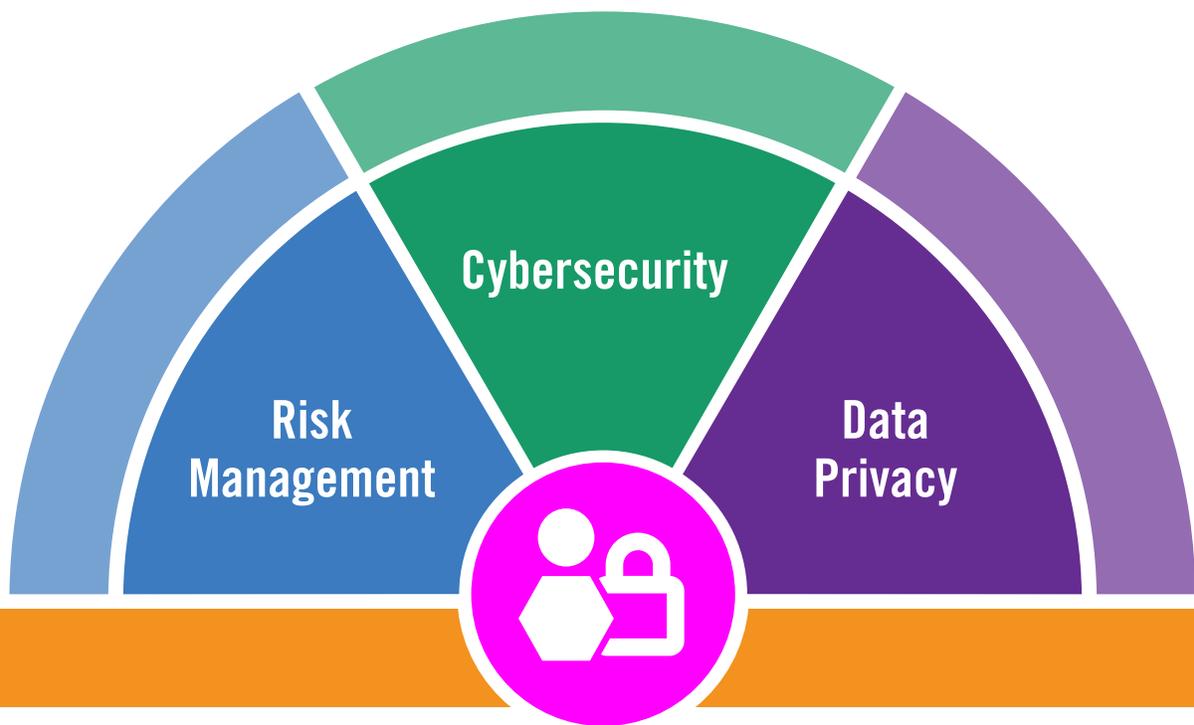


# Education Network Security

## RECOMMENDATIONS CHECKLIST



# Security Recommendations Checklist



This checklist is designed to assist in a quick review of your organization’s network security planning. This document focuses on three key areas:

- Risk management
- Cybersecurity
- Data privacy

## INSTRUCTIONS

Use the checklist as a tool to research and collect information on your organization’s best practices in the areas of risk management, cybersecurity, and data privacy. In the colored cells, rate your level of readiness using the following scale:

- 0 = No evidence** of best practice exists
- 1 = Awareness** – Some verbal awareness exists, but it is not documented or communicated
- 2 = Adaptation** – Some documentation exists for some of the best practice components, but it has not been updated in the last 12 months or is incomplete
- 3 = Best Practice** – Security plan has been updated in the last 12 months and is well documented and communicated





## Risk Management

Identifying, quantifying, and managing the risks that an organization faces.

### Governance

#### Executive Sponsorship/CIO, CTO

There is an executive leadership team that meets regularly to address network and data security health and wellness. There is a role and responsibility matrix that identifies accountability, sustainability, reporting, and communication. Team should include leaders from several different stakeholder groups, such as:

- Technology
- Human Resources
- Legal
- Instructional
- Communications
- Operations

#### Asset Management & Network Risk Assessment

The District/School conducts periodic network risk assessments. Examples of these assessments include:

- Annual penetration tests
- Every other year NIST assessments

Develop a Risk-Based Security Strategy:

- Identify network security assets
- Identify the risks and threats corresponding to these assets
- Define the potential loss or impact to the system from the identified risk or threat
- Evaluate direct and indirect effects/costs of these risks
- Recommend remediation for risks. Include level of effort and cost associated with mitigation

#### Security Policies and Procedures

The District/School has published security policies that correspond to the school's instructional, operational, and technical design

#### Communications

The District/School has developed proactive communications strategies for security-related events

