University at Albany
Office of the Chief Information Officer (CIO)

Job Description

DEPARTMENT: Office of the CIO
BUDGET TITLE: Senior Staff Associate
CAMPUS TITLE: Information Security Officer (ISO)

POSITION RELATIONSHIPS:

Reports to:	Chief Information Officer
Works with:	IT Unit Directors and staff, Office of Counsel, Internal Audit, University Police Department, Judicial Affairs, policy and governance groups, Deans and Directors
External Relationships:	SUNY, Educause, NYS Office of Cyber Security, IT suppliers/vendors, law enforcement

POSITION SUMMARY:

Under the general direction of the CIO, the Information Security Officer (ISO) is responsible for the development and delivery of a comprehensive information security and privacy program for the University at Albany UA). The scope of this program is university-wide, and includes information in electronic, print and other formats. The purposes of this program include: to assure that information created, acquired or maintained by UA, and its authorized users, is used in accordance with its intended purpose; to protect UA information and its infrastructure from external or internal threats; and to assure that UA complies with statutory and regulatory requirements regarding information access, security and privacy.

POSITION DUTIES, RESPONSIBILITIES AND COMPETENCIES

Policy
Coordinate the development of UA information security policies, standards and procedures. Work with key IT offices, data custodians and governance groups in the development of such policies. Ensure that university policies support compliance with external requirements. Oversee the dissemination of policies, standards and procedures to the university community.

Education and Training
Coordinate the development and delivery of an education and training program on information security and privacy matters for employees, other authorized users, and students.

Compliance and Enforcement
Serve as the university compliance officer with respect to UAlbany, state and federal information security policies and regulations[1]. Work with the campus-designated FERPA, Records Access and HIPAA-privacy Officers on compliance issues as necessary. Prepare and submit required reports to external agencies.

Incident Response
Develop and implement an Incident Reporting and Response System to address UAlbany security incidents (breaches), respond to alleged policy violations, or complaints from external parties. Serve as the official campus contact point for information security, privacy and copyright infringement incidents, including relationships with law enforcement entities.

Risk Assessment and Incident Prevention
Develop and implement an ongoing risk assessment program targeting information security and privacy matters; recommend methods for vulnerability detection and remediation, and oversee vulnerability testing.

Official Contact
Act as the CIO's designee representing UA on Information Security matters; serve as the campus contact point for external auditors and agencies, survey requests, etc on security/privacy matters.

Maintain Knowledgebase
Keep abreast of latest security and privacy legislation, regulations, advisories, alerts and vulnerabilities pertaining to the UA and its mission.

Emergency Preparedness
Take part in Campus Recovery Planning.

QUALIFICATIONS:

The emphasis of this position is on policy development, program administration and compliance/incident response activities. While technical knowledge of information technology and security issues is highly desirable, technical expertise and resources will be available from units such as Systems Management & Operations, and the Office of Telecommunications to support the information security and privacy program.

Education: Bachelors degree required. Advanced degree preferred.

Experience: Minimum seven years of experience in information security, information technology or related field. Experience in developing and administering an information security program desirable. Working knowledge of and experience in the policy and

[1] For example, FERPA, HIPAA, Gramm-Leach-Bliley, DMCA, NYS Cyber Security Policy, USA Patriot Act, et al.

regulatory environment of information security, especially in higher education is desirable. Excellent project management, written and oral communications skills desired. Ability to work collaboratively with a broad range of constituencies essential. A demonstrated ability to work with diverse groups of people is required.