Intel® Education | Frequently Asked Questions

DEVELOPING A SECURITY STRATEGY FOR K-12 EDUCATION

12 questions to answer as you begin creating a comprehensive security strategy

The more education goes digital, the more important it is to safeguard your digital assets and data. But security and privacy issues are not only more critical than ever—they're also more complex. With budgets stretched to the breaking point, how do you implement a comprehensive privacy and security strategy that makes the most of scarce resources?

Why is there so much focus on privacy and security right now?

Digital data and tools are more essential to K-12 education than ever before, so schools have more investments in digital technologies to protect. The amount and variety of data are rising. The school environment is more complex, with more third-parties having access to sensitive data. The regulatory climate continues to evolve to address rising expectations for data privacy. Parents and community members are more sensitive to the potential downsides of digital data collection.

Digital dangers are more diverse and serious than when the worst you had to worry about was a student hacking a set of grades. Today, students, teachers, and others are at risk of identity theft if relevant data falls into the wrong hands. School systems can fall prey to global criminals who lock the system's digital data and demand a ransom to release it. High-profile breaches, whether in school systems or in our lives as consumers, have made everyone more aware of the need for rigorous protection.

What do I need to protect?

Think of three areas:

1. Mobile devices and other physical technology.
2. Confidential student data, including data mandated confidential by state, national, or regional laws or regulations. This can include personal identifying information, health information, data pertaining to family finances, and other student or family information. It also includes students' education-related data, such as grades and assessment results.
3. Employee data, such as payroll information and data that could contribute to identity theft.

As an IT leader, you may also be involved in protecting the physical environment. Your insights may be invaluable as your school system chooses visitor management solutions, event notification systems, and other technologies designed to increase the physical safety of students and staff.

What's the difference between security and privacy?

Security refers to safeguarding digital assets from theft, misuse, and loss, as well as from malicious or inadvertent disclosure. Privacy addresses the need to protect the confidentiality of students, families, and employees while maximizing the educational value of data. Protecting privacy requires policies and procedures that define how the school system and any third parties it works with will collect, access, use, and share any data that can be used to identify the user.

Where are my points of vulnerability?

Data and other assets can be at risk in the classroom, administrative offices, district data center, off-premises cloud, homes, and community locations. Devices, networks, and platforms can be subject to theft, loss, or attack. Risk can occur at any point where it is collected, stored, used, or transmitted. Data is at risk whether it's at rest (i.e., when it's stored) or in flight (moving over the network). Potential points of attack can include mobile devices, network equipment, storage systems, servers, and cloud services. Bring-your-own (BYO) device programs and take-home programs for school-owned devices both require attention to security technologies and practices.

People and processes can expose you to risks—for example, users with weak passwords, service providers with lax security practices, or trusted employees who aren't properly trained in using technology.

Why is it important to have a comprehensive strategy for security and privacy?

Security and privacy requirements are complex, diverse, and interrelated. Security affects all parts of the digital environment and beyond, and it involves a wide range of stakeholders and activities. Security and privacy must be addressed through policies, hardware and software technologies, training, and behavior change. To be successful, you need a flexible, holistic strategy that covers your entire environment, including third-party partners and mobile devices used beyond the school walls.

What is at risk if my strategy fails?

Your school can incur costs to replace lost or damaged resources. The school or district may face lawsuits or financial penalties, especially if security failures result in a violation of legal or regulatory requirements. High-visibility breaches can damage the school system's reputation, and the resulting loss of trust can make innovation more difficult. Attacks on networks, servers, and cloud services can interfere with teaching and learning and result in lost productivity by students, teachers, administrators, and IT professionals.

So, where do I start, and how do I pay for all this?

We recommend basing your strategy on a three-level hierarchy of security and privacy requirements. This tiered approach lets you spread the costs while meeting important priorities.

1. **Baseline.** The crucial first step is to comply with the defined compliance needs for your state, area, region, and country. Work with legal advisors to ensure you are fully compliant with regulations pertaining to data acquisition, use, and disclosure. In the United States, for example, pay close attention to Federal standards such as the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Protection of Pupil Rights Amendment (PRRA), as well as the Health Insurance Portability and Accountability Act (HIPAA) for students' medical data. Baseline capabilities, which also help ensure compliance, include virus and firewall technologies and single-factor identity management to help keep "bad actors" off the district's or school system's network and provide a basic level of protection for information assets.
2. **Enhanced security.** Once compliance requirements are met, map out the next level of security. Work independently or with an industry-recognized organization to conduct regular, thorough risk assessments that identify the points where your assets and data are at greatest risk. Then, develop a roadmap for addressing them, for example, moving from single-factor authentication to dual-factor authentication to robust identity management.
3. **Advanced security.** The third tier of security execution includes more sophisticated capabilities such as end-to-end encryption of all data, predictive threat monitoring to identify attempted intrusions before they can get through, and digital forensic tools to investigate threats.

What technologies are going to be essential?

