



Chief Information Security Officer

6.3.26

[The University of Virginia](#) (UVA), one of the nation's leading public institutions, seeks an experienced, dynamic, and mission-driven leader to be the next Chief Information Security Officer (CISO). Reporting to the Vice President and Chief Information Officer (CIO), the CISO will provide strategic leadership and oversight to a diverse portfolio. They will lead high-performing teams and work collaboratively across a large, complex institution.

The CISO must enjoy engaging with the University community, drawing on strong communication skills, a natural ability to build relationships, and comfort explaining complex technical concepts to faculty and staff at all levels. The complexity of this position requires strong leadership, collaboration and partnership skills, and the ability to balance the urgency surrounding the risk of emerging threats with university strategies and business needs.

Position Summary

As a critical member of the [Information Technology Services \(ITS\)](#) leadership team, this pivotal role is responsible for establishing and maintaining a university-wide information security management program to ensure that the university's data and assets are adequately protected. The CISO must stay current with the evolving threat landscape (particularly involving AI-based threats), ensure staff are upskilling to keep pace, and challenging the status quo to ensure the University maximizes its investment in its information security resources. The candidate will work closely with IT leadership, administrative leaders, and academic faculties across Grounds to identify, evaluate, and report on information security risks in a manner that meets compliance and regulatory requirements and aligns with and supports the risk posture of the University.

The ideal candidate is:

- Curious — Asks thoughtful questions, listens actively, and seeks understanding before taking action.
- Entrepreneurial — Embraces new ideas, explores innovative solutions, and remains open to different approaches.
- Resourceful — Identifies practical solutions, navigates constraints effectively, and remains focused despite obstacles.
- Collaborative — Builds strong relationships, values consultation, and engages stakeholders in developing solutions.
- Adaptable — Questions existing processes constructively and adjusts effectively as priorities and circumstances evolve.
- User-Centered — Considers the impact of security practices and technologies on users' ability to work effectively and achieve their goals.
- Growth-Oriented — Fosters a culture of continuous learning, encourages skill development, and helps teams embrace new approaches as needs change.

Key Responsibilities

Program Leadership

- Establish and maintain/refine the strategic direction of the university's information security program. Work closely with IT leaders internal and external to ITS, including senior administration, academic leaders, and the university community in defining objectives and priorities for information security while building relationships and goodwill.
- Establish a durable and integrated partnership between central security, distributed IT, and academic technology units that enables shared ownership of institutional cyber risk. Lead security planning as a joint enterprise - co-developing an inclusive, comprehensive cybersecurity program that is embedded within academic, research, and administrative operations. Align strategies, capabilities, and governance across the distributed environment to ensure security is not implemented onto the institution but operated as part of it.
- Define security strategies, metrics, reporting mechanisms and program services, and create maturity models and a roadmap for continual program improvements. Identify and execute on opportunities for process improvements and automation, challenging the status quo to create service improvements and reduce barriers to participation.
- Systematically assess AI and machine learning-based tools and capabilities across the full information security lifecycle, from threat detection to incident response, applying appropriate evaluation criteria, executing POCs and pilots, generating resource investment recommendations (including training programs), and developing implementation plans in collaboration with relevant ITS teams.
- Continually evaluate emerging threats, tool sets, team processes, and relevant industry information security frameworks for best practices, and design and operate an institutional process to identify, ingest, triage, and track risks across academic and administrative units. 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 regularly with ITS and other units on risk posture and emerging concerns. Engage in professional development to maintain continual growth in professional skills, maintenance of certifications, and knowledge essential to the position.
- Serve as a standing member of IT and institutional governance bodies, with responsibility for recurring reporting on the status of the information security program and continuous assessment of the university's risk posture. Ensure leadership, including University Executives and the Board of Visitors, maintains an integrated understanding of cybersecurity conditions, emerging threats, and institutional resilience.

Team Leadership

- Manage the university's academic information security organization, including hiring, training, staff development, performance management, and performance reviews.
- Partner closely with UVA Health technology leadership to create opportunities for productive cross-agency collaboration that balances security requirements against their impact on users' ability to get work done efficiently.

- Continuously evaluate the team's capabilities (including strengths and opportunities for improvement), identify training needs, and set performance goals that collectively promote growth and position the team to best respond to new and emerging threats.
- Create a team environment where staff are encouraged to challenge conventional thinking and strive for continuous improvement.

