How to improve your school cyber health

10 BEST PRACTICES
FOR A MORE SECURE
SCHOOL SYSTEM

AXIS COMMUNICATIONS

Protect what matters

Cybersecurity is a shared responsibility that requires ongoing vigilance and a continuous commitment to the everyday practices that protect what matters most to your organization.

Whether you're protecting students, staff, or property, your IP-based physical security solutions handle critical data that must be safeguarded at every stage. In our evolving cybersecurity threat landscape, it's more critical than ever to protect the networked devices and software services in your IT (informational technology) system.

If your system is compromised, it can result in financial losses, reputational damage, campus operation disruptions and more. That's why it's essential to implement regular cybersecurity best practices to reduce your risk and maintain a cleaner bill of cyber health for your organization.

Check out the following pages to explore 10 best practices for maintaining more secure school systems.

1 Comply with data privacy regulations

Because regulations vary around the world, schools and campuses need to comply with local legislation and best practices.

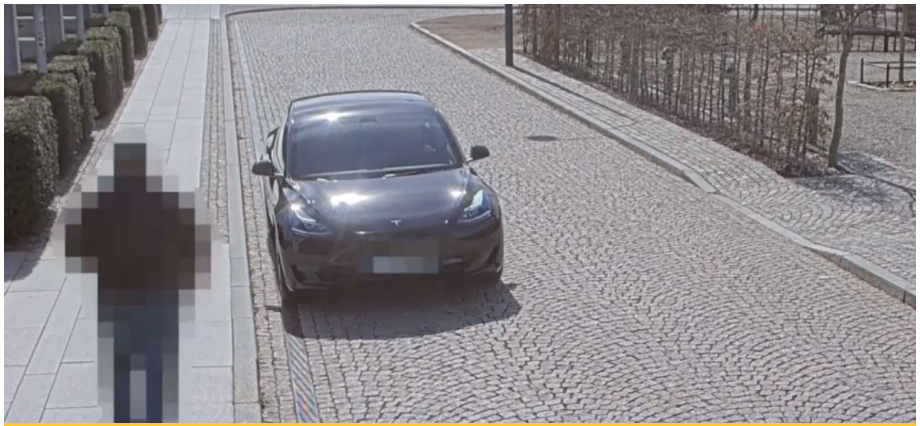
Student privacy data regulations are designed to protect sensitive student information, particularly in educational settings. Some examples of Country-specific regulations:

In USA
FERPA (Family Educational Rights and Privacy Act)
COPPA (Children's Online Privacy Protection Act)
HIPAA (Health Insurance Portability and Accountability Act)

In Canada
PIPEDA (Personal Information Protection and Electronic Documents Act)

In Australia
Schools falls under federal or state/territory jurisdiction. Specific legislation and departmental policies apply differently to different schools.
Privacy Act 1988

In Europe
GDPR (General Data Protection Regulation)



Did you know?
Malware is the primary attack type in the Education sector. Cyber criminals exploit its less robust security to access an abundance of sensitive student data, research, and intellectual property, which they monetize on dark web marketplaces.

Source: IBM. (2025). Cost of a Data Breach Report: The AI Oversight Gap.

2 Perform a risk analysis

A risk analysis will help define how much you can lose and how much you should invest in protection in the event of a cyber incident.

Start with taking an inventory of key assets and prioritize protection based on their value to your organization. Then, identify the most plausible threats and vulnerabilities.

Plausible threats:
> Unintentional human naivety and error
> Deliberate misuse of the system
> Physical tampering and sabotage
> Exploitation of software vulnerabilities

Plausible vulnerabilities:
> Weak credentials
> Out-of-date software
> Unencrypted communication
> Exposed ports or services

In the event your system is compromised, determine what the expected costs and damages may be. You may also want to consider if your organization follows a **Risk Management Framework (RMF)**, which can help provide processes and guidelines for risk management.

3 Understand the ecosystem

Understanding the broader ecosystem involved in creating, distributing and implementing your physical security products enables you to make more informed decisions about the technology you use and the measures you take to protect it.

In the supply chain, cybersecurity begins with the manufacturer. A reliable IT manufacturer will exercise careful control over their own supply chain and offer transparency into supplier governance, ensuring a more secure path from component level to finished product.

When it comes to product design, development, and production, cybersecurity best practices should be implemented at every stage. Products should be equipped with multiple layers of protection, such as built-in security features, and manufacturers should offer guidance on device hardening and software maintenance. And what happens when a weakness is discovered? A clear process for identifying, disclosing and patching vulnerabilities is essential in establishing trust and minimizing exposure to risk.

4 Establish clear policies

IT security policies are rules and procedures designed for employees and relevant stakeholders that utilize your organization's IT assets and resources to protect the confidentiality, integrity and availability of data.

