



A CENTER FOR DIGITAL EDUCATION HANDBOOK

# Safeguarding Data and Student Privacy: A Handbook for Higher Education



# Introduction

**C**olleges and universities are leveraging data analytics, artificial intelligence (AI) and other technologies to support student success, streamline operations and more. All these efforts involve the extensive use of data, including financial information, student and staff demographics, personal identifiable information (PII), and student engagement data created by institutional services and programs.

These advancements are revolutionary. But digital services and the increased use of data make higher education institutions prime targets for cyberattacks.

"Part of the reason attackers love higher ed is that we have just about anything and everything," says Ed Wozencroft, CIO and vice president of digital strategy at the New Jersey Institute of Technology (NJIT).

Technology leaders have a dilemma. While they must ensure this growing volume of data is secure, they must also enable stakeholders throughout the institution to use data to meet their institutions' evolving missions.

"Protecting the data is a key responsibility," says Brian Cohen, vice president of the Center for Digital Education (CDE). "But integrating the data, providing access to business users, and enabling data-driven decision-making are also key responsibilities."

This guide examines what it takes for higher education institutions to safeguard data, mitigate risks and remain compliant with institutional obligations to protect private information.

**"Part of the reason attackers love higher ed is that we have just about anything and everything."**

— Ed Wozencroft, CIO and Vice President of Digital Strategy,  
New Jersey Institute of Technology

## More on Protecting Privacy

These free webinars from the Center for Digital Education offer more insights from higher education CIOs and privacy experts:

- **Privacy Compliance 101 in Higher Education**
- **Technology to Keep Data Safe in Higher Education**





# The Challenge

**H**igher education faces unique challenges to safeguarding data.

- According to a 2023 survey by Sophos, the education sector has the highest rates of ransomware attacks, with 79% of higher education institutions surveyed reporting a breach — up from 64% in 2021.<sup>1</sup>
- The siloed culture of higher education and the intensive use of data across different departments make colleges and universities an appealing target.
- Many institutions operate healthcare facilities or conduct research, both of which involve sensitive — and lucrative — data. As an R1 research institution, NJIT manages more than \$160 million in research expenditures each year, according to Wozencroft. “We have students active in research, so I can’t necessarily secure a perimeter and say, ‘Researchers, go live here,’” he says. At the same time, he adds, a breach “could cause not just a reputational risk, but an issue for our revenue diversity and the integrity of our campus.”

“There are so many people functioning independently — HR offices, finance, enrollment, institutional research, fundraising, marketing and more,” says Cohen, who previously served in IT leadership roles in government and the City University of New York (CUNY). “Each department has its own data sources, and in some cases its own financial transactions. There is a risk they will

be distracted by their business needs instead of the need to protect the university and the people they’re serving.”

Other reasons cyber risks are increasing for higher education:

- **New digital tools and technologies.** “We’re all going through digital transformation, and there’s a cybersecurity risk there,” cautions CDE Senior Fellow Jim Jorstad, retired emeritus interim CIO and cybersecurity lead at the University of Wisconsin-La Crosse.
- **New vulnerabilities.** As in other organizations, higher education institutions are rapidly deploying sensors and other smart devices that are part of the Internet of Things (IoT). Insider Intelligence forecasts there will be 64 billion IoT devices worldwide by 2026 — every one of which could become an entry point for attackers.<sup>2</sup>
- **New advantages for bad actors.** Attacks are becoming more damaging and easier to deploy as cybercriminals use AI and other tools. According to IBM, it takes 277 days on average to identify and contain a breach, while the time it takes to deploy a ransomware attack has grown shorter — from two months just a few years ago to now under four days.<sup>3</sup>

“Every CIO has come to accept the fact that they’re going to have attacks or cyber events,” Cohen says. “The question is how organized they are from an institutional perspective to quickly respond and recover.



# Privacy Considerations

**C**yber breaches aren't the only way data poses reputational, financial and regulatory risks. Along with securing data, technology leaders must also ensure data privacy.

Institutions must conform to a growing number of privacy requirements, standards and policies, including those protecting student (FERPA) and medical (HIPPA) information, financial standards (PCI), international privacy laws (GDPR), and, in many cases, state privacy laws and requirements that institutions report security breaches to affected parties. Keeping up with rapidly changing privacy regulations was the top concern cited by higher education IT professionals during a November CDE webinar on data privacy.

"In the past, IT only had to worry about FERPA and HIPPA," Cohen says. "It's become far more complicated and convoluted"

As in other sectors, the challenge of protecting data privacy has grown more complicated as a result of the COVID-19 pandemic. Colleges and universities have rolled out new digital tools and platforms to

**Along with securing data, technology leaders must also ensure data privacy.**

help students, faculty and staff stay connected. These tools are immensely helpful in enhancing the learning experience and improving campus operations — but they pose new privacy risks.

"The value add of edtech is a no-brainer," says Cristina Blanton, chief privacy and data protection officer of the University of Texas system. "We all need it, we all use it, and we all want to add more."

Each digital tool has its own policies and practices for collecting, storing and using data, which institutional leaders must understand and evaluate to prevent breaches and misuse by third parties. "It can keep any privacy officer busy 24/7," she says.



# Data Privacy Strategies

**H**igher education CIOs and privacy experts have outlined a number of strategies to make data protection a priority.

## ✚ Take an ecosystem approach.

"If you don't have an enterprise perspective, it's hard to minimize risk," Cohen says.

Make sure senior leadership, including the president's office, CFO and board, understand and support the need for cybersecurity and privacy.

"Privacy and cybersecurity require senior-level leadership," Cohen says. "The CIO should not be on their own."