Policy, Compliance and Audit

- Develop, maintain, and publish up-to-date information security policies, standards, and guidelines and ensure information security and compliance with relevant legislation and legal interpretation. Oversee the approval, training on, and dissemination of security policies and practices.
- Proactively engage in understanding and positioning the university to respond to new/changing regulatory and compliance requirements covering areas such as AI and research security (e.g., NSPM-33, CMMC, etc.), as well as addressing requirements for PCI, ITAR, HIPAA, GDPR, etc.
- Continually assess and evaluate the adequacy of security controls across the institution, working in partnership with academic and administrative leadership to address deficiencies within their units, and with ITS leadership to remediate gaps in centrally managed services.
- Work directly with the schools/units and with auditors and outside consultants as appropriate on required security assessments and audits. Keep audit focus in scope, maintain excellent relationships with audit entities, and provide guidance, evaluation, and advocacy on audit responses.

Community and Partner Engagement

- Oversee the security awareness education program and engage directly with the schools/units to review security metrics, consult on priorities and information security work plans, and identify needed training for local service providers to maximize their effectiveness in enforcing/supporting security policies and standards at the local level.
- Develop and maintain external relationships with federal and local law enforcement when needed.

Risk Management, Security Operations, Projects, and Incident Response

- Provide leadership, direction, and guidance in identifying, evaluating, and prioritizing information security risks and monitor compliance with security standards and appropriate policies.
- Manage the daily IT security operations, disseminating information to the schools/units as appropriate. Oversee the management of the IT security operations team, inclusive of managed detection and response services, while working collaboratively with other members of ITS and administrative and academic IT staff to enact needed controls.
- Conduct a continuous assessment of current IT security operations practices and identify areas for improvement. Create and maintain the roadmap to track plans and progress.
- Coordinate information security projects with resources from the IT organization and business unit teams.
- Manage security incidents and events to protect IT assets, including intellectual property, highly sensitive/sensitive/non-public data, networks, and the university's reputation. Oversee the

investigation of reported security incidents. Maintain and regularly test/update the university's information security incident response plan.

Competencies and Qualifications

- A bachelor's degree in Information Technology, Computer Science, Information Systems, or a related field (advanced degree preferred).
- Professional security management certification is strongly desired, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), or other similar credentials.
- At least 10 years of experience in a combination of risk management, information security, and IT jobs (at least five must be in a senior leadership role).
- Knowledge of common information security management frameworks, such as ISO/IEC 27001, and NIST 800-53, 800-174, and Cybersecurity Framework (CSF).
- Familiarity with AI and machine learning-based tools used across the information security lifecycle.
- Experience with contract and vendor negotiations and management, including managed services.
- Experience with Cloud Computing/IaaS/PaaS/SaaS technologies and services.
- Strong understanding of the higher education sector's policy, regulatory, and legislative environment is preferred.
- Excellent written and verbal communication skills, interpersonal, relationship-building, and collaborative skills, and the ability to communicate security and risk-related concepts to technical and nontechnical audiences at all levels.

The CISO role is based in Charlottesville, VA, with an expectation of strong in-person presence to effectively engage with leadership and stakeholders. A hybrid work model is available, with flexibility to work remotely when appropriate and consistent with the needs of the organization.

To Apply

The University of Virginia has retained [Opus Partners](#) to support this recruitment. [Katie Dean](#), Senior Partner, and [Abigail Maynard](#), Managing Associate, are leading the search. Applications (resume and letter of interest), confidential inquiries, and nominations should be sent to Abigail Maynard at abigail.maynard@opuspartners.net.

University of Virginia

The University of Virginia (UVA) ranks as one of the leading Universities in the nation. A vibrant and student-centric institution, UVA is animated by the forward-looking spirit of its founder, Thomas Jefferson. In 2026, the University was ranked as the fourth best public university by U.S. News & World Report. In the 20 plus years since U.S. News began ranking public universities as a separate category, UVA has been in the top five, and it has consistently ranked in the Top 30 among the best of all national universities, public and private. UVA remains one of the only public universities to meet 100% of every undergraduate student's financial need and offers admission to students with no consideration of a family's income.

UVA brings together a diverse global community of approximately 25,000 students, hailing from virtually every state in the nation and 111 countries. UVA encompasses twelve schools in Charlottesville, as well as the College at Wise, a small, liberal-arts college in Southwest Virginia, and its newest campus in Northern Virginia. In Charlottesville, the University employs nearly 30,000 people, including approximately 16,000 faculty and staff and approximately 12,000 UVA Health employees.

