CYBER SECURITY ADMINISTRATOR

DISTINGUISHING FEATURES OF THE CLASS: This is a high-level position responsible for protecting the information technology infrastructure of Ulster County. Responsibilities include providing ongoing facilitation, monitoring, and oversight of system security processes, evaluating operational and technical safeguards and protecting the confidentiality, integrity and availability of systems and the information therein. The incumbent also provides direction and leadership to all County departments through education and awareness programs and the implementation of security policies, standards, and processes. The work is performed under the general supervision of a higher-level employee with wide leeway allowed for the exercise of independent judgment in work details. Supervision of others is not normally a function of this position. Does related work as required.

TYPICAL WORK ACTIVITIES: The typical work activities listed below, while providing representative examples of the variety of work assignments in the title, do not describe any individual position. Incumbents in this title may perform some or all of the following, as well as other related activities not described.

Develops, coordinates, and recommends the implementation of countywide information security policies, standards, procedures and other control processes to safeguard electronically maintained information and systems to ensure ongoing security compliance;

Participates as a member of the security incident response team, evaluates security incidents, developing solutions and communicating results to management; participates in after-hours on-call incident management;

Participates in the development, implementation and maintenance of disaster recovery processes and techniques to assure continuity of business and security controls in the event of system unavailability;

Prepares technical specifications for hardware and software purchases for security applications; provides input regarding security for all information technology system procurement;

Assures security awareness through training programs and other education for all County employees and, where appropriate, third party individuals;

Works with other units and teams to maintain integrity and confidence in the performance of the County's technology defenses;

Performs vulnerability scans and penetration tests by developing and maintaining scripts, routines, and software to perform vulnerability threat assessments;

Monitors and reviews intrusion detection systems and firewall logs, analyzing events and patterns and coordinating mitigation responses; reviews firewall and router rules and access control lists; reviews and analyzes system logs and access lists;

Performs design review and analysis; performs threat and risk analysis; develops and evaluates plans, principles, and procedures for accomplishing customer security studies and provides professional analysis of methods and objectives;

Develops and analyzes information security models, maintaining methodology to track security plans for each sensitive and critical application and general support system within the organizations;

Responds to and assists in information security assessment requests; evaluates vendor products and services; advises management of risks and best security practices.

FULL PERFORMANCE KNOWLEDGES, SKILLS, ABILITIES AND PERSONAL CHARACTERISTICS: Thorough knowledge of standard security practices and procedures of developing and implementing an information security program; thorough knowledge of network protocols, encryption techniques, firewalls, virtual private networks, database structures, wireless communications and access security techniques; good knowledge of the current principles, practices, procedures, data privacy regulations, and compliance issues of information technology and governmental agencies; good knowledge of current threats and exploits including threat detection, analysis, and remediation; ability to perform cyber-attack trend analysis, systems analysis, evidence management, investigation coordination, and business continuity planning; ability to establish effective working relationships; ability to express oneself effectively, both orally and in writing; ability to prioritize and execute tasks in a high-pressure environment and make sound decisions in an emergency situation; ability to plan and problem-solve effectively.

MINIMUM QUALIFICATIONS: Either:

A. Possession of a Master's degree in Cyber Security, Computer Science, Information Technology, Computer/Network Security or closely related field and one (1) year of full-time paid or its part-time equivalent work experience in information technology and cyber security; **OR**

B. Possession of a Bachelor's degree in Cyber Security, Computer Science, Information Technology, Computer/Network Security or closely related field and three (3) years of full-time paid or its part-time equivalent work experience in information technology and cyber security; **OR**

C. Possession of an Associate's degree in Cyber Security, Computer Science, Information Technology, Computer/Network Security or closely related field and five (5) years of full-time paid or its part-time equivalent work experience in information technology and cyber security; **OR**

D. High School graduation or possession of a high school equivalency diploma and seven (7) years of full-time paid or its part-time equivalent work experience in information technology and cyber security; **OR**

E. An equivalent combination of education and experience as indicated in A, B, C and D above.

Note: Your degree or college credits must have been awarded or earned 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: Possession of a valid New York State driver's license or otherwise demonstrates their ability to meet the transportation needs of the job.

ULSTER COUNTY Adopted: March 20, 2024
2075 CYB SC ADM
Classification: Competitive
Grade: 19
Union: CSEA