Chief Information Security Officer
Kent State University
September 7, 2018

Kent State University invites applications and nominations for the position of Chief Information Security Officer (CISO). The CISO serves as the University's senior information security executive charged with creating and executing IT security strategy, overseeing security operations, and developing policy and legal compliance efforts. Kent State seeks an experienced leader with a blend of technical, leadership and policy experience to mature a highly effective security program. The CISO reports to the University Vice President for Information Services (CIO), serves as a member of the CIO leadership team, and interacts frequently with senior academic and administrative leaders.

The Leadership Agenda

As the inaugural Kent State CISO, the successful candidate will architect strategies and practices to mature the University's security program. They will play a vital role in influencing behaviors and creating policies, competencies, and deploying technologies that protect the University while facilitating the vital work of our students and faculty.

The CISO leads the development and implementation of a security program that leverages collaborations and campus-wide resources, facilitates information security governance, advises senior leadership on security direction and resource investments, and designs appropriate policies to manage information security risk. The complexity of this position requires a leadership approach that is engaging, imaginative, and collaborative, with a sophisticated ability to work with other leaders to set the best balance between security strategies and other priorities at the campus level. The CISO will craft effective partnerships with Kent Sate's decentralized IT leadership, the Office of Legal Affairs, Police Department, and Internal Auditing to create a comprehensive approach to managing security risks. The CISO leads a team of 8 staff focused on security operations and risk assessment.

The CISO will develop a security agenda that takes a risk based strategy to secure Kent States protected and sensitive data and enhances capabilities to monitor, detect and respond to security breaches. The CISO will advise senior leadership on emerging security threats, changing regulatory requirements to protect research, student and financial data, and design strategies to protect the University in a manner that is cognizant of budget, sensitive to culture, and supportive of the research, teaching, and outreach missions of the University. The CISO will oversee security risk assessments of Information Services and distributed technology units, continue to evolve and expand information security training, and design monitoring mechanisms for technology services that are increasingly a hybrid of cloud and premise based solutions.

Additional duties and responsibilities include:

- Manage institution-wide information security governance processes, chair the Information Security Advisory Committee and lead Information Security Liaisons in the establishment of an information security program and project priorities.
- Establish annual and long-range security and compliance goals, define security strategies, metrics, reporting mechanisms and program services; and create maturity models and a roadmap for continual program improvements.

- Stay abreast of information security issues and regulatory changes affecting higher education at the state and national level, participate in national policy and practice discussions, and communicate to campus on a regular basis about those topics.
- Provide leadership philosophy for the Information Security Office to create a strong bridge between organizations, build respect for the contributions of all and bring groups together to share information and resources and create better decisions, policies and practices for the campus.
- Coordinate and track all information technology and security related audits including scope of audits, colleges/units involved, timelines, auditing agencies and outcomes. Work with auditors as appropriate to keep audit focus in scope, maintain excellent relationships with audit entities and provide a consistent perspective that continually puts the institution in its best light. Provide guidance, evaluation and advocacy on audit responses.
- Keep abreast of security incidents and act as primary control point during significant information security incidents. Convene a Cyber Incident Response Team (CIRT) as needed, or requested, in addressing and investigating security incidences that arise.
- Convene Ad Hoc Security Committee as appropriate and provide leadership for breach response and notification actions for the University.
- Examine impacts of new technologies on the University's overall information security. Establish processes to review implementation of new technologies to ensure security compliance.

Qualifications and Essential Experiences

Candidates must have a Bachelor's degree from an accredited institution of higher education and at least six years of experience directly related to the role. Demonstrated supervisory experience and a Certified Information Systems Security Professional (CISSP) certification or related security certification is also required. A Master's degree and 10 years experience as an information security professional is strongly preferred.

The ideal candidate will have a working knowledge of the strategic technology and information security issues facing higher education, specifically public universities. Additionally, the ideal candidate will have many of the following experiences:

- Developed comprehensive information security plans.
- Conducted security risk assessments of enterprise and distributed technology operations.
- Knowledge of State and Federal regulatory laws and standards for the safeguarding of sensitive information and data, including participation in the design and implementation of security strategies and policies to comply with FERPA, PCI, FISMA, GDPR and HIPAA requirements.
- Participated in the design and management of security operations centers and developed strategies to mine monitoring data to detect security threats.
- Designed policies and strategies to work with cloud sourced technologies and applications.
- Developed and tested critical incident response plans.
- Evaluated and selected security tools and related technologies including firewalls, host and network intrusion detection, and software to protect IT infrastructure and data assets.
- Managed the implementation of security technologies.
- Briefed senior leadership on security threats and recommended mitigation strategies.
- Involved in establishing the strategic direction for and in providing the operational management of an IT service organization.

The Division of Information Services (IS) is responsible for the strategy, planning, and delivery of information technology across all eight Kent State University campuses and their respective satellite locations. Four groups comprise IS and include: IT Enterprise Applications and Infrastructure Services and Support (EAI), Systems Development and Innovations, Educational Technology and Service Management and IS Finance and Business Operations. Specifically IS is responsible for:

- Designing, installing, and maintaining core computing and communications infrastructure, ensuring secure access to enterprise systems and the university network;
- Designing and developing innovative software applications, such as FlashLine and KSUMobile, that connect our students, faculty, and staff to the information they need;
- Managing hardware and software purchasing, installation and configuration to support teaching, learning, and research;
- Providing end user services to assist with their use of technology; and
- Managing and supporting the university's learning management system and other applications for teaching and learning

The Division is partnering with the campus to implement a new strategic direction for the IS organization and University technology. Hallmarks of this new direction are a services-based organization structure and culture and emphasizing data and the user experience as foundational to all services and strategies. Priority initiatives focus on improving IT governance processes, expanding research computing services, improving IT operations and services, and deploying new constituent relationship management and mobile strategies. To learn more about our division please visit the IS web site.

About Kent State

Kent State University is one of 76 public higher-research universities, as categorized by the Carnegie Foundation for the Advancement of Teaching, and is ranked in the first-tier list of Best National Universities by U.S. News & World Report. With eight campuses spanning Northeast Ohio, a College of Podiatric Medicine, a Regional Academic Center, and academic sites in major world capitals such as New York City, Geneva and Florence, Kent State is one of Ohio's leading public universities and a major educational, economic and cultural resource far beyond the Northeast Ohio region it has served since 1910.

The University is powered by a vision that our collaborative community created together. That vision, *A Strategic Roadmap to a Distinctive Kent State*, introduces goals and strategies to increase student success, accentuate the University's distinctiveness, position the University to succeed in a globally competitive environment, increase its impact on regional development and improve stewardship of institutional resources. Please visit our web site to learn more about Kent State's strategic roadmap, mission, vision, values and plans.

To Apply visit https://www.kent.edu/hr/job-opportunities

Kent State is an equal opportunity, affirmative action employer, and is committed to providing employment opportunities to all qualified applicants without regard to race, color, religion, age, sex, sexual orientation, gender identity, national origin, disability or protected veteran status.