and installed applications. 2. Cisco SecureX		
Process		1. Implement standardized logging on each device, OS and installed applications. 2. Acquire and implement a SIEM tool for log consolidation, correlation and analysis 3. Learn procedures for accessing and reviewing aggregated log data. 4. Review log data periodically on a regular schedule. 5. Implement Cisco SecureX on infrastructure to unify visibility, enable automation, and strengthen security across network, endpoints, cloud, and applications.		
Status		**(3) Maintaining:** Most installed equipment has log collecting capability, but in most cases, logging must become enabled, SIEM resources must be deployed, and network administrators must know how and practice auditing the logs. SecureX integrates Cisco's security product data within a single pane of glass. All other logs, reports & alerts are viewed and managed independently.		
Devices	**13.2**	**Deploy a Host-Based Intrusion Detection Solution** Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.	IG2 IG3	Detect
Tools		1. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 2. Micro Focus ZEN Configuration & Management System (ZCM) 3. Cisco Identity Services Engine (ISE) 4. Cisco Secure Endpoint Connectors 5. Cisco Umbrella Windows Roaming Client and iOS Security Connecter 6. Cisco Duo 7. Cisco SecureX		

Process		1. Create database of port, protocol and services from vender documentation to be whitelisted on OS and endpoint security enabled firewalls. 2. Leverage device management tools to enforce restrictions based on policy. 3. Monitor traffic to ensure policy-based restrictions are working as planned. 4. Utilize existing tools for file integrity checking activity, based on their strengths and limitations. 5. Implement Cisco SecureX on infrastructure to unify visibility, enable automation, and strengthen security across network, endpoints, cloud, and applications.		
Status		**(4) Enhancing**: Current tools in place can track changes in system, application and data files, reputation and network trajectory of transferred files. District's security appliances and end-point security resources provide best-in-class protection. Leveraging automation in reporting and remediation to reduce administrative efforts is desirable, and SecureX integrates Cisco's security product data within a single pane of glass.		
Network	**13.3**	**Deploy a Network Intrusion Detection Solution** Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.	IG2 IG3	**Detect**
Tools		1. Cisco Cloud E-Mail Security Appliance (ESA) w/ Advanced Malware Prevention (AMP) 2. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 3. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 4. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 5. Cisco SecureX		
Process		1. Configure firewall, content filter and e-mail security appliance access rules to deny inbound and outbound connections as needed. 2. Implement combination of Cisco file reputation, behavioral indicators, AMP sandboxing technology, and global threat intelligence (Cisco Talos Threat Intelligence Group) integrated in filtering products to provide automated web traffic restrictions. 3. Implement SSL decryption features built into filtering products to examine encrypted traffic for rule-based access analysis. 4. Implement Cisco SecureX on infrastructure to unify visibility, enable automation, and strengthen security across network, endpoints, cloud, and applications.		
Status		**(4) Enhancing**: A multi-layered approach to access control is in place, leveraging advanced threat intelligence data. District's security appliances and end-point security resources provide best-in-class protection. Leveraging automation in reporting and remediation to reduce administrative efforts is desirable, and SecureX integrates Cisco's security product data within a single pane of glass.		
Network	**13.4**	**Perform Traffic Filtering Between Network Segments** Perform traffic filtering between network segments, where appropriate.	IG2 IG3	**Protect**

Tools	1. Cisco Catalyst Switch InterVLAN Routing Configurations 2. Cisco HyperFlex HX Data Platform / VMware vSphere 3. Meraki Dashboard 4. Cisco Secure Endpoint - Wired & Wireless Devices			
Process	1. Create VLANs on network switches and associated interVLAN routing configurations. 2. Create VLANs in virtual network infrastructure associated interVLAN routing configurations. 3. Create separated wireless interfaces with independent IP subnet configurations and link them to associated SSIDs. 4. Disconnect identified systems from network. 5. Use Physical-to-Virtual (P2V) process to create clone of "live" physical systems with no network configuration. 6. Create new VMs as needed, meeting HW and OS requirements with no network connection. 7. Place clients with malware detections or known vulnerabilities into "Triage" mode via Secure Endpoint Management Console, removing network access during remediation activities.			
Status	**(3) Maintaining**: Network segmentation exists as recommended, preventing non-routable layer 2 traffic from moving laterally across subnets. Workstations and other user devices reside on VLANs that do not contain servers or other critical resources, however no ACLs or firewall filtering resources are currently in use. Last four manual options available as needed.			
Devices	**13.5**	**Manage Access Control for Remote Assets** Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.	IG2 IG3	**Protect**
Tools		1. Telnet, SSH, VNC, RDP 2. VMware vCenter 3. Micro Focus ZEN Configuration & Management System (ZCM) 4. Cisco AnyConnect VPN Client / Cisco Firepower Threat Defense 2140 (FTD)		
Process		1. Choose remote access applications for device administration that utilize encryption protocols. 2. Require secondary encryption channel (VPN) for performing off-site device administration tasks.		

