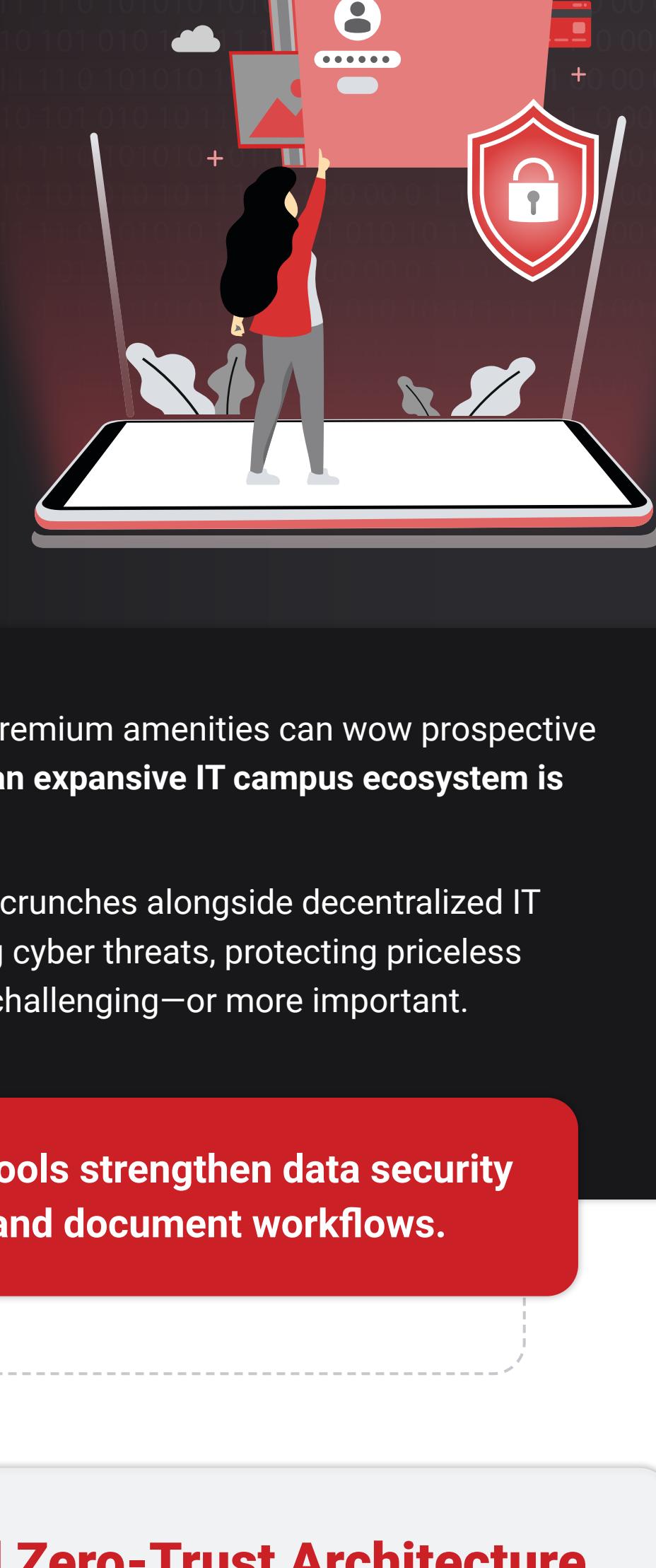


Canon

9 Smart Strategies to Help Secure Student Data in Higher Ed



On college tours, a beautiful campus and premium amenities can wow prospective students and their parents. Unfortunately, an expansive IT campus ecosystem is just as enticing to cybercriminals.

As higher education grapples with funding crunches alongside decentralized IT environments, limited staffing, and growing cyber threats, protecting priceless student information has never been more challenging—or more important.

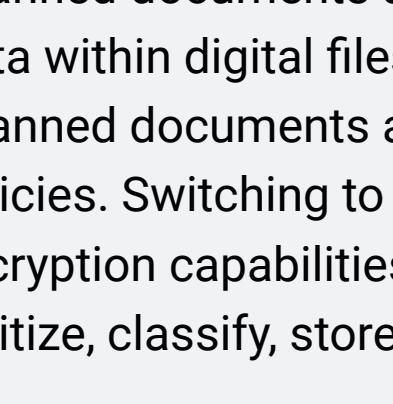
These nine steps can help schools strengthen data security with modern, secure print and document workflows.



