

Wayne-Finger Lakes BOCES Vacancies

Salary range: \$85,000 - \$95,000 based on education and demonstrated abilities

Locations: 1 in LeRoy and 1 in Newark

Appointment will be made on a Provisional basis, with permanent appointment following successful qualification in a Civil Service Examination which will be scheduled at a later date.

INFORMATION SECURITY ANALYST

MINIMUM QUALIFICATIONS: EITHER:

1. Possession of a Bachelor's degree in information security, information systems, computer science, information resources management, information technology, or a closely related field, AND two (2) years of full-time paid work experience, or its part-time equivalent, in information technology security, which included, or was closely related to, two or more domains of information security: Security and Risk Management; Asset Security; Security Engineering; Communication and Network Security; Identity and Access Management; Security Assessment and Testing; Security Operations; or Software Development Security; OR
2. Possession of an Associate's degree in a field noted in (1) above AND four (4) years of full-time paid experience, or its part-time equivalent, as described in (1) above.

SPECIAL NOTE: EDUCATION: 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.

DISTINGUISHING FEATURES OF THE CLASS: The work involves the responsibility for assessing, testing, reporting and recommending remediation measures to protect an organization's information technology systems and data, including end-user networks and devices. The incumbent will ensure information security access management, processes and industry standards are followed and maintained. The incumbent will assist in identifying and troubleshooting issues relating to data and systems security. Employees in this classification may be tasked with assisting administration with internal investigations. Work is performed under the general supervision of higher-level department employee. While supervision is not a function of this title, guidance and instruction may be provided to other agency employees. Does related work as required.

TYPICAL WORK ACTIVITIES: (Illustrative only)

Reviews daily security appliances and system logs;
Audits and monitors both electronic and physical security of IT systems and networks;
Monitors system vulnerability, analyzes findings and identifies areas requiring remediation;
Assists in developing information security policies, procedures, standards and guidelines based on knowledge of best practices and compliance requirements;
Performs or coordinates security scanning or testing;
Assists with activities for providing back-up, recovery and business continuity;
Updates configuration and certification acceptance of data signatures;
Advises and assists with system performance and data related tuning;
Supports forensic and audit reviews to ensure compliance with established standards;
Prepares reports as needed;
Communicates results of daily internal system log analysis and review to appropriate staff.
Supports internal investigations by monitoring, retrieving data and reports relating to employees charged with misconduct.

INFORMATION SECURITY ANALYST

FULL PERFORMANCE KNOWLEDGE, SKILLS, ABILITIES AND PERSONAL CHARACTERISTICS:

Thorough knowledge of networking and operating systems; thorough knowledge of modern principles and practices of computer system security administration; thorough knowledge of accepted information technology practices with regard to data integrity and security; good knowledge of security events incident management (SEIM) platforms; good knowledge of security login platforms; ability to analyze systems requirements of a variety of applications; ability to implement and maintain computer security policies and procedures; ability to communicate effectively, both orally and in writing; ability to understand and interpret complex technical material; ability to prepare written material, especially system security documentation; ability to form and maintain effective working relationships; ability to work well with customers and service agencies; physical condition commensurate with the demands of the position.

APPROVED: APRIL 28, 2023

CIVIL SERVICE CLASSIFICATION: COMPETITIVE