Status		**(4) Enhancing:** Remote access applications for use in device administration utilize encryption protocols, and they are used when management tasks are performed while directly connected to the district network on premises. Secure VPN connection is used when management tasks are performed while connected to the district network from a remote location.		
Network	**13.6**	**Collect Network Traffic Flow Logs** Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.	IG2 IG3	**Detect**
Tools		1. All network equipment and installed OS and installed applications. 2. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid)		
Process		1. Implement standardized logging on each device, OS and installed applications. 2. Learn procedures for accessing and reviewing log data. 3. Review log data periodically on a regular schedule.		
Status		**(3) Maintaining:** Most installed equipment has log collecting capability and network administrators must practice auditing the logs regularly. Current endpoint security tools in place can track changes in system, application and data files, reputation and network trajectory of transferred files.		
Devices	**13.7**	**Deploy a Host-Based Intrusion Prevention Solution** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.	IG3	**Protect**
Tools		1. Cisco Cloud E-Mail Security Appliance (ESA) w/ Advanced Malware Prevention (AMP) 2. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 3. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 4. Meraki Dashboard 5. Cisco Identity Services Engine (ISE) 6. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 7. Cisco Secure Endpoint Connector 8. Cisco Umbrella Windows Roaming Client and iOS Security Connecter		
Process		1. Continue implementation of listed security products on devices to include PCs, Windows servers and iOS devices. 2. Implement Meraki-Umbrella Integration 3. Select and implement anti-malware solution for Linux servers. 4. Monitor FMC, ESA, Umbrella, and Secure Endpoint detection and remediation activity via available system reporting tools. 5. Explore options for consolidation of all resource logs and reports.		

Status		**(4) Enhancing**: District's security appliances and end-point security resources provide best-in-class protection. Leveraging automation in reporting and remediation to reduce administrative efforts is desirable.		
Network	**13.8**	**Deploy a Network Intrusion Prevention Solution** Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.	**IG3**	**Protect**
Tools		1. Cisco Cloud E-Mail Security Appliance (ESA) w/ Advanced Malware Prevention (AMP) 2. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 3. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid) 4. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 5. Meraki Dashboard 6. Cisco SecureX		
Process		1. Review/analyze threat data supplied weekly by Multi-State Information Sharing and Analysis Center (MS-ISAC) for lists of reported malware propagating IP addresses and domains for manual blacklist maintenance. 2. Configure firewall and content filter access rules to deny connections as needed. 3. Implement combination of Cisco web reputation and global threat intelligence (Cisco Talos Threat Intelligence Group) integrated in filtering products to provide automated web traffic restrictions. 4. Implement SSL decryption features built into filtering products to examine encrypted traffic for rule-based access analysis. 5. Implement Meraki-Umbrella Integration 6. Implement Cisco SecureX on infrastructure to unify visibility, enable automation, and strengthen security across network, endpoints, cloud, and applications.		
Status		**(4) Enhancing**: A multi-layered approach to access control is in place, leveraging advanced threat intelligence data. District's security appliances and end-point security resources provide best-in-class protection. Leveraging automation in reporting and remediation to reduce administrative efforts is desirable, and SecureX integrates Cisco's security product data within a single pane of glass.		
Devices	**13.9**	**Deploy Port-Level Access Control** Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.	**IG3**	**Protect**
Tools		1. Cisco Identity Services Engine (ISE) 2. Cisco Catalyst (Switch) Integrated Security Features 3. Meraki Dashboard 4. Micro Focus eDirectory (LDAP)		

Process	1. Leverage 802.1x protocol in network switches to support port-based authentication as needed. 2. Deploy appropriate endpoint network access control agent to authorized devices 3. Deploy 802.1x authentication for APs towards switchports 4. Manage device and user identities with ISE (with LDAP connection)
Status	**(3) Maintaining:** 802.1x is running, but sys-auth-control is currently disabled on all Catalyst switches. ISE is currently used as a Radius server, linked to eDirectory as a user source via LDAP, for wireless authentication of users with personally-owned devices, and for VPN authentication from outside the network. Specified UDP and DTLS ports are configured in RADIUS protocol settings for these purposes, however port level access control is not used with internal wired devices. The Meraki wireless network offers the means for deploying certificate-based (EAP-TLS) authentication to district-owned iOS, Android, OS X, and Windows clients, and although this is ideal for us to seamlessly and securely authenticate users, while avoiding the additional requirements of an external RADIUS server, using WPA2 alone so far meets our needs.

Network	**13.10**	**Perform Application Layer Filtering** Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.	**IG3**	**Protect**
Tools		1. Cisco Cloud E-Mail Security Appliance (ESA) w/ Advanced Malware Prevention (AMP) 2. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 3. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 4. Cisco Firepower Threat Defense 2140 (FTD) 5. Cisco Secure Endpoint Console / Secure Malware Analytics (formerly Threat Grid)		
Process		1. Configure firewall, content filter and e-mail security appliance access rules to deny inbound and outbound connections as needed. 2. Implement combination of Cisco file reputation, behavioral indicators, AMP sandboxing technology, and global threat intelligence (Cisco Talos Threat Intelligence Group) integrated in filtering products to provide automated web traffic restrictions. 3. Implement SSL decryption features built into filtering products to examine encrypted traffic for rule-based access analysis. 4. Review/analyze threat data supplied weekly by Multi-State Information Sharing and Analysis Center (MS-ISAC) for lists of reported malware propagating IP addresses and domains for manual blacklist maintenance. 5. Leverage network traffic/application visibility in FMC and WSA to create security policies that restrict unwanted traffic from internal web applications. 6. Configure FMC and Umbrella to decrypt traffic prior to analysis. 7. Investigate all non-web-based applications to determine whether a firewall feature is available and enable those which are.		