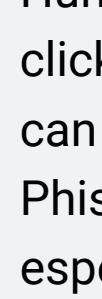
Move Toward Zero-Trust Architecture

A zero-trust model requires users to verify their identity continually. Multi-factor authentication (MFA), or using two or more credentials to access devices, helps prevent unauthorized access and bolsters a college's zero-trust posture.

While most universities already have MFA in place for their core systems, many fail to secure devices like printers, scanners, copiers, and multifunction devices (MFDs) properly, creating an easily exploitable gap. Cloud-connected print devices can be configured for MFA, creating consistent protection across every endpoint.



80% of higher education organizations have zero-trust strategies in place.¹



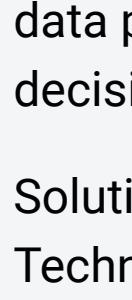
Shrink Attack Surfaces

Departmental silos and bring-your-own-device (BYOD) cultures on campus create large attack surfaces with multiple entry points for hackers. That's why many CIOs are reducing their IT footprint by consolidating one-off devices like desktop inkjet printers and replacing them with cloud-connected network fleets. Doing so narrows potential points of compromise. It also reduces licensing and IT support costs.



Secure Print Jobs

Some cybercrimes are decidedly low-tech. Consider a busy employee printing multiple documents from their desktop just before a critical meeting. In a rush, they grab a stack of papers off the printer but leave others behind. If those stray papers get into the wrong hands and they contain a student's social security number or a vendor's bank account information, that data is instantly compromised. Schools can avoid these scenarios with best-in-class devices that require badge access, so users must stand at the printer before releasing jobs.



Protect Scanned Documents

Scanned documents also open the door to multiple vulnerabilities. Data within digital files must be encrypted for full protection. Scanned documents also must comply with a university's retention policies. Switching to modern scanning technology with data encryption capabilities empowers educational institutions to digitize, classify, store, and retrieve information securely.

With such solutions, IT can encrypt set rules for the easy retrieval of scanned documents and improve information governance. They can also archive or dispose of outdated data in accordance with their retention schedules, supporting compliance initiatives. What's more, modern scanners can support master data management and enable the use of AI and machine learning to automate tasks and improve efficiency.

Sources:

¹EDU 2024 Nonprofit Standards Benchmarking—Higher Ed: The Importance of Zero Trust, July 2025.

²Doppel, Social Engineering Tactics: Higher Education Phishing Attacks Surge, September 2025.

³IBM, "What Is a Data Breach?", May 2025.

⁴EDU 2024 Nonprofit Standards Benchmarking—Higher Education Snapshot, October 2024.

⁵Canon USA does not provide legal counsel or regulatory compliance consultancy, including without limitation regarding Sarbanes-Oxley, HIPAA, CCPA, GDPR, GLBA, Checkoff 21, or the Patriot Act. Canon does offer certain security features, yet many variables can impact the advisability of a particular solution. Canon does not warrant that use of its features will prevent security issues. Some security features may impact functionality; you may want to test these settings in your environment.

⁶©2025 Canon U.S.A., Inc. All rights reserved.

Canon is a trademark of Canon Inc. in the United States and elsewhere.

Embrace Trusted Security Frameworks

Every new solution that colleges choose must be vetted fully for data protection capabilities. Trusted frameworks can help simplify decision-making for both IT and procurement leaders.

Solutions that align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) follow guidelines and best practices for governing and protecting information.

Cloud services achieving Federal Risk and Authorization Management Program (FedRAMP) authorization provide standardized security assessments, helping to reduce duplicate testing and accelerate procurement.

Safeguard Student Privacy With The Support of A Unified Approach

In the same way that it takes a village to educate a student, it takes a unified approach to keep sensitive student information safe. Consolidating multiple vendors into one contract can provide a secure, end-to-end, cloud-based digital workflow that helps to meet a university's printing needs and protects student data.

Canon offers an integrated ecosystem of technology (like uniFLOW Online), managed security services, and secure multifunction devices to help universities print securely, digitize smartly, and protect student data.

Explore how Canon supports student success in higher ed.

©2025 Canon U.S.A., Inc. All rights reserved.