

Notice of Job Opening

Position: Information Security Officer

Applicants must meet the requirements outlined in the enclosed job description.

The City of Albany's Department of Administrative Services is seeking a highly skilled and proactive **Information Security professional** to join our team. In this role, you'll be instrumental in shaping and maintaining our enterprise security vision, strategy, and programs, directly contributing to the protection of our information assets and technologies. You'll develop and manage security policies, assess organizational risks, guide third-party security practices, and lead the charge in formalizing asset management and incident response. This position demands strong leadership, exceptional communication, and the ability to collaborate across departments to ensure our security function consistently adds value to the business.

PLEASE NOTE: This position is in the competitive class and will be filled on a provisional basis pending the outcome of the civil service examination.

Department: Information Technology

Vacancies to be filled: 1

Rate of Pay: \$68,670 – \$98,280 Annually
Commensurate with qualifications and experience

Schedule: 37.5 hours/week

Application Deadline: **Until Filled**
All applicants must submit an application online via jobs.albanyny.gov to be considered for the job opening.

Residency Preference: Preference in hiring is given to qualified City of Albany residents. All candidates must reside in the following counties at the time of appointment and throughout their employment. Proof of residency will be required at time of appointment.

- Albany County
- Rensselaer County
- Schenectady County

The City of Albany is an Equal Opportunity /Affirmative Action Employer.

Reposted on Friday, November 14th, 2025



Mayor
Kathy M. Sheehan

Office of Human Resources
Tatiana Diaz, Director

Albany City Hall
24 Eagle Street, Rm 301
(p) 518-434-5049
(f) 518-434-5269

- Saratoga County
- Greene County
- Columbia County
- Schoharie County

The City of Albany is an Equal Opportunity /Affirmative Action Employer.

Reposted on Friday, November 14th, 2025

INFORMATION SECURITY OFFICER

DISTINGUISHING FEATURES OF THE CLASS: Under the general supervision of the Chief IT Officer or designee, the incumbent is responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are protected. Ensure that an organization's security function adds value to the business. Forge strong and secure connections between departments.

TYPICAL WORK ACTIVITIES: (Illustrative Only)

- Assist in the development and manage information and organizational security policies, standard and procedures to protect from internal and external threats and vulnerabilities;
- Provide methodology for assessing organizational and information risks, gap analysis based on current controls;
- Develop repeatable processes for risk tolerance, risk prioritization and mitigation;
- Guide Security practices with 3rd party providers such as cloud services, technology vendors, or any other services outsources to a 3rd party;
- Ensure 3rd parties are compliant with City of Albany Security Policies and Compliance Standards;
- Identify information assets and categorizes according to criticality and sensitivity;
- Formalize processes to catalog and maintain inventory of all software and hardware assets;
- Draft internal security training programs;
- Maintain training materials for employees and partners;
- Standardize subject access control to digital and physical assets, including data storage, applications and services, physical and network infrastructure;
- Provide management and support of infrastructure planning and acceptance, malware protection, cryptography, PKI, backup and recovery, network and media management;
- Assist departments in the secure development of new and existing systems;
- Assist in the development and implementation of plans to protect technology physical assets, including data centers and other controlled areas and controls for securing assets and equipment;
- Assist in the development of an incident management Lifecycle process that includes detection and analysis, containment, eradication and recovery, and post-incident activity;
- Collaborate with departments, assist in the development of a continuity plan, continuity of operations plan, and disaster recovery plan;
- Does related work as required.

FULL PERFORMANCE KNOWLEDGE, SKILLS, ABILITIES, AND PERSONAL CHARACTERISTICS:

- Knowledge of organizational management, public and business administration, and budgeting;
- Knowledge of the principles and methods of project management and contract management;
- Knowledge of sound financial and business practices as it relates to equipment and service acquisition, budgeting, funding, billing, and cost containment;
- Knowledge of how to develop partnership agreements;
- Excellent interpersonal, oral and written communication skills;
- Ability to develop partnership agreements;
- Ability to negotiate with vendors, contractors, and others;
- Ability to work effectively with elected officials, executive, management, administrative and technical staff;
- Ability to supervise the work of subordinate personnel;
- Ability to establish and maintain effective working relationships with others;
- Ability to plan, organize and supervise the work of a diverse and highly technical staff to meet organization-wide and departmental user needs for a wide variety of information and telecommunication needs;
- Ability to effectively communicate technical information in an easily understood manner;
- Ability to present ideas clearly and concisely, both orally and in writing;
- Strong leadership skills;
- Sound judgment; innovative; flexible; resourceful; initiative; tact;
- Physical condition commensurate with the requirements of the position.

MINIMUM QUALIFICATIONS: Either:

- A. Possession of a Bachelor's Degree (or higher) in Cyber Security of a related field and at least five (5) years of recent, IT security of multiple platforms, operating systems, software, and network protocols; OR
- B. Possession of an Associate's Degree in Cyber Security of a related field and at least seven (7) years of recent, IT security of multiple platforms, operating systems, software, and network protocols; OR

Note: Your degree must have been awarded by a college or university accredited by a regional, national, or specialized agency recognized as an accrediting agency by the U.S. Department of Education/U.S. Secretary of Education. If your degree was awarded by an educational institution outside the United States and its territories, you must provide independent verification of equivalency. A list of acceptable companies who provide this

service can be found on the Internet at <http://www.cs.ny.gov/jobseeker/degrees.cfm>. You must pay the required evaluation fee.

SPECIAL REQUIREMENT

This position may require an incumbent to work flexible hours including weekends.

Issued: 05/31/2025