Status		**(4) Enhancing**: A multi-layered approach to access control is in place, leveraging advanced threat intelligence data. We have network edge firewall resources that employ application filtering rules effectively. Additional OS-based firewall products are employed as well on servers and clients, however application specific firewall products, if any, are currently not enabled.		
Network	**13.11**	**Tune Security Event Alerting Thresholds** Tune security event alerting thresholds monthly, or more frequently.	**IG3**	**Detect**
Tools		1. Cisco Cloud E-Mail Security Appliance (ESA) w/ Advanced Malware Prevention (AMP) 2. Cisco FirePower Management Center (FMC) w/ Advanced Malware Prevention (AMP) 3. Cisco Umbrella (OpenDNS) w/ Advanced Malware Prevention (AMP) 4. Cisco Firepower Threat Defense 2140 (FTD) 5. Cisco Secure Endpoint Console / Secure Malware Analytics 6. Meraki Dashboard 7. Google Workspace for Education Pro 8. Microsoft Office 365 9. Nutanix Prism 10. Unitrends UniView Portal 11. Cisco Intersight		
Process		1. Implement standardized logging on each device, OS and installed applications. 2. Enable real-time incident alerts in all security products via email/SMS to network administrator 3. Enable weekly activity reports for all security products via email to network administrator		
Status		**4) Enhancing**: Most security products and/or data management (protection) products have customizable real-time alerting or scheduled reporting features that we utilize on a regular basis. These alerts and reports go directly to the Director of Technology and technicians for response, remediation or recovery in a timely fashion.		

CSC 14: Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

CSC 14: Security Awareness and Skills Training				
CSC 14 Rating: 2.89				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
N/A	**14.1**	**Establish and Maintain a Security Awareness Program** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	IG1 IG2 IG3	**Protect**
Tools		1. Global Compliance Network – Digital Security & Protection Session 2. D2 Cybersecurity SAFE Cybersecurity Awareness Training Program		
Process		1. Mandatory self-paced training for all staff each year 2. Mandatory remediation cyber security training for staff inadequate performance during phishing simulation campaigns 3. Follow-up with in-house delivered training on relevant topics 4. Provide "Stay Safe Online" handbooks to all new staff 5. Provide access to all cybersecurity policies & procedures posted on district website 6. Provide updates from these and other security intelligence sources: a. Multi-State Information Sharing and Analysis Center (MS-ISAC) – Advisories b. Center for Internet Security, Inc. (CIS) – Controls, Benchmarks & Tools c. Homeland Security Information Network (HSIN) d. NJ Cybersecurity & Communications Integration Cell – Bulletins		
Status		**(4) Enhancing**: A blending of mandatory and informal opportunities for knowledge transfer is provided to all staff each year. Remediation is required for instances of poor performance by staff during simulations.		
N/A	**14.2**	**Train Workforce Members to Recognize Social Engineering Attacks** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	IG1 IG2 IG3	**Protect**

Tools	1. Global Compliance Network – Mandatory Annual Digital Security & Protection Session 2. D2 Cybersecurity SAFE Cybersecurity Awareness Training Program 3. In-house delivered training on relevant topics			
Process	1. Content included in mandatory self-paced training for all staff each year 2. Mandatory remediation cyber security training for staff inadequate performance during phishing simulation campaigns 3. Examples of real-world incidents reported by security intelligence sources are shared with all staff when relevant.			
Status	**(4) Enhancing:** A blending of mandatory and informal opportunities for knowledge transfer is provided to all staff each year.			
N/A	**14.3**	**Train Workforce Members on Authentication Best Practices** Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	IG1 IG2 IG3	**Protect**
Tools	1. Global Compliance Network – Mandatory Annual Digital Security & Protection Session 2. D2 Cybersecurity SAFE Cybersecurity Awareness Training Program 3. In-house delivered training on relevant topics			
Process	1. Content included in mandatory self-paced training for all staff each year 2. Training during implementation of enforced MFA on designated resources 3. Examples of real-world incidents reported by security intelligence sources are shared with all staff when relevant.			
Status	**(4) Enhancing**: A blending of mandatory and informal opportunities for knowledge transfer is provided to all staff each year. Remediation is required for instances of poor performance by staff during simulations.			
N/A	**14.4**	**Train Workforce on Data Handling Best Practices** Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.	IG1 IG2 IG3	**Protect**
Tools	1. Global Compliance Network – Mandatory Annual Digital Security & Protection Session 2. D2 Cybersecurity SAFE Cybersecurity Awareness Training Program 3. In-house delivered training on relevant topics 4. Review of VTSD Data Security and Privacy Handbook (document) & VTSD Security and Privacy Guide (document)			