#### Professional Development (PD)

The District/School has ongoing security-related PD and documentation

## Incident Response Plan

The District/School has created and practiced implementing an incident response plan and procedures that include the following areas:

- Description of roles and responsibilities of team members and external service providers – know who to call in the event of an incident or breach, and the roles and responsibilities of those individuals
- Identification of possible risks and development of corresponding risk mitigation strategies
- Preparation for unique incidents that may require unique responses
- Verification that an incident really did occur. Verification of an incident before you communicate is essential as communication that is not accurate contributes to an erosion of trust.
- Restoration of instructional and/or business continuity. Continuity plans are business plans not IT plans. How do you keep the “lights on” when technology is off?
- Communication procedures that identify who needs to be contacted and when. Communication must be clear about what happened and what steps are being taken to mitigate the incident. Focus on issue resolution instead of finger pointing.
- Communications templates that can be used in an emergency. They can be altered to fit the incident, but having them prepared in advance saves time.
- Security audit process to determine how the incident occurred and identify the vulnerability and potential continued risk
- Remediation or mitigation strategy to make sure the risk does not continue
- Evaluation process to review and improve the security evaluation process

## Governance and Policy Development

Policies form a foundation for any cybersecurity program. Policies define how organizations will approach security, how staff and students are to approach security, and how certain situations will be handled. The following are considered baseline best practices for policy development.

 The District/School has a current **Acceptable Use Policy for Staff and Students** defining the intended uses of the network that includes, but is not limited to, the following areas:

- Who should and should not have access to the network
- Clearly defined prohibited activities based on best practices and past experience “use cases”
- Blanket statements that address engaging in unlawful activities
- A monitoring disclosure statement
- Consequences for non-compliance
- Designated policy enforcement officer
- Contact information for reporting malicious or suspicious activity
- Statements concerning FERPA, COPPA, CIPA, PPRA, PCI, HIPAA or reference to Electronic or Digital Communications Policy

**The District/School has a Digital Communications Policy to assist in preventing the spread of viruses and malware as well as defining issues surrounding cyberbullying, defamatory communications, and social networking. The Digital Communications Policy includes, but is not limited to, the following areas:**

- Acceptable Use Policy
- Appropriate use of written, audible, and visual communications
- A statement defining types of security issues (e.g. malware, viruses, spoofing)
- A monitoring disclosure statement
- Consequences for non-compliance
- Designated policy enforcement officer
- Contact information for reporting malicious or suspicious activity
- Clear statements concerning FERPA, COPPA, CIPA, PPRA, PCI, HIPAA

**The District/School has a Remote Access Policy that defines standards for connecting to the organizational network from outside of the physical network and security standards for devices that are allowed to connect. The Remote Access Policy includes, but is not limited to, the following areas:**

- Clear definition of secure remote access methods (e.g. OOB, VPN, SSH) and clear definition of unauthorized, non-secure methods (e.g. RDP, telnet, http)
- Statement of internal resources available through secure remote access
- Statement of internal resources not available through remote access
- Anti-virus and malware prevention software standards needed on devices used for remote access
- Guidelines for requesting, approval, and denial of remote access

## Communications and User Training

Communications and PD should be provided for all individuals who have access to network resources or the Internet (teachers, staff, administration, students, volunteers, and parents). PD should be delivered frequently and in a variety of easily accessible formats such as documentation, webinars, face-to-face instruction, videos, and online classes. The following are considered baseline best practices for network security PD:

**The District/School conducts tabletop drills and/or exploratory exercises of potential breaches with leadership teams to practice implementing the incident response plan**

**The District/School has ongoing PD and documentation regarding cybersecurity threats and network security best practices**

**Distribute and communicate Acceptable Use and Digital Communications Policies to all district stakeholders listed above with acknowledgment of receipt to appropriate administrator or staff**

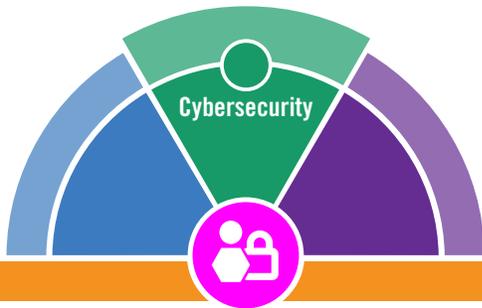
**Make all policies available to all stakeholders online**

**Distribute and communicate the legal definition of state and federal laws and regulations (e.g. FERPA, COPPA, CIPA, PPRA, and HIPAA) to all school personnel**

