CYBER SECURITY ADMINISTRATOR

DISTINGUISHING FEATURES OF THE CLASS

This is a high-level position responsible for protecting the information technology infrastructure of Dutchess 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 in them. 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. Supervision of others is not a normal function of this position.

TYPICAL WORK ACTIVITIES

Typical work activities for incumbents in this title include those listed below in addition to those work activities performed by lower level titles in this series. They are indicative of the level and types of activities performed by incumbents in this title. They are not meant to be all inclusive and do not preclude a supervisor from assigning activities not listed which could reasonably be expected to be performed by an employee in this title.

1. 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;
2. Participates as a member of the security incident response team, evaluates security incidents, developing solutions and communicating results to management; participate in after-hours on-call incident management.
3. 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;
4. Prepares technical specifications for hardware and software purchases for security applications; provides input regarding security for all information technology system procurement;
5. Assures security awareness through training programs and other education for all County employees and, where appropriate, third party individuals;
6. Works with other units and teams to maintain integrity and confidence in the performance of the County's technology defenses.
7. Performs vulnerability scans and penetration tests by developing and maintaining scripts, routines, and software to perform vulnerability threat assessments;
8. Monitors and reviews intrusion detection systems and firewall logs, analyzing events and patterns and coordinating mitigation responses; review firewall and router rules and access control lists; review and analyze system logs and access lists.
9. Performs design review and analysis; perform threat and risk analysis; develop and evaluate plans, principles, and procedures for accomplishing customer security studies and provide professional analysis of methods and objectives.
10. Develop and analyze information security models, maintaining methodology to track Security Plans for each sensitive and critical application and general support system within the organizations.
11. Respond to and assist in information security assessment requests; evaluate vendor products and services; advise management of risks and best security practices.

FULL PERFORMANCE KNOWLEDGES, SKILLS, ABILITIES AND PERSONAL CHARACTERISTICS

Knowledge of standard security practices and procedures of developing and implementing an information security program;

Knowledge of standard security practices, network architecture, routing, and TCP/IP protocols, Microsoft operating systems, project planning and management, use of third-party applications and native scripts and languages, risk assessment process and practices, general business processes and standards associated with areas of assignment;

FULL PERFORMANCE KNOWLEDGES, SKILLS, ABILITIES AND PERSONAL CHARACTERISTICS *(cont'd)*

Knowledge of the current principles, practice, procedures, data privacy regulations, and compliance issues of information technology and Governmental agency's;

Knowledge of current threats and exploits to include experience with threat detection, analysis, and remediation.

Knowledge of training methods in staff development;

Ability to perform cyber-attack trend analysis, conduct independent systems analysis of complex business processes, manage evidentiary process, maintain the chain-of-custody process and procedures, conduct investigations and coordinate security anomalies and events, business continuity planning, documentation and evaluation;

Ability to establish effective working relationships with clients, associates and official representatives;

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;

Personal characteristics necessary to perform the duties of the position;

Physical condition commensurate with the demands of the position.

MINIMUM QUALIFICATIONS

Graduation from high school or possession of a high school equivalency diploma AND:

EITHER:	(A)	Master's degree in Cyber Security, Computer Science, or Computer/Network Security AND one (1) year of full-time paid work experience in information technology and cyber security;
OR:	(B)	Bachelor's degree in Cyber Security, Computer Science, or Computer/Network Security AND three (3) years of full-time paid work experience in information technology and cyber security;
OR:	(C)	Associate's degree in Cyber Security, Computer Science, Computer/Network Security or a closely related field or a related field AND five (5) years of full-time paid work experience in information technology and cyber security;
OR:	(D)	An equivalent combination of education and experience as indicated in (A) and (B) above.

SPECIAL REQUIREMENT:

Eligible for Government Access Clearance.

Possession of a valid Driver License to operate a motor vehicle to operate a vehicle in New York State at time of application and to maintain appointment.

ADOPTED: 1/1/2019