Process	1. Content included in mandatory self-paced training for all staff each year 2. Examples of real-world incidents reported by security intelligence sources are shared with all staff when relevant.			
Status	**(3) Maintaining:** A blending of mandatory and informal opportunities for knowledge transfer is provided to all staff each year.			
N/A	**14.5**	**Train Workforce Members on Causes of Unintentional Data Exposure** Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	IG1 IG2 IG3	**Protect**
Tools	1. Global Compliance Network – Mandatory Annual Digital Security & Protection Session 2. D2 Cybersecurity SAFE Cybersecurity Awareness Training Program 3. In-house delivered training on relevant topics 4. Review of VTSD Data Security and Privacy Handbook (document) & VTSD Security and Privacy Guide (document)			
Process	1. Content included in mandatory self-paced training for all staff each year 2. Examples of real-world incidents reported by security intelligence sources are shared with all staff when relevant.			
Status	**(3) Maintaining:** A blending of mandatory and informal opportunities for knowledge transfer is provided to all staff each year.			
N/A	**14.6**	**Train Workforce Members on Recognizing and Reporting Security Incidents** Train workforce members to be able to recognize a potential incident and be able to report such an incident.	IG1 IG2 IG3	**Protect**
Tools	1. Global Compliance Network – Mandatory Annual Digital Security & Protection Session 2. D2 Cybersecurity SAFE Cybersecurity Awareness Training Program 3. In-house delivered training on relevant topics 4. Review of VTSD Data Security and Privacy Handbook (document) & VTSD Cybersecurity Incident Response Plan (document)			
Process	1. Content included in mandatory self-paced training for all staff each year 2. Examples of real-world incidents reported by security intelligence sources are shared with all staff when relevant.			
Status	**(3) Maintaining:** A blending of mandatory and informal opportunities for knowledge transfer is provided to all staff each year.			

N/A	**14.7**	**Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates** Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	IG1 IG2 IG3	**Protect**
Tools		1. Windows Notification Area Alerts 2. Windows Taskbar Application Alerts 3. iOS Software Update Notifications 4. Cisco Secure Endpoint Notifications 5. Web Browser Update Notificatioins		
Process		1. Train staff about notifications that appear periodically 2. Train staff how to initiate the update process in cases where they are able 3. Train staff how to report persistent update notifications they cannot resolve 4. Train staff how to report failed update attempts when they occur		
Status		**(3) Maintaining:** We have not included these skills in formal training opportunities, but we periodically make staff aware of what to look for and how to respond to notifications. Year-end PC maintenance is conducted by staff based to instructions and resources provided by the IT department.		
N/A	**14.8**	**Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks** Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	IG1 IG2 IG3	**Protect**
Tools		1. Global Compliance Network – Mandatory Annual Digital Security & Protection Session 2. D2 Cybersecurity SAFE Cybersecurity Awareness Training Program 3. In-house delivered training on relevant topics		
Process		1. Content included in mandatory self-paced training for all staff each year 2. Examples of real-world incidents reported by security intelligence sources are shared with all staff when relevant.		
Status		**(3) Maintaining:** A blending of mandatory and informal opportunities for knowledge transfer is provided to all staff each year.		

N/A	**14.9**	**<u>Conduct Role-Specific Security Awareness and Skills Training</u>** Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.	**IG2** **IG3**	**Protect**
Tools		1. Global Compliance Network – Mandatory Annual Digital Security & Protection Session 2. D2 Cybersecurity SAFE Cybersecurity Awareness Training Program 3. In-house delivered training on relevant topics		
Process		1. Content included in mandatory self-paced training for all staff each year 2. Mandatory remediation cyber security training for staff inadequate performance during phishing simulation campaigns that target specific groups. 3. Examples of real-world incidents reported by security intelligence sources are shared with all staff when relevant.		
Status		**<u>(4) Enhancing</u>**: A blending of mandatory and informal opportunities for knowledge transfer is provided to all staff each year. Remediation is required for instances of poor performance by staff during simulations.		

CSC 15: Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

CSC 15: Service Provider Management				
CSC 15 Rating: 2.86				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
N/A	**15.1**	**Establish and Maintain an Inventory of Service Providers** Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	IG1 IG2 IG3	**Identify**
Tools		1. VTSD Cybersecurity Incident Response Plan (document) Directory: a. Data Management System Vendor/Partner Support Resources b. System/Network Product Vendor Support Resources 2. Other approved vendor list managed in the Board of Education office by the School Business Administrator		
Process		1. Combine both lists to create a comprehensive master list 2. Designate an enterprise contact for each service provider 3. Review/approve/update the inventory regularly or as needed		
Status		**(3) Maintaining:** Although the service provider inventory does exist in components, and an approved vendor list exists following a vetting process, the creation of a single master list broken into categories is desirable.		
N/A	**15.2**	**Establish and Maintain a Service Provider Management Policy** Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.	IG2 IG3	**Identify**
Tools		1. VTSD Third Party Vendor Contracting Guide (document)		

Process		1. Identify all third-party vendors on comprehensive list 2. Ensure district administration adheres to the guidelines defined in the Third Party Vendor Contracting Guide, which ensures the security of student and district data when dealing with external companies or agencies.		
Status		**(3) Maintaining:** Although the service provider inventory does exist in components, and an approved vendor list exists following a vetting process, the creation of a single master list broken into categories is desirable. Although a management policy exists, it is unclear who enforces it.		
N/A	**15.3**	**Classify Service Providers** Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.	IG2 IG3	**Identify**
Tools		1. VTSD Cybersecurity Incident Response Plan (document) Directory: a. Data Management System Vendor/Partner Support Resources b. System/Network Product Vendor Support Resources 2. NJ Student Privacy Alliance membership offers access to organization vetted vendor data privacy agreements 3. Other approved vendor list managed in the Board of Education office by the School Business Administrator		
Process		1. Identify all third-party vendors on comprehensive master list 2. Explore the guidelines defined in the Third Party Vendor Contracting Guide, which ensures the security of student and district data when dealing with external companies or agencies. 3. Classify service provider on the master list		
Status		**(4) Enhancing**: NJSPA initiative operates as part of the Student Data Privacy Consortium (SDPC), led by Access 4 Learning (A4L), and The Education Cooperative's (TEC) Student Data Privacy Alliance (SDPA). NJSPA partnership allows the district to leverage vetted data privacy agreements already in place across over a dozen other states and other districts throughout New Jersey. This shared model significantly reduces administrative burden and helps ensure compliance with both state and federal privacy regulations.		
N/A	**15.4**	**Ensure Service Provider Contracts Include Security Requirements** Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.	IG2 IG3	**Protect**

