

Cybersecurity Supply Chain Risk Management

This category asks whether the district knows every vendor that touches its data or keeps school running, holds them to written security requirements, and verifies they deliver.

Why it matters

- Student information systems, learning platforms, transportation, nutrition and special education software keep district data on vendor servers. When one of those vendors is breached, families and reporters call the district, and the district carries the notification work and the loss of trust.
- Contract terms decide what happens in a vendor incident: how quickly the vendor must tell you, whether it shares what the investigation found, and whether your data is deleted when the contract ends. Without those terms, the district has little leverage once an incident is under way.
- Many vendors have remote support access to district systems such as HVAC controls, phone systems and the student information system (SIS). Knowing who has that access and requiring multi-factor authentication (MFA) for it closes a route into the network that bypasses staff entirely.

K12 has learned this the hard way: in the PowerSchool breach, student and staff records were exposed through the vendor's systems for districts across the country, regardless of how well each district ran its own security. When a vendor fails, the district still owns the breach notifications, the community trust damage, the state scrutiny, and the insurance claim, so vendor risk is district risk.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	Vendors are chosen for features and price, and no one has a full list of who holds district data or can reach district systems. Security questions come up only after a vendor reports a problem. Moving up: Start the supplier inventory — every vendor and the systems, components, or services they provide — and stand up a repeatable way to evaluate key vendors, with compliance improvement efforts underway for the most important ones.	<ul style="list-style-type: none"> • No vendor inventory beyond accounts payable records • Contracts signed on vendor paper with no breach notification or data deletion terms • An unknown number of teacher-adopted apps connected to student Google or Microsoft accounts
2 · Repeatable	A vendor inventory is being built and the most important vendors get a consistent review before purchase or renewal. The district has started asking key vendors to fix weak terms or practices. Moving up: Fold suppliers into documented risk management processes: identify, document, and prioritize them, then routinely confirm contractual obligations through audits, test results, SOC 2 reviews, or questionnaire cycles.	<ul style="list-style-type: none"> • Partial vendor inventory seeded from single sign-on dashboards and purchasing records • Standard security questions used for new SIS, learning management system (LMS) or finance purchases • Requests to key vendors for updated data privacy agreements (DPAs) or MFA on their support access
3 · Defined	Every vendor that touches district data or systems is in the inventory, ranked by criticality and covered by documented security requirements. Critical vendors are checked on a schedule using audit reports, questionnaires or test results to confirm they meet their contracts. Moving up: Require key vendors to demonstrate routine testing of their own controls, insist on independent audits and valid certifications, and track corrective actions on any identified weaknesses to closure.	<ul style="list-style-type: none"> • Vendor inventory with data types, type of access and criticality tier • Standard contract security exhibit or the National Data Privacy Agreement (NDPA) used for new purchases • Annual review file for each Tier 1 vendor with a current System and Organization Controls 2 (SOC 2) report or completed questionnaire
4 · Managed	Critical vendors must show that they test their own controls and must provide independent audit reports or valid certifications. Weaknesses found in vendor reviews are tracked with the vendor until they are fixed. Moving up: Select vendors based on risk and mission impact, run response and recovery planning and testing with critical providers at least annually, and feed the results into continuous improvement of the program.	<ul style="list-style-type: none"> • Contract terms requiring annual independent audit reports or certifications from critical vendors • Vendor corrective-action tracker with due dates and vendor responses • Cabinet briefing on the risk status of critical vendors

Level	What you would see	Artifacts that show it
5 · Optimized	Security and mission impact are weighed in every vendor selection, and critical vendors take part in the district's response and recovery exercises each year. Results from exercises and reviews shape renewals and the next round of requirements.	<ul style="list-style-type: none"> Procurement scoring sheets that weigh security and data risk alongside cost and features Annual tabletop or recovery test that includes the SIS, identity or backup provider Contract changes or vendor decisions that resulted from exercises and reviews, with records to show it

