CyberNut

PENNSYLVANIA'S CYBER READINESS STARTS HERE

Cybersecurity Readiness Guide for Your State

A quick, state-by-state look at how K–12 schools are protecting student data, meeting cybersecurity laws, and preparing for digital threats.

State-Specific Laws

Key data privacy and cybersecurity laws for K–12 schools.

Staff Readiness

FERPA alignment and annual phishing training.

Incident Preparedness

Breach notification and response steps.

Nationwide Context

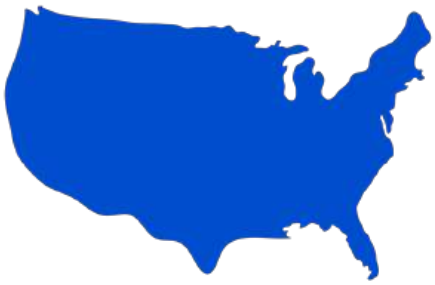
How your state compares in K–12 cyber readiness.

K-12 Threat Landscape

National

K–12 schools are increasingly targeted by cyberattacks that disrupt learning, compromise student data, and cost districts hundreds of thousands of dollars in recovery.

Preparing now helps minimize risk, protect families, and avoid costly downtime.



- **92%** of K–12 data breaches begin with phishing
- **$50K–$1M** average recovery cost
- Cyber incidents are now the leading cause of **school closures** unrelated to weather

Pennsylvania

In Pennsylvania, districts must comply with SCR Act of 2023, 73 P.S. § 2301, and § 13-1303a, which govern how schools handle student data and respond to cyber incidents.

Understanding Your State's Cybersecurity Laws:

SCR Act of 2023	All About Act 3 of 2023: New Cybersecurity Requirements for Pennsylvania Schools
73 P.S. § 2301	What to Know About Pennsylvania's Data Breach Notification Law
§ 13-1303a	All About FERPA Alignment in the PA Public School Code

School Cybersecurity Readiness Checklist

Network

- ◯ Ensure firewalls are configured to block unauthorized traffic
- ◯ Enable intrusion detection/prevention systems (IDS/IPS)
- ◯ Conduct regular vulnerability scans on school networks
- ◯ Enforce network segmentation (separate student/staff networks)
- ◯ Implement DNS filtering to block malicious sites

Account & Access

- ◯ Require multi-factor authentication (MFA) for all admin accounts
- ◯ Enforce strong password policies (length, complexity, expiration)
- ◯ Implement role-based access control (RBAC) for staff and students
- ◯ Set automatic account lockouts after failed login attempts
- ◯ Regularly audit user access & remove inactive accounts

Device & Endpoint

- ◯ Ensure all devices have endpoint protection & antivirus software
- ◯ Enable automatic software & OS updates on all school-owned devices
- ◯ Restrict USB and removable media access to prevent data theft
- ◯ Deploy mobile device management (MDM) for remote monitoring
- ◯ Require full-disk encryption for staff and admin laptops

Email & Phishing

- ◯ Configure DMARC, SPF, and DKIM to prevent email spoofing
- ◯ Implement phishing simulation training for staff & students
- ◯ Enable email filtering to block spam & malicious attachments
- ◯ Use safe browsing tools to prevent credential theft
- ◯ Implement a real-time threat reporting system to streamline user-reported attacks, rapidly remove malicious emails, and reinforce ongoing security awareness.

Data Protection & Compliance

- ◯ Encrypt sensitive student & staff data (both in transit & at rest)
- ◯ Ensure backups are performed daily and stored securely
- ◯ Regularly test data recovery procedures
- ◯ Implement data retention & deletion policies
- ◯ Comply with federal regulations like: FERPA, CIPA, and COPPA
- ◯ Comply with states regulations like: SCR Act of 2023, 73 P.S. § 2301, and § 13-1303a

Incident Response & Disaster

- ◯ Develop a cybersecurity incident response plan
- ◯ Conduct quarterly security drills (ransomware, data breach scenarios)
- ◯ Ensure staff knows who to contact in case of a cyber incident
- ◯ Maintain cyber insurance coverage for potential breaches
- ◯ Review & update disaster recovery plans annually

Resources & Next Steps

National Resources

Explore trusted national organizations dedicated to student data privacy and K-12 cybersecurity.

Department of Education
Student Privacy Policy Office (SPPO)
Learn more

Federal Trade Commission
Protecting Student Privacy
Learn more

National Institute of Standards and Technology (NIST)
Cybersecurity Framework
Learn more

Cybersecurity & Infrastructure Security Agency (CISA) K-12 Resources
Learn more

Pennsylvania Resources

Explore state-specific departments, privacy laws, and cybersecurity initiatives supporting K-12 protection.

State Department of Education
Learn more

Student Data Privacy Laws or Acts
Learn more

Cybersecurity Frameworks, Regulations, or Funding Initiatives
Learn more

CYBERNUT RESOURCES

Staying Ahead of the Curve: Cybersecurity in the Age of AI

Learn how AI is transforming cyber threats in schools and what your district can do to stay secure.

Schools are high-value cyber targets. This report explains the latest AI-driven threats and gives district leaders practical strategies to defend against them.

DOWNLOAD

CyberNut's Adaptive Cybersecurity Training Platform Overview

LEARN MORE

Our platform equips K-12 institutions with essential tools to combat cyber threats. Experience a comprehensive approach to security awareness through engaging simulations and real-time analytics.

FREE PHISHING VULNERABILITY ASSESSMENT

The goal is to quickly and discreetly identify your district's cybersecurity vulnerabilities. CyberNut's baseline phishing assessment quickly and quietly measures your district's current cybersecurity risk—without disrupting school operations.

- Quick & Invisible
- Actionable Results
- Zero Setup Required
- Budget-Friendly Evidence

GET YOUR FREE ASSESSMENT NOW