Tools		1. VTSD Cybersecurity Incident Response Plan (document) Directory: a. Data Management System Vendor/Partner Support Resources b. System/Network Product Vendor Support Resources 1. Other approved vendor list managed in the Board of Education office by the School Business Administrator		
Process		1. Identify all third-party vendors on comprehensive master list 2. Explore the guidelines defined in the Third Party Vendor Contracting Guide, which ensures the security of student and district data when dealing with external companies or agencies. 3. Review the Privacy Statements on vendor websites (links available in directory on IRP) 4. Review security-related components on any signed contracts with vendors		
Status		**(3) Maintaining:** Although the service provider inventory does exist in components, and an approved vendor list exists following a vetting process, the creation of a single master list broken into categories is desirable. Although a management policy exists that includes guidelines about securing student and district data, a review of published company privacy statements and contract language must always be performed.		
N/A	**15.5**	**Assess Service Providers** Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.	**IG3**	**Identify**
Tools		1. VTSD Cybersecurity Incident Response Plan (document) Directory: a. Data Management System Vendor/Partner Support Resources b. System/Network Product Vendor Support Resources 2. Other approved vendor list managed in the Board of Education office by the School Business Administrator		
Process		1. Identify all third-party vendors on comprehensive master list 2. Explore the guidelines defined in the Third Party Vendor Contracting Guide, which ensures the security of student and district data when dealing with external companies or agencies. 3. Review the Privacy Statements on vendor websites (links available in directory on IRP) 4. Review security-related components on any contracts with vendors before signing/renewing 5. Reassess service providers annually		

Status		**(3) Maintaining:** Although the service provider inventory does exist in components, and an approved vendor list exists following a vetting process, the creation of a single master list broken into categories is desirable. Although a management policy exists that includes guidelines about securing student and district data, a review of published company privacy statements and contract language must be performed prior to entering into a new contract or renewing an existing one.		
Data	**15.6**	**Monitor Service Providers** Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.	**IG3**	**Detect**
Tools		1. VTSD Cybersecurity Incident Response Plan (document) Directory: a. Data Management System Vendor/Partner Support Resources b. System/Network Product Vendor Support Resources 2. Other approved vendor list managed in the Board of Education office by the School Business Administrator		
Process		1. Identify all third-party vendors on comprehensive master list 2. Explore the guidelines defined in the Third Party Vendor Contracting Guide, which ensures the security of student and district data when dealing with external companies or agencies. 3. Review the Privacy Statements on vendor websites (links available in directory on IRP) 4. Review security-related components on any contracts with vendors before signing/renewing 5. Monitor/reassess service providers periodically during the year for established security and compliance criteria		
Status		**(3) Maintaining:** Although the service provider inventory does exist in components, and an approved vendor list exists following a vetting process, the creation of a single master list broken into categories is desirable. Although a management policy exists that includes guidelines about securing student and district data, a review of published company privacy statements and contract language must be performed prior to entering into a new contract or renewing an existing one. Periodic reassessment and monitoring is important to ensure vendor adherence to security and compliance commitments.		
Data	**15.7**	**Securely Decommission Service Providers** Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.	**IG3**	**Protect**
Tools		1. VTSD Cybersecurity Incident Response Plan (document) Directory: a. Data Management System Vendor/Partner Support Resources b. System/Network Product Vendor Support Resources 2. Other approved vendor list managed in the Board of Education office by the School Business Administrator		

Process	1. Monitor/reassess service providers periodically during the year or annually for established performance, security and compliance criteria 2. For any non-renewals of existing contracts, decommission all vendor accounts and dispose of enterprise data.
Status	**(3) Maintaining:** Although the service provider inventory does exist in components, and an annually approved vendor list exists following a vetting process, the creation of a single master list broken into categories is desirable. Contract non-renewals for any reason must trigger decommissioning of vendor accounts and disposal of data.

CSC 16: Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

CSC 16: Application Software Security				
CSC 16 Rating: N/A				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
Applications	**16.1**	**Establish and Maintain a Secure Application Development Process** Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	IG2 IG3	**Protect**
Tools		N/A – No In-House Developed Software Used		
Process		N/A – No In-House Developed Software Used		
Status		**N/A:** We have no in-house developed software, so our status for this control item is stable.		

Applications	**16.2**	**Establish and Maintain a Process to Accept and Address Software Vulnerabilities** Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.	**IG2** **IG3**	**Protect**
Tools		1. VTSD Data Security and Privacy Handbook (document) 2. Voorhees Technology for Digital Learning Plan 2023-26 (document) 3. Cisco Secure Endpoint connector/console		
Process		1. Identify software standards and procedures in Handbook 2. Identify related tasks/roles assigned to IT staff in Technology Plan 3. Implement Secure Endpoint Connector to perform vulnerability scanning on local systems, perform cloud lookup to check file disposition for files executed, moved or copied, and identify all vulnerable computers and their vulnerable applications. 4. Schedule period scans of all systems to gather vulnerability data Leverage OS and server-based firewall products on critical hosts. 5. Configure alerts/automated actions when anomalies are discovered. 6. Place clients with malware detections or known vulnerabilities into “Triage” mode via Secure Endpoint Management Console, removing network access during remediation activities.		