Security technologies will align with the three key aspects of the threat-defense lifecycle:

1. **Protect.** Protecting the environment involves the use of solutions such as firewalls, virus software, data encryption, and identity management solutions to keep attacks from occurring and avoid damage if a breach occurs.
2. **Detect.** Intrusion detection solutions proactively watch for signs of an attack, enabling a faster response to an impending or ongoing breach.
3. **Correct.** Rapidly responding to a breach is essential to mitigating its damage. Solutions that automate the detection and response functions can reduce risk while reducing the burdens on busy IT staff.

TABLE 1. TECHNOLOGIES FOR BASIC, ENHANCED, AND ADVANCED SECURITY

BASELINE SECURITY CAPABILITIES	ENHANCED SECURITY CAPABILITIES	ADVANCED SECURITY CAPABILITIES
End-point device encryption with hardware acceleration	Client solid-state drives (SSDs) with encryption	Server SSDs with encryption
Mobile device management	End-point DLP	NDLP prevention
Penetration testing and vulnerability scanning	Network DLP (NDLP) monitoring	Database activity monitoring
Data Loss Prevention (DLP) discovery	Anti-theft solutions that remotely locate, lock, and wipe a lost or stolen device	Digital forensics
Device control	Multifactor authentication with time-out	Integrated security information management and security event management (SIEM)
Anti-malware	Secure remote administration, hardware-enabled	Threat intelligence exchange and collaboration
Single-factor access control	Policy-based encryption for files and folders	Multifactor authentication with walk-away lock
User awareness training	Hardware-accelerated encryption of servers, databases, and backup systems	Client and server application white-listing
E-mail and web gateways	Network Intrusion Prevention System (IPS)	
Vulnerability management and patching		

Table 1. Suggests technology solutions for basic, enhanced, and advanced security capabilities.

What should I consider in addition to the technologies?

People are one of the most important elements of a comprehensive security strategy, so explore what changes to training, policies, and processes can strengthen your school system's security and privacy protections. Provide training on basic security practices, and encourage everyone to make security and privacy a priority. Develop thorough incident response plans, and prepare staff to implement them if needed.

Consider physical as well as digital security, including basics such as access-controlled server rooms, locked cabinets for servers, and physical security of the network operation center. Explore solutions for identifying visitors and maintaining the physical security of the school. Develop a plan for disaster prevention and recovery, and arrange for offsite or cloud-based backup for all critical data.

What best practices can help us increase strategy?

- **Engage stakeholders** in discussions to broaden understanding of security risks and develop an integrated approach to managing those risks.
- **Conduct a risk assessment** to identify security gaps. Establish priorities to address gaps, factoring in issues such as how likely it is that a security event will occur and how serious the consequences would be if it did. Then, develop an implementation plan that aligns processes, policies, and technologies.
- **Train everyone** who uses digital resources. Educate students on digital citizenship, and help them understand that they are building their digital identity with every action they take online.
- **Establish a security chief** to lead in creating a security-aware school culture. The security chief also keeps up with the latest Federal and State regulatory requirements, and works with stakeholders to protect digital resources while using them to drive student outcomes.
- **Practice minimalism.** Don't collect and store more data than you need. This helps reduce storage costs as you safeguard data.
- **Develop policies** that spell out what data can be stored on teacher and administrator laptops. Implement strong security measures to protect any sensitive data.
- **Address security and privacy concerns** in all contracts with third parties. Collect and share only the data necessary to provide the desired level of service.
- **Examine the security implications** of all purchases, including mobile devices. For example, will devices have mature management software available? Are any security and privacy protections built in?
- **Choose robust, proven security solutions** that are easy to use. Solutions that simplify IT operations can enhance IT productivity and reduce costs.
- **Make it a living program.** Create a cycle of continuous improvements based on lessons learned. Continue to evolve your security strategy as threats and compliance requirements evolve, and new solutions become available.

What resources are available?

- The Consortium for School Networking (CoSN) offers a Protecting Privacy Toolkit and other resources.
- The U.S. Department of Education Privacy Technical Assistance Center's PTAC Toolkit provides resources to help education stakeholders understand confidentiality and security issues related to student-level longitudinal data systems.
- The U.S. National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, while focused on the United States, offers a broadly applicable framework for managing security risks.

How can Intel help?

Intel is a global technology leader with more than a decade of collaboration with education and government leaders around the world. Intel builds security into many of its products, designs security innovations, and can advise school leaders on security issues.[+]

Digital data and resources are increasingly essential to providing each student with a personalized learning experience that improves student outcomes and helps students achieve their life goals. By choosing devices and systems based on Intel® technologies and implementing a robust privacy and security strategy, your school system can safeguard privacy and protect assets while delivering the full educational benefits of digital technologies.

See how Intel® Education can help.
www.intel.com/content/www/us/en/education/intel-education.html

intel
Education

[+] No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® processors may require additional software, hardware, services, and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details. For more information visit www.intel.com/technology/security.

Printed in USA 0116/MM/HBD/PDF ♻ Please Recycle 333835-001US