SERKET-TECH SECURITY

Defending Education from Evolving Threats

Cybersecurity, compliance, and resilience services for colleges, universities, research centers, online programs, and higher education service providers.

Protect student, financial aid, research, payment, and institutional data while supporting academic, research, and administrative continuity.

Higher education institutions operate across classrooms, research environments, student systems, financial aid platforms, cloud services, payment workflows, and a broad mix of departmental technology. A compromised identity, ransomware event, or vendor gap can expose protected records, interrupt teaching and research, affect enrollment or payroll, and weaken institutional trust.

Serket-Tech Security helps colleges, universities, research programs, affiliated entities, and higher education service providers build security programs that fit decentralized operations and limited internal staffing. We support governance, research security, assurance, testing, response, managed protection, and executive guidance across modern academic and administrative environments.

Protect Students, Resources, and Records

Safeguard SIS, LMS, ERP, registrar, advising, email, and cloud systems that handle FERPA records, GLBA-covered data, and other sensitive campus information.

Secure Research, CUI, and Sponsored Programs

Support labs, research computing, and grant-funded environments that may require NIST 800-171 controls, CUI enclaves, stronger segmentation, or CMMC readiness.

Reduce HECVAT, Edtech, and Vendor Friction

Prepare for HECVAT reviews, AI and SaaS risk questions, contract requirements, accessibility and privacy reviews, and remediation follow-through with clearer evidence.

Prepare for Ransomware, Fraud, and Disruption

Improve response, recovery, tabletop exercises, and executive decision-making before a cyber event affects instruction, enrollment, payroll, research, or campus operations.

Best fit for colleges and universities, community colleges, research institutes, university-affiliated entities, online and continuing education teams, shared service units, and education technology providers serving higher education.

SERKET-TECH SECURITY

Comprehensive Service Portfolio

A single partner that can support governance, technical validation, research security, response readiness, and ongoing operations across the higher education security lifecycle.

Governance, Risk, and Compliance

- Higher education security program and policy support
- Risk assessments, control design, and roadmap development
- FERPA, GLBA, Red Flags, privacy, and governance alignment

Data, Identity, and Cloud Security

- Email, endpoint, identity, tenant, and collaboration hardening
- MFA, privilege, conditional access, and segmentation reviews
- Logging, encryption, backup, and cloud security design

Third-Party, Procurement, and HECVAT Support

- Vendor due diligence, contract review, and data flow analysis
- HECVAT preparation, response support, and evidence collection
- Edtech, AI, accessibility, and remediation workflow support

Security Assessments and Testing

- Security posture, maturity, and architecture assessments
- Vulnerability assessments, attack surface review, and remediation planning
- Internal, external, cloud, web application, and identity testing

Research, CUI, and CMMC Readiness

- NIST 800-171 gap assessments, SSPs, and POA&Ms
- CUI enclave strategy, access control, segmentation, and monitoring
- CMMC readiness support for DoD research and affiliated entities

Assurance and Trust Support

- SOC 2 readiness and attestation support for edtech, platforms, and shared services
- HITRUST readiness where health, partner, or data sharing requirements apply
- Evidence planning, remediation coordination, and control ownership

Response, Resilience, and Managed Services

- Ransomware, BEC, and business disruption playbooks and exercises
- Breach support, forensic coordination, and recovery planning
- Ongoing monitoring, detection, response, and issue tracking

Leadership and Program Development

- Fractional CISO and strategic advisory support
- Roadmaps, budget prioritization, and governance design
- Executive briefings, board reporting, and tabletop facilitation

Programs can be tailored to FERPA, GLBA, Red Flags, HECVAT, NIST 800-171, CMMC readiness, PCI DSS, sponsor terms, and, where applicable, HIPAA, CJIS, and export control needs.

SERKET-TECH SECURITY

Built for Higher Education Sector Realities

Serket-Tech Security focuses on the overlapping pressures higher education leaders face across open campuses, decentralized technology, research obligations, procurement scrutiny, and lean internal staffing.

- **Decentralized Campuses and Identity Sprawl**
  Reduce risk across colleges, departments, labs, shared services, student workers, adjuncts, alums, contractors, and hybrid identity environments with stronger access and visibility.
- **Student Aid, Records, and Fraud Pressure**
  Protect education records, financial aid systems, FAFSA-related data, and sensitive communications while improving controls around account compromise, impersonation, and process abuse.
- **Research Security, CUI, and Export-Controlled Work**
  Support funded programs that handle CUI or other sensitive research data, and help align secure enclaves, NIST 800-171 controls, CMMC readiness, and sponsor expectations.
- **Payments, Special Units, and Staffing Limits**
  Address PCI DSS and third-party payment flows, and where applicable, the needs of campus health, public safety, or affiliated entities, while augmenting limited internal teams.

How Clients Engage Serket-Tech Security

Engagements can start with a readiness review, targeted assessment, HECVAT or vendor risk initiative, research security and CMMC readiness effort, tabletop exercise, penetration test, assurance initiative, or recurring advisory and managed support program.

1. Assess
Review current posture, obligations, data types, and business priorities

2. Prioritize
Define the roadmap, scope controls, and remediation sequence

3. Implement
Deploy controls, prepare evidence, perform testing, and close gaps.

4. Operate
Monitor, report, respond, and keep the program up to date.

Build a higher education security program that protects trust, supports teaching and research, and withstands sponsor and regulatory scrutiny.