	Status	**(4) Enhancing:** An informal, yet comprehensive software audit is performed in an ongoing fashion. The district maintains support contracts and licensing with entitlement to current versions of software with alerts and notifications concerning forfeiture of support services in the event software versions are not kept current at the minimum level based on terms and conditions for entitlement. Current tools in place can track changes in system and application files and show the number of vulnerable applications that have been executed, moved, or copied, together with the number of vulnerable computers. Whenever an executable file is moved, copied, or executed, the Secure Endpoint Connector performs a cloud lookup to check the file disposition (clean, malicious, or unknown). If the executable file is an application with known vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database, that information is displayed. District's end-point security resources provide best-in-class protection. All Cisco products are licensed with Advanced Malware Protection (AMP), which is integrated with the Cisco Talos Security Intelligence and Research Group for detection, analysis and protection against known and emerging treats. Agent status for Secure Endpoint and Security Connector may be monitored via cloud-based AMP console, and leveraging automation in reporting and remediation to reduce administrative efforts is desirable.		
Applications	**16.3**	**Perform Root Cause Analysis on Security Vulnerabilities** Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise..	IG2 IG3	**Protect**
	Tools	N/A – No In-House Developed Software Used		
	Process	N/A – No In-House Developed Software Used		
	Status	**N/A:** We have no in-house developed software, so our status for this control item is stable.		
Applications	**16.4**	**Establish and Manage an Inventory of Third-Party Software Components** Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.	IG2 IG3	**Protect**

Tools	N/A – No In-House Developed Software Used			
Process	N/A – No In-House Developed Software Used			
Status	**N/A:** We have no in-house developed software, so our status for this control item is stable.			
Applications	**16.5**	**Use Up-to-Date and Trusted Third-Party Software Components** Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.	IG2 IG3	**Protect**
Tools	N/A – No In-House Developed Software Used			
Process	N/A – No In-House Developed Software Used			
Status	**N/A:** We have no in-house developed software, so our status for this control item is stable.			
Applications	**16.6**	**Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities** Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.	IG2 IG3	**Protect**
Tools	N/A – No In-House Developed Software Used			
Process	N/A – No In-House Developed Software Used			
Status	**N/A:** We have no in-house developed software, so our status for this control item is stable.			

Applications	**16.7**	**<u>Use Standard Hardening Configuration Templates for Application Infrastructure</u>** Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.	**IG2** **IG3**	**Protect**
Tools		N/A – No In-House Developed Software Used		
Process		N/A – No In-House Developed Software Used		
Status		**<u>N/A:</u>** We have no in-house developed software, so our status for this control item is stable.		
Applications	**16.8**	**<u>Separate Production and Non-Production Systems</u>** Maintain separate environments for production and non-production systems.	**IG2** **IG3**	**Protect**
Tools		N/A – No In-House Developed Software Used		
Process		N/A – No In-House Developed Software Used		
Status		**<u>N/A:</u>** We have no in-house developed software, so our status for this control item is stable.		
Applications	**16.9**	**<u>Train Developers in Application Security Concepts and Secure Coding</u>** Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.	**IG2** **IG3**	**Protect**
Tools		N/A – No In-House Developed Software Used		
Process		N/A – No In-House Developed Software Used		

Status		**N/A:** We have no in-house developed software, so our status for this control item is stable.		
Applications	**16.10**	**Apply Secure Design Principles in Application Architectures** Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.	IG2 IG3	**Protect**
Tools		N/A – No In-House Developed Software Used		
Process		N/A – No In-House Developed Software Used		
Status		**N/A:** We have no in-house developed software, so our status for this control item is stable.		
Applications	**16.11**	**Leverage Vetted Modules or Services for Application Security Components** Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.	IG2 IG3	**Protect**
Tools		N/A – No In-House Developed Software Used		
Process		N/A – No In-House Developed Software Used		
Status		**N/A:** We have no in-house developed software, so our status for this control item is stable.		

Applications	**16.12**	**Implement Code-Level Security Checks** Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.	**IG3**	**Protect**
Tools		N/A – No In-House Developed Software Used		
Process		N/A – No In-House Developed Software Used		
Status		**N/A:** We have no in-house developed software, so our status for this control item is stable.		
Applications	**16.13**	**Conduct Application Penetration Testing** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.	**IG3**	**Protect**
Tools		N/A – No In-House Developed Software Used		
Process		N/A – No In-House Developed Software Used		
Status		**N/A:** We have no in-house developed software, so our status for this control item is stable.		
Applications	**16.14**	**Conduct Threat Modeling** Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.	**IG3**	**Protect**
Tools		N/A – No In-House Developed Software Used		
Process		N/A – No In-House Developed Software Used		
Status		**N/A:** We have no in-house developed software, so our status for this control item is stable.		

