PRINCETON UNIVERSITY

Boyden Executive Search Contact

Lisa Vuona | 508.320.6445| lvuona@boyden.com

Sara Swisher-Anderson | 917.566.5881 | sswisher@boyden.com

Position Summary

The Chief Information Security Officer (CISO) at Princeton is responsible for developing, expanding and maturing the University information security policy and strategy and draws on domain expertise, a capacity for vision and change management and communication skills to establish a high level of understanding of and attention to information security in a world-class institution of teaching, learning and research.

The CISO works collaboratively with University leadership and departmental technical and administrative staff throughout campus. The CISO develops and leads outreach, communication and education efforts to raise campus-wide awareness of information security risk, requirements and solutions; provides strategic and technical guidance and assistance in the design and implementation of appropriate security processes for campus-wide information systems; directs the University IT Risk Assessment process; recommends and monitors computing practices to prevent and recover from security breaches and handles breaches when they occur; provides vision, leadership and development of robust security operations and vulnerability management; and leads the operations and success of access security requirements.

The CISO reports to the Vice President for Information Technology and Chief Information Officer and collaborates with OIT senior staff and key campus business and IT leaders to shape security and business-continuity standards and action plans. The CISO plays a leadership role in the implementation of security practices and policies through collaboration with technical staff. The CISO also plays a key role in preparing and presenting strategic updates and recommendations to the University's Board of Trustees, ensuring transparency, accountability, and informed decision-making at the highest level of governance. The CISO has dotted line responsibilities to the VP and Dean for Research, and is designated as the University Research Security Officer for federal grants and projects.

Responsibilities

Strategic Planning and Policy Development

- Provides guidance and counsel on information security to the CIO, the University's Board of Trustees, University Cabinet members, OIT senior staff and senior level University stakeholders.
- Works with campus leadership to develop a strategy for information security that balances Princeton's academic values with institutional attention to the risks and requirements generated by the University's increasingly information-rich environment and external regulations.
- Recommends strategies and practices to ensure information security and leads the design, development and implementation of the University's security and data-governance policies and procedures in consultation with University leadership, OIT and campus technical staff and IT advisory bodies.
- Represents the University in assessing and approving research security needs and establishes and maintains a strong partnership with Research Protections and Administration, and the Research Integrity Office.
- Advises University leaders on emerging information security risks and opportunities created by Princeton's role as a world-class institution of teaching, learning and research with increasing global relationships and activities.

- Tracks industry and higher-ed information security best practices to keep abreast of current techniques, systems and applications.
- Assumes responsibility for information-security policies and effective IT risk management and compliance across the University; coordinates campus-wide data governance and security initiatives.
- As a member of the CIO leadership team, contributes to the overall development of OIT's strategic goals, performance metrics, communication practices and culture.

Management

- Leads the overall management and success of a robust, current and expanding information security office.
- Leads an annual IT Risk Assessment process and maintains the efficacy of an IT Business Continuity Plan.
- Maintains a close relationship with the offices of General Counsel, Audit and Compliance and Public Safety; serves as liaison between these groups and IT professionals for matters pertaining to campus IT security.
- Assesses hardware/software/services being considered for purchase or implementation for security strengths/risks and information security features; provides security requirements for software/services RFPs.

Training and Outreach

- Develops and leads education and training programs on institutional policy, guidelines, federal and state laws and regulations and best practices around information security.

Job Qualifications

Essential Qualifications

- At least 10 years of current experience directly related to the responsibilities of the role Demonstrated domain expertise.
- A strategic grasp of information security at both institutional and operational levels.
- The capacity to articulate a vision for information security that engages all constituents, satisfies internal and external requirements, and enables Princeton's ongoing pursuit of excellence and innovation in its academic and research fields.
- Communication and collaboration skills to build support for security-related initiatives and objectives.
- Experience in higher education or a research environment is preferred.
- Broad knowledge of computer security issues, requirements, and trends.
- Exceptional interpersonal and communication skills, plus the ability to achieve goals through influence, collaboration and cooperation.
- Demonstrated ability to work effectively with an array of constituencies in a community that is both demographically and technologically diverse.
- Skill in developing policy and procedure in a complex, decentralized, and mission-oriented environment that maintains in a department-based model of resource allocation and deployment.
- Experience providing education and training programs on security policies and practices to a range of technical and non-technical constituents.
- The ability to establish, implement, maintain, and modify computer and data security guidelines and procedures to achieve the compliance objectives of an organization in harmony with the principles of academic freedom that remain core to a world-class university.
- The ability to evaluate security software products, oversee their installation and implementation, and interpret findings for practical use by law enforcement, legal counsel, and senior management as applicable.
- Experience evaluating and providing guidance on the information-security elements of software and hardware acquisitions, IT services, cloud-based solutions, mobility, and other present and emerging dimensions of IT solutions and services in a complex environment Integrity and high standards of personal and professional conduct.

- Education: Bachelor's degree required, preferably in computer science or information technology; Graduate degree preferred in computer science or related field, or equivalent experience and relevant professional credentials.

Preferred Qualifications

- Graduate degree in computer science or related field, or equivalent experience and relevant professional credentials.

Boyden Contacts

Lisa Vuona
Managing Partner
lvuona@boyden.com
M +1 508.320.6445

Sara Swisher-Anderson
Principal
sswisher@boyden.com
M +1 917.566.5881

About Boyden

Founded in 1946, Boyden global executive search was the first firm to focus entirely on retained executive search. Others would soon follow, using many of the basic tenets and principles that Sidney Boyden put in place: maintaining a strict code of ethics and standards; establishing a global presence; creating uniform processes; and working with highly experienced business partners. These aspects of Sidney Boyden's vision are still in use today.

Boyden continues to be a leader in the executive search industry. Through the ever-expanding use of cutting-edge technology, while always adhering to strict ethical standards, we remain true to our rich heritage as the founders of retained executive search. We cover the globe with over 70 offices in more than 40 countries, led by resident professionals adept at working in a global economy. We are poised to help our clients find the people who will lead them today and into the future. In addition to retained executive search, Boyden works with clients seeking advice regarding their Boards. We also assist clients with interim management and leadership assessment.