CISO Job Description Template

Last reviewed: March 2017

Recommendations if you are developing a job announcement or description for your institution:

1. Review the *sample* CISO job description (below). Previous job postings from Princeton University and University of Albany are also available (in PDF format).
2. Review the National Cybersecurity Workforce Framework published by NIST, which includes *sample job titles* and *key tasks*.
3. Review the 2016 IT Workforce in Higher Education research hub for the most recent EDUCAUSE research on the evolving IT workforce needed to support contemporary models of IT service delivery.
4. Consider alternative solutions, such as Bucknell University, Franklin & Marshall College, and Susquehanna University collaborating to create a joint CISO position among the three institutions. A non-higher ed example is Howard County, Maryland's HOCO CISO program , which provides "virtual" CISOs.
5. For potential locations to post IT or information security job openings, visit the Career and Workforce Development chapter.

Examples of current or archived higher ed CISO job postings:

- CISO, University of Edinburgh, Scotland
- CISO, Appalachian State University (archived)
- CISO, University of Oregon (archived)
- CISO, University of Virginia (archived)

Also consider searching the Security Discussion Group or CIO Discussion Group listserv archives.

Policies Defining CIO and CISO Responsibilities

- Appalachian State University Information Security Policy (*refer to section on roles and responsibilities*)
- Virginia Tech IT Security and Authority Resolution (*affirms the authority of the CIO*) and University Policy 7010 (*delegates authority from the CIO to the ISO*)

CISO Job Description Template

Institution Name

Title (e.g., Information Security Officer, Chief Information Security Officer, Director of Information Security, Manager of Information Security)

Institution's Job or Reference #

The **Institution** seeks an experienced, energetic, engaging and visionary leader who wants to become part of an exciting, vibrant community of information technology professionals supporting the **institution's** mission: providing a comprehensive, high-quality education that engages students in discovery through research and broad-based scholarship.

Information technology plays a vital and ever-expanding role in the institutional mission. The **Institution's** information technology environment is highly distributed and diverse, with strong leadership and coordination from Chief Information Officer (CIO) and direct report units. We are seeking a strong, knowledgeable leader to provide vision, strategy, broad-based planning, and hands-on responsibility as the University Information Security Officer (UISO).

The UISO reports to the CIO, 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 UISO is an advocate for the **Institution'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 UISO 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 a university-wide information security organization that is organized toward a common goal in information security.
- Promote collaborative, empowered working environments across campus, removing barriers and realizing possibilities.
- 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.
- 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 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.
- Mentor the Information Security Office team members and implement professional development plans for all members of the team.
- Represent the university on committees and boards associated with the **Institution's** System 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 management regarding the adequacy of the security controls for the University's information and technology systems.
- Work with Internal Audit, State Board of Regents, Auditor General's Office and outside consultants as appropriate on required security assessments and audits.
- 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.
- Work with university leadership 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 dealing with increasing number of audits, compliance checks and external assessment processes for internal/external auditors, PCI, ITAR, HIPAA, and FISMA.

Outreach, Education and Training

- Work closely with IT leaders, technical experts, deans and 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 Network Managers, Information Security Liaisons and technical organizations such as University Information Technology Services 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 incidences that arise.
- Convene Ad Hoc Security Committee 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 the **Institution's** overall information security. Establish processes to review implementation of new technologies to ensure security compliance.

For complete details and to apply, please visit: ***Institution's URL***

*PLEASE NOTE: In order to receive proper consideration, applications must be submitted directly via the **Institution's** career site. Applications submitted via any other source will not be considered.*

The **Institution** is an EEO/AA: M/W/D/V (Equal Opportunity/Affirmative Action Employer: Male/Female/Disabled/Veteran) Employer.

Questions or comments? Contact us.

Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).