CSC 17: Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

CSC 17: Incident Response Management				
CSC 17 Rating: 3.78				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
N/A	**17.1**	**Designate Personnel to Manage Incident Handling** Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	IG1 IG2 IG3	Respond
Tools		1. Voorhees Technology for Digital Learning Plan 2023-26 (document) 2. VTSD Cybersecurity Incident Response Plan (document) 3. VTSD Technology Disaster Recovery Plan (document) 4. VTSD Data Security and Privacy Handbook (document) 5. Voorhees Township School District Data Governance Plan (document) 6. VTSD Third Party Vendor Contracting Guide (document) 7. VTSD Security and Privacy Guide (document)		
Process		1. Establish decision-making hierarchy with defined thresholds 2. Publish roles in all relevant plans to establish continuity 3. Establish communications plan 4. Revise all plans as needed		
Status		**(4) Enhancing**: Technology staff as CIRT team members have been identified with titles based on established role in the Incident Response Plan. There is CIRT organizational chart and member list, cyber incident escalation and workflow diagram, as well as sensitive data exposure response available in the plan for review.		

N/A	**17.2**	**<u>Establish and Maintain Contact Information for Reporting Security Incidents</u>** Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	**IG1** **IG2** **IG3**	**Respond**
Tools		1. VTSD Cybersecurity Incident Response Plan (document) 2. VTSD Technology Disaster Recovery Plan (document)		
Process		1. Create and publish directory of both internal and third-party contact information, including which situations should invoke contact and who (role) should initiate it.		
Status		**<u>(4) Enhancing</u>**: Technology staff as CIRT team members have been identified with titles based on established role in the Incident Response Plan. There is CIRT organizational chart and member list, cyber incident escalation and workflow diagram, as well as sensitive data exposure response available in the plan for review. Incident reporting may be performed at www.voorhees.k12.nj.us/cybersecurity or via e-mail at IT_Security@voorhees.k12.nj.us		
N/A	**17.3**	**<u>Establish and Maintain an Enterprise Process for Reporting Incidents</u>** Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	**IG1** **IG2** **IG3**	**Respond**
Tools		1. VTSD Cybersecurity Incident Response Plan (document)		
Process		1. Create standard internal incident reporting tools, procedures and regulations (e.g., time) 2. Explore legal and regulatory reporting requirements and build notification conditions and procedures into communications plan.		

Status		**(4) Enhancing**: Technology staff as CIRT team members have been identified with titles based on established role in the Incident Response Plan. There is CIRT organizational chart and member list, cyber incident escalation and workflow diagram, as well as sensitive data exposure response available in the plan for review.		
N/A	**17.4**	**Train Workforce on Social Engineering Attacks, Establish and Maintain an Incident Response Process** Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	IG2 IG3	**Respond**
Tools		1. VTSD Cybersecurity Incident Response Plan (document) 2. VTSD Data Security and Privacy Handbook (document) 3. VTSD Security and Privacy Guide (document)		
Process		1. Examine existing response plans that have associated relevance to cybersecurity. 2. List various types of incidents that require response planning (e.g., data breach, malware attack, etc.) 3. Define various personnel roles needed in responding to incidents. 4. For each incident type, create a phased set of tasks required for proper handling 5. Assign roles to tasks 6. Establish sequence for task completion		
Status		**(4) Enhancing:** A comprehensive Incident Response Plan containing required documented elements procedures has been created and is currently available.		
N/A	**17.5**	**Assign Key Roles and Responsibilities** Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	IG2 IG3	**Respond**
Tools		1. Voorhees Technology for Digital Learning Plan 2023-26 (document) 2. VTSD Cybersecurity Incident Response Plan (document) 3. VTSD Technology Disaster Recovery Plan (document) 4. VTSD Data Security and Privacy Handbook (document) 5. Voorhees Township School District Data Governance Plan (document) 6. VTSD Third Party Vendor Contracting Guide (document) **7.** VTSD Security and Privacy Guide (document)		

Process		1. Establish decision-making hierarchy with defined thresholds 2. Publish roles in all relevant plans to establish continuity 3. Establish communications plan 4. Revise all plans as needed		
Status		**(4) Enhancing**: Technology staff as CIRT team members have been identified with titles based on established role in the Incident Response Plan. There is CIRT organizational chart and member list, cyber incident escalation and workflow diagram, as well as sensitive data exposure response available in the plan for review.		
N/A	**17.6**	**Define Mechanisms for Communicating During Incident Response** Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	**IG2** **IG3**	**Respond**
Tools		1. VTSD Cybersecurity Incident Response Plan (document) 2. VTSD Technology Disaster Recovery Plan (document)		
Process		1. Create and publish directory of both internal and third-party contact information, including which situations should invoke contact and who (role) should initiate it.		
Status		**(4) Enhancing**: Technology staff as CIRT team members have been identified with titles based on established role in the Incident Response Plan. There is CIRT organizational chart and member list, cyber incident escalation and workflow diagram, as well as sensitive data exposure response available in the plan for review. Incident reporting may be performed at www.voorhees.k12.nj.us/cybersecurity or via e-mail at IT_Security@voorhees.k12.nj.us		
N/A	**17.7**	**Conduct Routine Incident Response Exercises** Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.	**IG2** **IG3**	**Recover**
Tools		1. Third-party cyber event simulation providers 2. Articulation meetings		
Process		1. Compile samples of real-world incident scenarios, e.g., phishing campaign 2. Periodically run through scenarios to review roles, tasks, communications and decision-making aspects		

