# Solving Identity Management in Higher Education

**One of the biggest technology** priorities in higher education is giving students and staff secure, frictionless access to a variety of devices, applications and data sources.

Modern cloud-based identity and access management (IAM) platforms help colleges and universities meet this need by consolidating identities, simplifying role policies and strengthening cyber-defense strategies.

## Cloud IAM Platform Advantages

User behavior varies considerably in higher education. A student with five logins might drop out after three semesters, while a tenured professor might have 10 logins and stay for decades. Guest lecturers, alumni and visiting researchers add more variables to the mix.

Cybercriminals take advantage of these complex dynamics to gain access. Modernizing IAM gives campus IT teams the tools to prevent identity-based cyber intrusions — if they choose technology carefully.

"Getting IAM right is like the holy grail," says Ronald Bergmann, a senior fellow with the Center for Digital Education and former vice president for information technology and chief information officer at the City University of New York's Lehman College. "Some schools have been dealing with this for five or 10 years."

Cloud-based IAM gives higher education IT leaders and users a path to easier, simpler and more secure identity management. "Putting more of these workloads in the cloud offsets a tremendous amount of the campus IT team's work on things like updates and patches, and reduces the strain on the help desk for password resets," Bergmann says.

The longer you wait to modernize IAM, the harder it may be to reconcile legacy technologies with new capabilities. Here are the most compelling reasons to modernize IAM:

**The longer you wait to modernize, the harder it may be to reconcile legacy techologies with new capabilities.**

### Consolidated Identities

**Challenge**
Students, faculty, staff and IT team members have a complex variety of logins.

**Solution**
Single sign-on (SSO) consolidates identities, creating a seamless experience.

IAM-related anxiety across the public and private sectors inspired vendors to flood the market with identity technologies. Soon, there was too much of a good thing.

"This overgrowth of identity solutions means higher education IT teams might be integrating as many as 60 IAM platforms," says Sean Frazier, federal chief security officer with Okta, whose cloud platform helps simplify and streamline IAM. "It's gotten expensive and time-consuming."

Campus users, meanwhile, become frustrated using separate credentials for each application they use every day. "Organizations have recognized the need for an SSO solution that works for everybody," Frazier says.

SSO gives users identical credentials on every app they use to get their work done, paving the way to a more frictionless campus experience.

An identity cloud platform is essentially a complete access management solution, capable of solving for student and administrator needs with ease. Rather than build their own consolidated solution, institutions can partner with a best-in-class identity cloud to increase their resiliency.

### Simplified Management

**Challenge**
Users access networks anywhere, anytime, on any device, creating massive workloads and security complexity for IT teams.

**Solution**
Standardized policies defining user, device, access and application roles are managed from a centralized platform, easing the pressure on IT teams.

"You can be a student, a staff member, a faculty member and an alum all at once, or you can shift between these roles semester by semester," Bergmann says. "Some people may have multiple roles in multiple systems. It's difficult to manage."

A robust cloud platform provides a policy engine that standardizes IAM at the system level. Users, campuses, devices and applications operate under similar parameters. "If you're not standardizing policies, then you're maintaining two, three or four times the amount of work to run the IT systems," Frazier says.

## Stronger Defense Posture

**Challenge**
**Phishing, social engineering and other cyber threats create an almost unmanageable list of vulnerabilities.**

**Solution**
**Phishing-resistant MFA and AI-based monitoring/response deter intruders and reinforce a Zero-Trust security posture.**

Credentials are popular targets because it's easy to get people to click on a link taking them to a realistic replica of their campus log-in page. Within seconds, their credentials can be compromised. Conventional castle-and-moat security frees intruders to navigate through networks until they find valuable data.

A cloud-based identity platform helps institutions adopt a Zero-Trust framework, which requires verification of every user, device and app while limiting access only to the areas people need to get work done. A cloud platform can also enable AI-based network monitoring to scan for anomalies and flag intruders.

Institutions should also consider adopting phishing-resistant multifactor authentication (MFA).

"MFA alone is better than nothing. But it's time to adopt passwordless and phishing-resistant authentication because attackers have already figured out ways around MFA," Frazier says. Modernizing on a cloud IAM platform is a practical way to adopt a next-generation identity defense.

## IAM Best Practices

Implementing IAM on a cloud platform requires a firm understanding of its human impact. "You need a user-centric approach to modernization," Bergmann says. "You want to enhance, not degrade, the customer experience."

### Practical tips for IAM modernization include:

- **Analyze your environment.** Document all current policies, devices, applications, users and data sources. This lays the groundwork for a sound, secure IAM program.
- **Manage change.** Build the business case and start winning over stakeholders. Prepare everybody for the new technology and provide thorough training. Ensure people follow best practices at every stage of the user journey, from onboarding to departure.
- **Time the transition.** Use slow times like seasonal breaks to test systems and avoid disruptions. It might take multiple summers to complete the transition.
- **Choose partners carefully.** The best platforms create a seamless user experience and enable the latest defense techniques. "Look for partners who are leaders in the space, who understand education, and who will work with you over the long term and not just implement a tool and then walk away," Bergmann says.

## Looking Ahead

Digital identities are a big part of campus life. The success of students and higher education in general rests in part on the ability to keep them secure.

Modernizing IAM means you'll need to transform your institution's culture to help people adopt newer, safer login practices. "There must be education and training so everyone understands their role in IT security," Bergmann says.

**A cloud-based identity platform helps institutions adopt a Zero-Trust framework.**

*This piece was written and produced by the Center for Digital Education Content Studio, with information and input from Okta.*

Produced by:

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 21st century.
**www.centerdigitaled.com**

Sponsored by:

okta

Okta is the World's Identity Company. We free everyone to safely use any technology—anywhere, on any device or app. Our Workforce and Customer Identity Clouds enable secure yet flexible access, authentication, and automation that transforms how people move through the digital world and puts Identity at the heart of business security and growth. Learn more at **okta.com/education**.

SHUTTERSTOCK.COM