DUTCHESS COUNTY CLASS SPECIFICATION	**CYBER SECURITY ADMINISTRATOR**	
DATE ADOPTED: 1/1/2019	LAST REVISION: 9/16/2025	Page 1 of 3

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 is exercised over the work of lower level titles.

TYPICAL WORK ACTIVITES:

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. Coordinates the cybersecurity components of disaster recovery and business continuity planning, including tabletop exercises;
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, including legal and risk management, to maintain integrity and confidence in the performance of the County's technology defenses;
7. Performs or coordinates vulnerability scans and penetration tests by developing and maintaining scripts, routines, and software to perform vulnerability threat assessments, or by coordinating with third-party solution providers to perform these tasks;
8. Coordinates remediation of vulnerabilities and threats to reduce organizational cybersecurity risk.
9. 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;
10. 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;
11. 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.

12. Respond to and assist in information security assessment requests; evaluate vendor products and services; advise management of risks and best security practices;
13. Coordinates cybersecurity audits and assessments, including internal and third-party evaluations.
14. Researches and attends training to stay current with cybersecurity trends and best practices.

FULL PERFORMANCE KNOWLEDGE, SKILLS, AND ABILITIES:

Knowledge of standard practices and procedures for developing and implementing an information security program, including knowledge of standard cybersecurity frameworks and controls such as NIST CSF, CIS Controls;

Knowledge of standard security practices, network architecture, routing, and TCP/IP protocols, Microsoft operating systems, Linux 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 current data privacy laws, regulations, and compliance issues applicable to information systems in local government, including the NY SHIELD Act, HIPAA, CJIS, PCI-DSS, etc.;

Knowledge of cybersecurity insurance requirements and cyber risk mitigation strategies;

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

Knowledge of modern cybersecurity platforms and tools, including zero trust architecture, endpoint detection and response (EDR), multifactor authentication, SIEM's etc.;

Knowledge of cloud security principles and tools;

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 solve problems effectively;

Ability to plan and supervise the work of others;

Personal characteristics necessary to perform the duties of the position;

Physical condition commensurate with the demands of the position.

MINIMUM QUALIFICATIONS:

EITHER: (A) Master's degree in cyber security, computer/network security, or a related field with a minor/concentration in cybersecurity AND one (1) year of full-time paid work experience in information technology and cyber security;

OR: (B) Bachelor's degree in a field described in (A) AND three (3) years of full-time paid work experience as described in (A);

OR: (C) Associate's degree in a field described in (A) AND five (5) years of full-time paid work experience as described in (A);

OR: (D) An equivalent combination of education and experience as indicated in (A) and (C) above.

NOTE: Your degree or college credit 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.

SPECIAL REQUIREMENTS:

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.

COUNTY USE ONLY:

BARGANING UNIT: CSEA	**JURISDICTIONAL CLASSIFICATION: COMPETITIVE**
GRADE: 19	**FLSA Code: OT Exempt**
REVISION HISTORY:	