CROWN CASTLE

Modern network security for higher education.

College and university networks are supporting more connected devices than ever. At the same time, they're enabling quantum computing, AI and other important technologies that are revolutionizing the way research and learning occur on and off campus. The promise and excitement are real—but so are the new vulnerabilities being exposed. See how our security solutions keep your network safe without slowing down your faculty, researchers and students.

Follow the journey to see how the right solutions facilitate safer, seamless learning and research.

Collaborating and discovering.

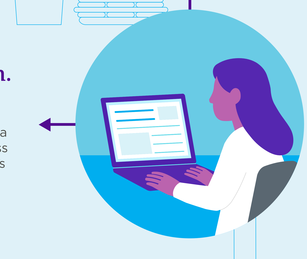
Researchers can freely collaborate with partner organizations, while **Cyber Defense XDR** detects and responds to ransomware and insider threats to keep sensitive data safe.

Managing tight budgets.

Campus network administrators are expected to do more with less. SASE solutions like **Managed SD-WAN** reduce cost and complexity by consolidating multiple functions into a single cloud-managed service.

Breaking for lunch.

Outside the lab, **Secure Remote User** verifies university devices, allowing a researcher to securely access data and verify a colleague's hunch from anywhere.



Getting the message.

Students, faculty and researchers can communicate freely on university email while **Cyber Defense Email Security** blocks phishing and ransomware threats.

Making the grade.

From the library to the dining hall, students can work and study on an ever-expanding network of university-managed computers and devices—all scanned and monitored for risks by **Cyber Defense CRI**.

Bringing home the win.

Attention on campus turns to the game, but a fully staffed **security operations center (SOC)** never loses focus—monitoring traffic, detecting threats and responding in real time.

Advanced solutions bring advanced capabilities.

We have the solutions to secure your network for students, faculty and researchers.

Unified threat management

Monitor network traffic to detect and block viruses and malware.

Cyber risk intelligence

Proactively improve your security posture by identifying and mitigating internal security gaps and weaknesses with automated patch management.

CMMC compliance

Work on and pursue DoD-funded projects using our FedRAMP-authorized platforms and secure GovCloud infrastructure—built to meet CMMC (Cybersecurity Maturity Model Certification) Level 2 requirements.

Penetration testing

Simulate cyberattacks to expose and fix hidden vulnerabilities and gain actionable insights that help you optimize your defenses.

Analytics

Make more informed decisions with improved visibility and transparency into how faculty and students are using the network.

Secure remote access

Use cloud-based security to extend network access to university-owned devices—even when students and staff are off-site.

DDoS protection

Monitor traffic, detect threats and alert key personnel to mitigate DDoS attacks before operations are impacted.

Security operations center (SOC)

Get 24/7 network monitoring from a fully staffed team of experts who detect threats with 98% accuracy and have an average auto triage response time of just 3.63 minutes.*

*As of August 2025

Ready to connect?
Give us a call at 1-888-392-7108.

CROWN CASTLE

Crown Castle owns, operates and leases approximately 40,000 cell towers and approximately 90,000 route miles of fiber supporting small cells and fiber solutions across every major US market. This nationwide portfolio of communications infrastructure connects cities and communities to essential data, technology and wireless service—bringing information, ideas and innovations to the people and businesses that need them.