APPALACHIAN STATE UNIVERSITY
Chief Information Security Officer

The Chief Information Security Officer (CISO) reports to the Chief Information Officer, is a member of the CIO leadership team and serves a key role in university leadership, working closely with senior administration, academic leaders, and the campus community. The CISO is an advocate for Appalachian State University's total information security needs and is responsible for the development and delivery of a comprehensive information security strategy to optimize the security posture of the university. 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.

Duties and Responsibilities

University and Program Leadership

- Responsible for the strategic leadership of the University's information security program.
- Provide guidance and counsel to the CIO and key members of the university leadership team, working closely with senior administration, academic leaders, and the campus community in defining objectives for information security, while building relationships and goodwill.
- Work with campus leadership to oversee the formation and operations of university-wide information security resources organized toward a common cause in information security. Promote collaborative, empowered working environments across campus, removing barriers and realizing possibilities.
- Manage institution-wide information security governance processes, including formation of an Information Security Advisory Committee and development of a department liaison program, to support campus-wide information security program and project priorities.
- Lead information security planning processes to establish an inclusive and comprehensive information security program for the entire institution in support of academic, research, and administrative information systems and technology. 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. Engage in professional development to maintain continual growth in professional skills and knowledge essential to the position.
- Provide leadership philosophy for the Information Security Team 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. Mentor the Information Security Team members and implement professional development plans for all members of the team.

- Represent the university on committees and boards associated with the University of North Carolina and in national and regional consortiums and collaborations.
- Perform special projects and other duties as assigned.

Policy, Compliance and Audit

- Lead the development and implementation of effective and reasonable policies and practices to secure protected and sensitive data and ensure information security and compliance with relevant legislation and legal interpretation.
- Lead efforts to internally assess, evaluate and make recommendations to administration regarding the adequacy of the security controls for the University's information and technology systems.
- Work with Internal Audit, Institutional Research Board, University of North Carolina General Administration, State Auditor's Office, Office of the State Chief Information Officer and outside consultants as appropriate on required security assessments and audits. Responsible for coordinating and tracking 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.
- Work with university leadership, General Counsel and relevant responsible compliance department leadership to build cohesive security and compliance programs for the university to effectively address state and federal statutory and regulatory requirements. Develop a strategy for cohesively dealing with audits, compliance checks and external assessment processes for internal / external auditors, PCI, ITAR, HIPAA, FISMA and other applicable standards.

Outreach, Education and Training

- Work closely with IT leaders, technical experts and college and other administrative leaders across campus on a wide variety of security issues that require an in-depth understanding of the IT environment in their units, as well as the research landscape and federal regulations that pertain to their unit's research areas.
- Create education and awareness programs and advise operating units at all levels on security issues, best practices, and vulnerabilities.
- Work with campus groups such as Information Technology Services, ASU Technology Group, department liaisons and technical organizations in Business Affairs, Academic Affairs, University Advancement and Student Development to build awareness and a sense of common purpose around security.
- Pursue student security initiatives to address unique needs in protecting identity theft, mobile social media security and online reputation program.

Risk Management and Incident Response

- Keep abreast of security incidents and act as primary control point during significant information security incidents. Convene a Security Incident Response Team (SIRT) as needed, or requested, in addressing and investigating security incidents.
- Convene Security Committee consisting of General Counsel, University Communications, CIO, Vice Chancellors and relevant department administrators as appropriate and provide leadership for breach response and notification actions for the University.
- Develop, implement and administer technical security standards, as well as a suite of security services and tools to address and mitigate security risk.
- Provide leadership, direction and guidance in assessing and evaluating information security risks and monitor compliance with security standards and appropriate policies.
- Examine impacts of new technologies on Appalachian State University's overall information security. Establish processes to review implementation of new technologies to ensure security compliance.

Required and Preferred Qualifications

The emphasis of this position is on leadership and judgment, with a sophisticated ability to work with other leaders and to set the best balance between security strategies and other priorities at the campus level. Experience as an Information Security Officer, developing and administering an information security program in a complex higher education environment is highly desirable.

A bachelor's degree in Management Information Science or other related field is required; an advanced degree is preferred.

The position requires an intelligent, articulate, consensus building, and persuasive leader who can work effectively with senior administration, academic leaders, and the campus community and communicate information security-related concepts to a broad range of technical and non-technical staff.

Demonstrated experience advising and collaborating with senior management is required. The ability to work in a team/collaborative environment with a broad range of constituencies is essential.

Success in this position depends on ability to work in a highly decentralized environment, without reliance on line authority. For this reason, excellent communication and social skills are required.

Ability to exhibit maturity, reliability, composure, and stability under pressure as required for handling on-the-job challenges is essential. Must be able to give and take constructive criticism well and be gracious and slow to anger.

Demonstrated success in working with Internal Audit, System Auditors, outside consultants and/or Office of the State Auditor in a lead capacity to coordinate representation of institutional technology systems and practices is highly desired.

Professional certification (e.g., CISSP) is highly desirable. Candidates lacking such certification may be competitive if they present comparable credentials or involvement in continuous professional development.

Significant experience in computing and information security, network security issues, and security incident response and recovery in a higher education environment is highly desirable.

Working knowledge and experience in the policy and regulatory environment of information security, particularly in higher education, is highly desirable.

A security and criminal background check, and verification of eligibility for employment, will be required prior to hire.