**Annually conduct an online safety and digital citizenship course for students**

**Make definitions of state and federal laws and regulations available to all stakeholders online**

- Provide real-world examples of threats and attacks that have already occurred in other districts to all internal personnel**
- Provide everyone with basic knowledge of, and common vocabulary for, possible threats such as virus, malware, phishing, and social engineering**
- Provide all stakeholders with tips and recommendations for proper system access etiquette, including:**
  - Protect your password, do not display it on a screen or piece of paper or give out
  - Use an alphanumeric password that is at least 8 characters long
  - Do not use a district account for personal use
  - Do not allow a user to use a computer you have already logged into
  - Log out of a computer when you are finished or walk out of your room
  - Refrain from logging into more than one device at a time
  - Report any suspicious activities or emails
  - Do not open any attachments from others that you do not know
  - Do not open any attachments with the file extension (.exe)
  - Do not respond to emails asking for sensitive information



## Connectivity

Careful attention to infrastructure design and systems configuration will create security standardization and reduce vulnerabilities, threats, and attacks. Having a clear understanding of every network component and its configuration capabilities is very important. A regular assessment of infrastructure should be performed to identify each network-supporting device and its function within the organization's infrastructure. Best practices are outlined below.

- Internet Access. Some best practices include**
  - Use filter lists that match the District/School's Acceptable Use Policy
  - Consider bandwidth shaping to decrease non-critical application usage to preserve bandwidth if availability is restricted
  - Distribute Network Address Translation of public IPv4 addressing across locations or private networks
  - Where possible, scan for malicious payloads (e.g. email, http, ftp)
  - Engage a network service provider that has DDoS mitigation capabilities and strategies
  - Establish resilient egress to ensure continuity of service in the event of a failure

## Network Security

**□ Maintain an asset inventory of key information technologies on your network. Regularly perform device discovery and inventory updates. The components may include:**

- Firewall
- Router and switch infrastructure
- Wireless network devices
- VPN
- Networked end user devices
- Intrusion prevention
- Content security
- Identity management
- An endpoint protection platform (EPP)
- Endpoint detection response (EDR)

**□ Basic firewall best practices include:**

- Latest patches and updates are installed
- Effective filters are in place to prevent malicious traffic from entering the perimeter
- Unused ports are blocked by default
- Unused protocols are blocked by default
- 'Deny All' should be the default posture on all access lists – inbound and outbound
- IPsec is configured for encrypted communication within the perimeter network
- Intrusion detection is enabled at the firewall
- Careful use of 1:1 Network Address Translations (NAT)
- Use of Port Address Translations (PAT) for Internet-facing services
- Distribute NAT addressing between locations and services
- Logging enabled and audited
- Routine audits for unused or legacy rules
- Employ management user authentication and authorization with user accounting
- Routinely back up configurations and audit changes
- Consider disabling Remote Desktop Protocol (RDP)

**□ Intrusion Protection System (IPS) best practices include**

- Ensure all stakeholders understand the business and technical needs for real-time threat protection
- Consider current and future bandwidth requirements
- Determine the correct sensor placement
- Evaluate needs and consider applications that run only periodically
- Establish compliance-reporting requirements and procedures
- Configure for data retention and backup
- Establish a periodic schedule of system evaluation



### **Router best practices include:**

- Latest patches and updates are installed
- Standardize router configurations
- Assign static IP addresses to all management interfaces
- Block known vulnerable ports
- Use only secure routing protocols that use authentication
- Use the most secure remote access method your platform offers (typically the newest version of SSH)
- Disable telnet and other remote access methods not used
- Use strong passwords for both remote and local connections
- Ingress and egress filtering is enabled so incoming and outgoing packets are confirmed to have come from public or internal networks
- Web-facing administration is disabled
- Directed broadcast traffic is not received or forwarded
- Unused services are disabled
- Logging is enabled and audited for unusual traffic or patterns
- Large ping packets are screened
- Restrict remote access to only known management networks
- Employ management user authentication and authorization with user accounting
- Routinely backup configurations and audit changes

### **Switch best practices include:**

- Latest patches and updates are installed
- Standardize switch configurations
- Assign static IP addresses to all management interfaces
- Use strong administrative passwords
- Use VLANs to segregate traffic types and reduce broadcast domains
- Unused administrative interfaces are disabled
- Unused services are disabled
- Available services are secured
- Employ management user authentication and authorization with user accounting
- Routinely backup configurations and audit changes

### **Wireless network device best practices include:**

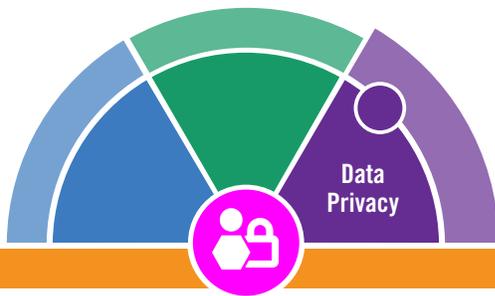
- Use SSIDs that cannot be easily associated with your school
- Do not broadcast SSID not meant for casual use
- Use 802.11x for authentication to your wireless network so only approved devices can connect
- Use the strongest encryption method possible, WPA2 Enterprise preferred
- Never use WEP encryption
- Only permit guest network connectivity to connect to the Internet, not to internal resources
- Apply bandwidth restrictions to guest or open networks