Status		**(2) Developing**: Incident simulations are usually discussed during planning sessions for training, or as a debriefing after someone experiences a "live" incident. Building these activities, or even table top exercises, into regularly scheduled meetings/training sessions has merit.		
N/A	**17.8**	**Conduct Post-Incident Reviews** Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.	IG2 IG3	**Recover**
Tools		1. VTSD Cybersecurity Incident Response Plan (document) 2. Articulation meetings		
Process		1. Follow Incident Closure process in IRP 2. Use Post-Incident Checklists in IRP to do so 3. Initiate follow-up action(s) if necessary		
Status		**(4) Enhancing:** A comprehensive Incident Response Plan containing required documented elements procedures has been created and is currently available.		
N/A	**17.9**	**Establish and Maintain Security Incident Thresholds** Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	IG3	**Recover**
Tools		1. VTSD Cybersecurity Incident Response Plan (document) 2. VTSD Data Security and Privacy Handbook (document) **3.** VTSD Security and Privacy Guide (document)		
Process		1. Review incident and event definitions in published security plans 2. Use Inspection Checklists in IRP when needed		
Status		**(4) Enhancing:** A comprehensive Incident Response Plan and related guides containing required documented elements procedures has been created and is currently available.		

CSC 18: Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

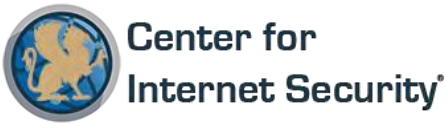
CSC 18: Penetration Testing				
CSC 18 Rating: 1.00				
Asset Type	**CSC**	**Control Description**	**CIS Implement Group**	**NIST Security Function**
N/A	**18.1**	**Establish and Maintain a Penetration Testing Program** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.	IG2 IG3	**Identify**
Tools		1. Third-Party Risk Assessment Service Provider 2. Cybersecurity & Infrastructure Security Agency (CISA) Cyber Hygiene (Vulnerability) Assessment 3. New Jersey Cybersecurity & Communications Cell (NJCCIC) sponsored Security Scorecard		
Process		1. Engage third-party risk assessment service provider to perform periodic Internal and External PEN Test using multiple vectors 2. Continue participation in CISA Assessment, with weekly vulnerability scanning and reporting 3. Continue NJCCIC domain and IP monitoring via Security Scorecard program 4. Pursue remediation based on feedback from listed services/activities		
Status		**(4) Enhancing:** Data gathered from these activities is used to remediate identified vulnerabilities to minimize exposure to known and potential risks.		

Network	**18.2**	**Perform Periodic External Penetration Tests** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.	IG2 IG3	**Identify**
	Tools	1. Third-Party Risk Assessment Service Provider 2. Cybersecurity & Infrastructure Security Agency (CISA) Cyber Hygiene (Vulnerability) Assessment 3. New Jersey Cybersecurity & Communications Cell (NJCCIC) sponsored Security Scorecard		
	Process	1. Engage third-party risk assessment service provider to perform periodic Internal and External PEN Test using multiple vectors 2. Continue participation in CISA Assessment, with weekly vulnerability scanning and reporting 3. Continue NJCCIC domain and IP monitoring via Security Scorecard program Pursue remediation based on feedback from listed services/activities		
	Status	**(4) Enhancing:** Data gathered from these activities is used to remediate identified vulnerabilities to minimize exposure to known and potential risks.		
Network	**18.3**	**Remediate Penetration Test Findings** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.	IG2 IG3	**Protect**
	Tools	1. Third-Party Risk Assessment Service Provider 2. Cybersecurity & Infrastructure Security Agency (CISA) Cyber Hygiene (Vulnerability) Assessment 3. New Jersey Cybersecurity & Communications Cell (NJCCIC) sponsored Security Scorecard		
	Process	1. Engage third-party risk assessment service provider to perform periodic Internal and External PEN Test using multiple vectors 2. Continue participation in CISA Assessment, with weekly vulnerability scanning and reporting		
	Status	**(4) Enhancing:** Data gathered from these activities is used to remediate identified vulnerabilities to minimize exposure to known and potential risks.		

Network	**18.4**	**Validate Security Measures** Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.	**IG3**	**Protect**
Tools		1. Third-Party Risk Assessment Service Provider 2. Cybersecurity & Infrastructure Security Agency (CISA) Cyber Hygiene (Vulnerability) Assessment 3. New Jersey Cybersecurity & Communications Cell (NJCCIC) sponsored Security Scorecard		
Process		1. Engage third-party risk assessment service provider to perform periodic Internal and External PEN Test using multiple vectors 2. Continue participation in CISA Assessment, with weekly vulnerability scanning and reporting		
Status		**(4) Enhancing:** Data gathered from these activities is used to remediate identified vulnerabilities to minimize exposure to known and potential risks.		
N/A	**18.5**	**Perform Periodic Internal Penetration Tests** Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.	**IG3**	**Identify**
Tools		1. Third-Party Risk Assessment Service Provider 2. Cybersecurity & Infrastructure Security Agency (CISA) Cyber Hygiene (Vulnerability) Assessment 3. New Jersey Cybersecurity & Communications Cell (NJCCIC) sponsored Security Scorecard		
Process		1. Engage third-party risk assessment service provider to perform periodic Internal and External PEN Test using multiple vectors 2. Continue participation in CISA Assessment, with weekly vulnerability scanning and reporting		
Status		**(4) Enhancing:** Data gathered from these activities is used to remediate identified vulnerabilities to minimize exposure to known and potential risks.		

Conditions of Use

License for Use



The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cyber security; deliver world-class cyber security solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace.

For additional information, go to <http://www.cisecurity.org/>