DUTCHESS COUNTY CLASS SPECIFICATION		**CYBERSECURITY ANALYST**
DATE ADOPTED: 8/26/24	LAST REVISION:	Page 1 of 3

DISTINGUISHING FEATURES OF THE CLASS:

This is a highly specialized position responsible for protecting the digital and electronic information assets of Dutchess County. Responsibilities include ongoing analysis and monitoring of security information and event sources, working with other staff to implement cybersecurity policies, standards, and procedures, and working to protect the confidentiality, integrity, and availability of information assets. The incumbent also provides advice and direction to all County departments through education and awareness programs and the implementation of cybersecurity policies, standards, and procedures. Supervision of others is not a normal function of this position.

TYPICAL WORK ACTIVITIES:

The following is indicative of the level and types of activities performed by incumbents in this title. It is not meant to be all-inclusive and does not preclude a supervisor from assigning activities not listed that could reasonably be expected to be performed by an employee in this title.

1. Monitors logs and detection systems, and analyze events and patterns to identify potential vulnerabilities, threats, and cybersecurity incidents;
2. Monitors cyber intelligence sources for alerts and vulnerabilities that may impact County information assets, distribute notifications to proper parties, and coordinate with appropriate staff to implement vulnerability management;
3. Contributes to the development of county-wide or departmental policies, standards, and procedures related to the implementation of cybersecurity best practices;
4. Works with OCIS staff to develop cybersecurity models, and implement the models through the installation, configuration, and monitoring of security tools and procedures;
5. Configures appropriate security controls to enforce policies, standards, and procedures to protect information assets;
6. Develops standards and procedures for secure software configuration and design;
7. Participates in the system development life cycle to review software configuration and design, and perform threat and risk analysis to ensure proper security practices are used;
8. Performs vulnerability scans and security tests using commercial and open-source tools, and by developing and maintaining scripts and procedures to perform threat assessments;
9. Participates as a member of the security incident response team, evaluate security incidents to develop solutions, and participate in after-hours or on-call incident management;
10. Ensures security awareness through training programs and education for all County employees and OCIS staff;
11. Responds to and assists in cybersecurity assessment requests; evaluates vendor products and services; prepares technical specifications for technology procurement and evaluates potential purchases from a cybersecurity perspective;
12. Researches and attends training to stay current with cybersecurity trends and best practices.

FULL PERFORMANCE KNOWLEDGE, SKILLS, AND ABILITIES:

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;

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

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

Knowledge of training methods in staff development;

Ability to exercise independent judgment to assess cybersecurity requirements for system design and implementation;

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, participate in investigations and coordinate security anomalies and events;

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

Ability to prepare written documentation to communicate cybersecurity related material to end-users, OCIS staff, and management; 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:

EITHER:	(A)	Bachelor’s degree in cybersecurity, computer science, computer/network security or a closely related field AND two (2) years of full-time paid work experience in information technology and cybersecurity;
OR:	(B)	Associate’s degree as described in (A) AND four (4) years of full-time paid work experience as described in (A);
OR:	(C)	An equivalent combination of education and experience as indicated in (A) and (B).

NOTE: Education beyond the bachelor’s level may be substituted for up to one year of work experience.

NOTE: Certification as a Certified Information Systems Security Professional (CISSP), Certified Secure Software Lifecycle Professional (CSSLP), or CompTIA Security+ may be substituted for up to one year of work experience.

SPECIAL REQUIREMENTS:

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

COUNTY USE ONLY:

BARGANING UNIT/GRADE: CSEA 17		**JURISDICTIONAL CLASSIFICATION: Competitive**	
EEO Category:	**FLSA Code: EXEMPT**	**WC Code:**	**NYSLRS Job Code:**
REVISION HISTORY:			