PowerSchool

DIGITAL CHECKLIST:

20-Point Cybersecurity Inspection for Edtech Vendors

HERE'S WHAT YOUR EDTECH VENDORS NEED TO PROVIDE TO HELP PROTECT YOUR VALUABLE DATA FROM CYBERSECURITY THREATS

Cybersecurity is a collaborative effort. And your No. 1 partner in protecting valuable student, staff, and school data should be your K-12 edtech vendor, bringing expertise and certifications to prove their value.

When choosing or re-evaluating your edtech partners, make sure you work with vendors that are transparent in their cybersecurity policies and practices. **Vendors should offer holistic cybersecurity measures that encompass:**

Company best practices

Product security

Software hosting

Use this helpful checklist to put your software vendor and its commitment and ability to protect your data to the test.

Check any of these features your edtech vendor can verify.

Edtech Company

Your software vendor should be a good custodian of your student data—taking all reasonable and appropriate countermeasures in ensuring data confidentiality, integrity and availability.

- ☐ **Dedicated Security Team**—Chief Information Security Officer leads a team of experienced professionals
- ☐ **24x7 Security Operations Center**—fully staffed 24x7, monitoring for security events, proactively hunting for threats
- ☐ **Compliance/Student Privacy Pledge**—signatory of the national Student Privacy Pledge, and adherence to FERPA, HIPAA, the Children's Online Privacy Protection Act, Breach Laws, Data Residency Laws, the Digital Millennium Copyright Act (DMCA), the Sarbanes-Oxley Act, and state contracts for reporting
- ☐ **Customer Data Handling**—ensuring data residency, with no information going offshore, and strict policies and processes to handle data safely
- ☐ **Security Awareness Training**—extensive and ongoing security/cybersecurity training for all vendor employees, along with secure coding training for software engineers
- ☐ **SSO/MFA**—utilizing single sign-on and multifactor authentication to access business systems
- ☐ **ISO 27001/SOC 2 Controls**—independent audit (certified and renewed annually) to verify business operations are run securely and professionally, including company strategy, operations, HR, and finance
- ☐ **Responsible Disclosure Policy**—actively engaging with security researchers to identify and resolve vulnerabilities

___ **/8 Number of Boxes Checked**

LEARN MORE: Blog: K-12 Data Security Tips from a Chief Information Security Officer? >

Product Security

Your software vendor should certify the application, database, and infrastructure security of its solutions.

- ☐ **Penetration Testing/Vulnerability Scans**—penetration tests should be conducted by independent testers at least annually, and vulnerability scanning is done continuously as part of development
- ☐ **ISO 27001/SOC 2 Controls**—ensuring software is adequately tested prior to deployment, and that robust security and privacy practices are in place
- ☐ **Secure Software Development/OWASP**—confirming security is considered in the entire end-to-end process of developing software, including training, processes, code reviews, and vulnerability scanning
- ☐ **SSO/MFA Support**—for advanced security, product platforms should support SSO integrations with an external identity where MFA can be enabled for an additional layer of security

___ **/4 Number of Boxes Checked**

LEARN MORE: eBook: Security Tips That Will Protect Student Data Today >

Cloud Hosting

Hosting with a reliable provider gives you a secure, responsive software environment to reduce risk, foster an efficient edtech environment, and save staff time and infrastructure costs.

- ☐ **Top Cloud Provider with Proven Physical Security**—physical access is strictly controlled at the building perimeter and data center floors with video surveillance, biometric identification, and professional security staff
- ☐ **ISO 27001/SOC 2 Audits and Reports**—supporting the most critical processes of managing student, class, and school data with a commitment to the highest standards of protection for this data
- ☐ **Cybersecurity/DoS/Malware Protection**—managed EDR/NGAV protection against malware and viruses, industry-standard AES-256 data at rest encryption, internal servers isolated from the internet, NGFW/IPS/IDS to monitor for cybersecurity threats, and web traffic protection includes TLS for secured data in transit and perimeter edge DoS prevention and mitigation
- ☐ **Formal Incident Response Plan**—modeled after the PICERL process (Preparation, Identification, Containment, Eradication, Recovery, and Lessons)
- ☐ **Secured Access Controls**—for vendor staff to access your hosting systems, an automated password and session management solution provides secure access control, auditing, alerting, and recording
- ☐ **Security Operations Center (SOC)**—a centralized unit that deals with security issues on an organizational and technical level, and outlines audits, tools, and how to configure the network to keep information secure
- ☐ **SOC 2 Compliance for Service Organizations**—report (audited annually) to ensure risk and exposure to your data is minimized, requiring companies to establish and follow strict information security policies and procedures
- ☐ **DR/Rapid Deployment**—ensuring a robust process for safe and efficient backups located in independent infrastructure, and automated processes for rapidly deploying new systems in the event of catastrophic events

___ **/8 Number of Boxes Checked**

LEARN MORE: On-Demand Webinar: Top Benefits of Moving to Cloud Hosting >

☐ **Total Number of Boxes Checked**

SEE YOUR RESULTS >

What's Your Vendor Cybersecurity Score?

How many boxes did you check? _____

Look at the areas with lower scores to determine where to prioritize your next steps.

10 or less:

It's time for a new edtech vendor.

Your vendor isn't committed to protecting your data, leaving you at risk for cyberattacks.

11-14:

Your vendor is using some best practices, but not enough.

You need more comprehensive protecting and practices in place.

15-19:

The vendor isn't doing all it can to keep data secure.

While data security is a high priority, there are still key areas where your edtech vendor is falling short and potentially leaving your information at risk.

20:

Congratulations! Your vendor is a model of excellent cybersecurity.

Your edtech vendor is an excellent custodian of student data, placing a high priority on cybersecurity.

Learn more about PowerSchool Security

Find out how partnering with a company that makes your data security its top priority can benefit your entire operations.

Visit www.PowerSchool.com/security or call 1-877-873-1550

PowerSchool

PS-PS-fl-004-011921