Quick wins

Quick win and how	Cost	Effort	Usual owner
Export the app list from Clever, ClassLink, or your Google/Microsoft admin console to seed the inventory In the Google Admin console go to Security, then Access and data control, then API controls to see third-party apps with access to district accounts; in Microsoft Entra, review Enterprise applications. Combine that with the single sign-on dashboard export and flag every app that reaches student data.	Free	Hours	Network and systems administrator
Join your state SDPC alliance and adopt the NDPA Join through your state's Student Data Privacy Consortium (SDPC) alliance, or the national SDPC if your state has none, and search its registry for agreements your vendors have already signed. Send the National Data Privacy Agreement (NDPA) to vendors without one and record each status in the vendor inventory.	Low cost	Days	Data privacy officer
Tier your top 10 vendors by data sensitivity in one meeting Bring the technology director, business official and a curriculum lead together and sort vendors into tiers: Tier 1 holds bulk student or staff data or keeps school open, Tier 2 holds limited data, Tier 3 holds none. Record the tier in the inventory and agree on what review each tier gets.	Free	Hours	Technology director
Add a breach-notification clause to the next contract renewal With legal counsel, write standard language requiring the vendor to notify the district within a defined period after discovering an incident affecting district data, cooperate with the investigation, and return or delete data at contract end. Add it to the next renewal on the calendar and reuse it as a standard exhibit.	Low cost	Days	Procurement and contracts lead
Subscribe to K12 SIX advisories to catch vendor incidents early Review K12 SIX membership options and sign up the technology director and a backup to receive its threat alerts, confirming cost before committing. When an alert names a vendor you use, check the inventory and contact the vendor's security contact the same day.	Low cost	Hours	Information security lead

Free means staff time, existing licenses or free government services. Effort: hours, days or weeks.

Common pitfalls

- Vetting only purchased software. Free apps teachers connect to student accounts collect data too; route them through the same approval and data privacy agreement process, and restrict unapproved third-party app access in the admin console.
- Accepting marketing claims as due diligence. A vendor web page saying data is 'encrypted and secure' is not evidence; for critical vendors ask for a System and Organization Controls 2 (SOC 2) report or completed questionnaire, and treat a vendor that cannot answer as a risk in itself.
- Forgetting vendor remote access. Support tools left open for HVAC, phone, camera or SIS vendors give outsiders a way into the network; inventory every vendor remote access method, require MFA, and enable access only when it is needed.
- Letting data stay behind after a contract ends. A former vendor may keep student records unless the contract says otherwise; request written confirmation of deletion when the relationship ends and remove its accounts and integrations.
- Leaving vendors out of incident planning. In a vendor-caused incident you need the vendor's security contact, not the sales representative; put escalation contacts for critical vendors in the incident response plan and confirm them each year.

Evidence that proves it

- Vendor inventory with data types and criticality tiers
- Signed DPAs and NDPA registry entries for edtech vendors
- Contract security exhibit or standard clause template
- SOC 2 reports or completed security questionnaires on file for Tier 1 vendors
- Annual vendor risk review notes
- Vendor escalation contacts embedded in the incident response plan
- Data deletion certificates from offboarded vendors

Who usually owns it

Technology director	Maintains the vendor inventory and tiers, performs pre-purchase security review and runs the recurring vendor assessment cycle.
Procurement and contracts lead	Makes sure purchases and renewals include the required security and privacy terms before signature.
Data privacy officer	Manages data privacy agreements and the approved-apps list and confirms data deletion when vendors are offboarded.
Curriculum and instruction lead	Routes instructional apps through approval and helps teachers find approved alternatives.

Insurance relevance · High

Carriers ask whether the district inventories its vendors, checks their security before granting access, and holds them to contract terms for data protection, breach notice and data return. Some policies also limit recovery if the district gave up its rights against a vendor that caused the loss, so contract terms matter to the claim as well as to security.

- Do you keep an inventory of vendors that access your systems or hold your data?
- Do you assess a vendor's security before giving it access to your network or sensitive data?
- Do vendor contracts require data protection, breach notification and return or destruction of data?
- Must vendors with remote access to your network use multi-factor authentication?

Tip: Before answering yes to the contract questions, confirm that your largest data holders actually have signed agreements with those terms, and note any exceptions.

Funding and free help

CISA K-12 cybersecurity resources and toolkit

Always available

Free federal guidance for K-12: the K-12 cybersecurity report and toolkit, plus access to regional CISA advisors and no-cost services. A resource, not funding.

Programs, eligibility and deadlines change; confirm on the official page before applying.

Learn more

- Cybersecurity Guidance for K-12 Technology Acquisitions (CISA)
<https://www.cisa.gov/resources-tools/resources/cybersecurity-guidance-k-12-technology-acquisitions>
- Student Data Privacy Consortium (SDPC) (Access 4 Learning Community) <https://privacy.a4l.org/>
- Protecting Student Privacy (U.S. Department of Education) <https://studentprivacy.ed.gov/>
- Information and Communications Technology Supply Chain Security (CISA)
<https://www.cisa.gov/topics/information-communications-technology-supply-chain-security>
- The K12 SIX Essentials Series (K12 SIX) <https://www.k12six.org/essentials-series>
- Multi-State Information Sharing and Analysis Center (MS-ISAC) (CIS) <https://www.cisecurity.org/ms-isac>