## Access Control and Authentication

Access control and authentication are two of the most important foundations of network security. In short, these are the fundamentals of who can access your systems and resources as well as authenticate that these individuals are who they claim to be. If these two pieces are not addressed appropriately, any other security efforts could be rendered ineffective. The following are best practice recommendations:

### Access control and authentication

- Implement password management solutions (e.g. identity management, single sign-on)
- Multi-factor authentication (MFA) for teachers and administrators
- Passwords should be unique and easily memorable to the individual user
- Create strong password guidelines
  - Password should be a least 8 characters or longer
  - Use complexity as much as possible without reducing memorability: alphanumeric, upper and lower case, symbols
  - Don't reuse passwords
  - Remove the force change line completely (no longer considered best practice)



## Data Privacy

Securely and properly handling the management of critical data concerning consent, notice, sensitivity, and regulatory concerns.

## Policy Development

School districts need to create a clear and comprehensive compliance policy regarding data privacy. This policy needs to be reviewed and updated at least annually. The following are some baseline best practices for developing a data privacy compliance policy:

### Establish an executive leadership team that is responsible for creating, executing, and reviewing the policy. Team should include leaders from several stakeholder groups, such as:

- Technology
- Human Resources
- Legal
- Instructional

### Develop data privacy policies for teachers, staff, and students

### Address state and federal laws and regulations within the policy (e.g., FERPA, SHERPA, COPPA, and HIPAA)

### Create a compliance approval process for the review of EdTech applications utilized in the organization

## Certification and Compliance Training

**It is imperative that school districts require vendors to adhere to the district's data privacy policy. Vendor compliance best practices include:**

- Ensure vendors comply with FERPA, applicable state laws, and local policies
- Hold vendors accountable to data privacy compliance regulations
- Require vendors to sign your district's compliance protocol and commitment policy

**Adopt or attain a program that gives full visibility to district leaders into the applications utilized throughout the district to manage compliance**

**User compliance training best practices include:**

- Create ongoing professional development and documentation for teachers, staff, administration, and students regarding compliance and privacy policies. Some baseline best practices include:
  - Create an oversight team to oversee professional development and compliance training
  - Develop benchmarks to measure results, identify gaps, and assess ongoing training needs
  - Stay abreast of local, state, and federal regulations and regularly research and review data privacy guidelines, resources, and updates from reputable organizations and experts.
- Create a library of reputable data privacy resources, guidelines, and training materials. Recommended resources include:
  - The Educator's Guide to Data Privacy, FERPA SHERPA
  - iKeepSafe educator resources
  - CommonSense Media Privacy Evaluation Program
  - Student Data Privacy Consortium
  - Future of Privacy Forum Best Practices and Code of Conduct
  - 5 Encryption Best Practices For Securing Sensitive Data In Higher Education Organizations





## Communications

Communications should be distributed to all individuals who have access to network resources or the Internet. The following should be considered baseline best practices for communication practices and procedures regarding data privacy.

- Distribute and communicate acceptable use and data privacy compliance policies to all district stakeholders with acknowledgment or receipt to appropriate administrators or staff**
- Make all policies available online**
- Make definitions of state and federal laws and regulations available to all stakeholders online**
- Create an online library of recommended data privacy resources available to all stakeholders**
- Provide real-world examples of threats and ramifications that have occurred in the K-12 community, such as K12 Cybersecurity Resource Center ([k12cybersecure.com/map](http://k12cybersecure.com/map))**
- Develop a communication plan to manage messaging and media relations in the event of an incident or breach**
- Provide visibility and reports to leadership teams, as well as teachers and staff into EdTech application usage, results, and privacy compliance**

## Addressing Vulnerabilities

- Create a data privacy leadership team that includes administration, technology, and instruction team members**
- Conduct self-audits on a semiannual to annual basis to identify all vulnerabilities and gaps in current data privacy practices and policies**
- Develop a plan that includes a comprehensive timeline and action steps to address vulnerabilities**



# Keeping your network and data secure so you can focus on what matters most.

Our robust portfolio of services keeps your network secure, ensuring you are prepared for the unexpected.

Learn more at [www.ena.com](http://www.ena.com)



ENA delivers transformative connectivity, communication, cloud, security, and data analytics solutions supported by exceptional customer care. For more information, please visit [www.ena.com](http://www.ena.com), call 866-615-1101, or e-mail [info@ena.com](mailto:info@ena.com).