The University has developed an exceptionally strong financial foundation and a consensus triple-A bond rating. The three major rating agencies have noted the University's excellent reputation; student demand, highly selective admissions, and broad geographic reach; sponsored research prowess; superior wealth and liquidity management; exceptional strategic positioning supported by strong planning, risk management, and ongoing prospects to support programmatic investments; the Medical Center's prominent clinical reputation and ability to compete for patient care revenue; and remarkable donor support, among other factors. In recent years, UVA has transformed significant parts of its operations (HR and Finance) and implemented new cloud-based systems that will enable best-in-class analysis, services, and support in a rapidly changing environment.

Research

A Carnegie Research 1 university, UVA has strong partnerships with leading federal and state agencies and some of the world's largest companies across a wide range of industries. In FY25, sponsored research awards total \$570 million from all sources, including federal and state agencies, industry, and private foundations. In FY24, UVA researchers made 146 invention disclosures, with 56 patents issued. UVA's Licensing and Ventures Group helps bring innovative companies and products to market, making Charlottesville one of the most vibrant venture capital markets in the country. UVA has a large research park located near the Charlottesville airport.

The University identifies five priority focus areas for research: Democracy, Environmental Resilience and Sustainability, Precision Medicine/Health, the Brain and Neuroscience, and Digital Technology and Society. The Grand Challenges Research program is intended to make a substantial difference through large strategic investments in these areas—to move the needle and not just fund business as usual. We plan to focus on opportunities that will have high impact, such as significant research infrastructure or new faculty (cluster hires or key leaders). We do not plan to support routine research expenses or replace externally sponsored research funding. This transformative new investment is designed to expand and complement our current research portfolio. In fact, the Research Computing team within Information Technology was the recipient of one of these awards, which is focused on building out a Data Analytics Center in support of researchers at UVA.

UVA Health

UVA Health is an academic health system that strives to provide excellence, innovation, and exceptional quality in the care of patients, the training of health professionals, and the creation and sharing of knowledge within a culture that promotes equity, diversity, and inclusivity. UVA Health is an expansive network comprising the UVA Medical Center, Novant Health / UVA Health System, UVA Transitional Care Hospital, University of Virginia Physicians Group, UVA School of Medicine, UVA School of Nursing, Claude Moore Health Sciences Library, and several other strategic partnerships and alliances.

UVA Health prides itself on providing exemplary clinical care to patients from across the Commonwealth of Virginia and the surrounding region. The UVA Medical Center has received national accolades for outstanding clinical services in several disciplines, including oncology, cardiovascular, and women and children's services. The Medical Center includes the flagship 696-bed Magnet® recognized University Hospital located in Charlottesville, Virginia, which houses a Level I trauma center, the UVA Children's Hospital, the Emily Couric Clinical Cancer Center, the Charles Strickler Transplant Center, and more than 100 primary and specialty care clinics throughout Virginia. Physicians who work at UVA Medical Center are faculty in the School of Medicine's 21 clinical departments and are also employed by the UVA Physicians Group. UVA Health's commitment to patient care and employee wellbeing is reflected in a comprehensive values system. At UVA Health, faculty and staff ASPIRE to embody UVA's values of Accountability, Stewardship, Professionalism, Integrity, Respect, and Excellence. UVA Health aims to create a safe, inclusive, and compassionate environment for faculty, staff, and patients. UVA Health is supported by its own technology leadership, including a Chief Information Officer (CIO) and Chief Information Security Officer (CISO) who are dedicated to the protection of patient and UVA Health data.

Charlottesville

Located in the heart of Central Virginia at the foothills of the Blue Ridge Mountains, and just 100 miles south of Washington, D.C., Charlottesville offers an exceptional quality of life that blends natural beauty, rich history, cultural vibrancy, and professional opportunity. Home to the University of Virginia, the city is consistently recognized as one of the best places to live in the United States for its strong sense of community, intellectual energy, and outstanding amenities.

In the span of a single day, residents can hike portions of the Appalachian Trail, attend a concert or sporting event, enjoy award-winning cuisine at one of Charlottesville's many celebrated restaurants, stroll the historic Downtown Mall, or explore iconic destinations such as Monticello, the Fralin Museum of Art, and the Jefferson School African American Heritage Center. The surrounding region also features scenic outdoor destinations and world-class wineries, breweries, and distilleries that make Central Virginia one of the most beautiful regions on the East Coast.

Whether you are seeking a dynamic professional environment, a family-friendly community, access to outdoor recreation, or a vibrant arts and culinary scene, Charlottesville offers the livability and warmth of a small city with the amenities and cultural experiences of a much larger metropolitan area. For more information, go to: [Visit Charlottesville](#).

The University of Virginia is an equal opportunity employer. All interested persons are encouraged to apply, including veterans and individuals with disabilities. Learn more about [UVA's commitment to non-discrimination and equal opportunity employment](#).