The process for developing IT security policies typically involves:

> Establishing scope and clear objectives based on school/campus needs
> Performing a risk assessment
> Establishing security controls to mitigate risks noted in the assessment
> Defining timelines for patching systems and software-based vulnerabilities
> Receiving support and approval from relevant stakeholders
> Training employees on new procedures and expectations
> Publishing the policy
> Regularly reviewing and updating the policy

Like any other IP-based device, it's important to ensure that all physical security products adhere to existing policies and continue to meet standards for IT security as our technological landscape evolves.

5 Use strong passwords

Obvious as it may seem, weak passwords are one of the most common vulnerabilities exploited by cyber criminals to gain unauthorized access.

Most IP-based devices are shipped with default passwords and settings. Sometimes, these passwords are easy to guess and even published online.

Here's some tips for stronger passwords:
> Update default passwords to distinct passwords that are unique to each device
> Use a minimum of 12 characters and avoid common phrases or names
> Use certificates to encrypt passwords and usernames
> Update passwords regularly
> Change default user accounts in accordance with IT or company policies

6 Secure your network

Connected devices do not exist in a silo. Your IP-based devices operate within a broader web of interconnected technologies – and your network may only be as strong as its weakest link.

To minimize the risk of unauthorized access, work closely with IT to ensure safeguards like firewalls and access control lists are in place. A good vendor will also provide a network port list to ensure their solutions can work across your network. Plus, consider using network segmentation, like **VLANS (Virtual Local Area Networks)**, to help prevent threats from reaching more sensitive areas of the network.

For an added layer of protection, some educational institutions adopt IT architectures based on zero trust principles. In a **zero trust network**, no entity (whether human or machine) connecting to or operating within the network can be trusted. This demands that entities be verified multiple times, and in multiple ways, depending on the nature of the data.

Zero trust networking requires that your vendor meet certain IT requirements, frameworks and standards that support such environments. Implementing robust protocols for port-based network access control and device authentication are essential for secure integration into IT infrastructures.

7 Implement devices according to IT policy

Adding compromised or inadequately hardened devices to your network could lead to unauthorized access to your system, extraction of sensitive data, and other potentially costly outcomes.

To protect your network and minimize risk, ensure you are only installing trusted applications and disable all unused services, protocols, and ports on your devices. If left enabled, services such as **File Transfer Protocol (FTP)**, **Telnet and Secure Shell (SSH)** could become entry points for exploitation and used to install malicious applications or scripts.

Proper physical installation of IP-based security products is also essential in safeguarding your system. Network ports and SD cards should never be exposed or publicly accessible to prevent unauthorized access, installation of malware or other forms of physical tampering.

8 Enforce clear access rights

Unclear roles and access rights can lead to network security failures – intentional or not - and overall confusion over responsibilities for system management.

When evaluating user access, it's recommended to use the principle of **"least privileged accounts."** This means that access is limited to just the resources needed to effectively perform the job - and nothing more. The only clients that should be allowed to interact with devices are video management systems (VMS) or device administration and management tools. System users should never be allowed to access devices directly.

Enforcing proper user account management and password policies ensures that your devices are protected from unauthorized access or attempts to reach devices outside of a video management system.

9 Encrypt your connections

Data transmitted over a network can be vulnerable to interception or eavesdropping while in transit.

That's why encrypted connections should be used on all networks — even local or internal ones. Modern systems should use at least one common protocol, like HTTPS or HTTP Digest Authentication, which encrypt information before it's transmitted.

Additional security measures include:

> Secure Real-Time Transport Protocol (SRTP) - encrypts video streams (requires support from camera and video management system)
> IEEE 802.1AE Media Access Control Security (MACsec) – encrypts and authenticates traffic at the data link layer (requires support from device and network switch)
> Encrypt SD cards used for local video storage
> Ensure video is encrypted on the storage array when using a video management system.

10 Update software; follow a maintenance plan

No software is 100% free of vulnerabilities. Regularly updating software (including software for devices) and adhering to a maintenance plan is crucial for the overall health, security, and stability of your school system.

Software updates and security patches address vulnerabilities, bugs and other performance issues. Maintenance plans should be assessed annually (at minimum) to ensure they support the needs of your organization.

Some routine practices include:

> Regularly monitoring devices and checking system logs to detect suspicious activities
> Enabling system notifications when available to help stay on top of changes in real time
> Updating software to patch vulnerabilities and fix bugs
> Reviewing IT security policies to maintain alignment with company goals
> Auditing user accounts and permissions and updating passwords

To learn about cybersecurity at Axis, visit:
www.axis.com/cybersecurity

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.