An enterprisewide approach requires support from other stakeholders, including representatives from IT, legal, compliance and research, as well as academic deans, provosts and student services staff.

## ✚ Create data governance structures.

Formal governance committees and structures can help institutions adapt to the changing realities of data use and regulations.

They also help bring together the many different stakeholders using data. "Breaking down silos is such a big deal, and only governance can get you there," says Bhavani Koneru, CIO of Oakland University in Michigan.

It's important to understand the unique privacy needs of different parts of your institution. In the University of Texas system, for example, privacy questionnaires collect information about data use and help stakeholders understand the importance of a comprehensive privacy framework.

"We look at the use cases and work through the principles — what data is it, what is it being used for, who is getting the data, how are they planning to secure it, and how do we ensure we're using the data in ways that maintain the chain of custody," Blanton says. Ideally, these conversations should take place before a new project or tool is ever embedded into the institution's IT ecosystem.

## ✚ Develop policies and procedures.

Armed with knowledge of the business needs for data use and the compliance and regulatory frameworks they must follow, IT leaders and governance committees can develop actionable policies and procedures.

Shared responsibility is one guiding principle of privacy and security policies. "You own this along with us," Wozencroft says.

Policies must strike a balance between data access and risk mitigation — in other words, reducing the amount of sensitive data in use and the number of people who have access to it.

Ongoing audits are also an important part of privacy policies, according to Koneru, who stresses the value of communication with stakeholders. “Sometimes it’s not easy to explain why we’re doing the audits,” she says. “Pick up the phone if you have to.”

#### ✚ Adopt proper controls.

Once policies are in place, they must be implemented and monitored. “Compliance doesn’t just come out of the box,” Cohen warns.

For example, institutions must establish controls to make sure only authorized individuals have access to data. Under a Zero-Trust framework, permissions to access data and applications are closely monitored across internal and external users.

Other vital access control solutions include multifactor authentication, network segmentation and firewalls, data encryption, and tools to monitor network traffic and flag anomalies — a capability Cohen calls “the most important thing in a CIO’s toolkit.”

#### ✚ Make sure third-party technology meets privacy requirements.

Given the growing number of solutions developed by third-party vendors and housed in the cloud, institutions must verify that each application and service meets privacy and security requirements. “Having a good vendor management compliance program is crucial,” Blanton says.

One strategy is to work with procurement officials to make sure new devices, solutions and services align with security and privacy regulations and policies. At Oakland University, for example, a partnership between IT and the purchasing department ensures that no hardware or software is procured without a full IT review. Koneru estimates her department reviews 10 to 20 new products each month, often with support from the university’s legal and risk management departments. “The biggest piece of that compliance review is data privacy,” she says.

Once technology is in place, it’s important to regularly review third-party vendors’ policies and procedures. At NJIT, for example, Wozencroft holds quarterly briefing sessions with his technology partners and encourages IT staff to stay informed of changes. “That’s not just your security staff — that’s everyone,” he says.

#### ✚ Train faculty, staff and students.

Making sure all stakeholders are aware of privacy and cybersecurity is essential at all levels of the institution, including:

- **Leadership.** Brief leaders about how data is collected, the potential threats and any reported incidents — “not just at the cabinet level but at the board level so they see the visibility,” Koneru says.
- **Students, faculty and staff.** Along with mandatory cybersecurity training, many institutions conduct “penetration tests,” including sending fake phishing emails to assess student and staff awareness and promote a greater understanding of the importance of cybersecurity.
- **Student government and institutional structures** like the faculty senate can also share information. Make the danger of breaches personal — for example, using faculty who have lost data in attacks as advocates to demonstrate to colleagues that “it happened to them, and it can happen to you,” Jorstad says.
- **IT staff.** Training is also critical to make sure all IT staff are aware of the tools they are using and any changes in policies and procedures. All staff should also know about the compliance and privacy regulations the institution must follow.

“When the entire IT team fully understands the rules and requirements, they’re in a better position to ensure the systems they’re developing maintain compliance,” Cohen says. “Otherwise, they’re flying blind.”

#### ✚ Develop recovery plans.

Cyber incidents are inevitable. Implement a business continuity and disaster recovery plan to mitigate the damage from ransomware attacks, natural disasters and other incidents that block access to data.

These plans should identify a response team of IT experts and other staff with clearly defined roles and responsibilities. Institutional knowledge of internal processes is critical to ensuring these teams can react quickly and reduce recovery time.

# Conclusion

**A**s the volume of data that institutions manage continues to grow, so will the challenges — and the opportunities. For example, the rapid proliferation of generative AI tools in the past year has raised new privacy concerns. At the same time, the technology has sparked productive discussions about the potential risks of losing custody of sensitive information.

“Every single thing that comes to your table as a threat, take it as an opportunity to change what you are doing today,” Koneru says. “That is how you mitigate risk.”



1. <https://news.sophos.com/en-us/2023/07/20/the-state-of-ransomware-in-education-2023>
2. <https://www.insiderintelligence.com/insights/internet-of-things-definition>
3. <https://www.ibm.com/reports/data-breach-action-guide>

*This piece was written and produced by the Center for Digital Education Content Studio.*



#### **Produced by the Center for Digital Education**

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21<sup>st</sup> century.

**[www.centerdigitaled.com](http://www.centerdigitaled.com)**



#### **Sponsored by Zscaler**

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile and secure. The Zscaler Zero Trust Exchange, a SASE-based platform, is the world's largest inline cloud security platform, protecting thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications over any network.

**[www.zscaler.com](http://www.zscaler.com)**