<u>SENIOR COMPLIANCE AND NETWORK SPECIALIST</u>

<u>DISTINGUISHING FEATURES OF THE CLASS</u>: This is a technical position involving networking, system integrations and maintenance of related hardware and operating systems. The works involves the safekeeping of computer data from illegal or unauthorized disclosure, modification or destruction by directing data security activities, monitoring security threats, and communicating associated risks. The incumbent analyzes and diagnoses hardware and software network problems, administers various systems and applications as they apply to data risk management and security policy formulation and provides guidance to Information Technology staff on issues relating to data access security, data protection, backup and recovery. This position differs from Technology Compliance Specialist in that it performs various network and information technology tasks in addition to the security duties. Supervision is not a function of an employee in this class. Work is performed under general supervision of the Director of Information Services with wide leeway allowed for the exercise of independent judgment in carrying out the details of the work. A <u>Senior Compliance and Network Specialist</u> does related work as required.

<u>TYPICAL WORK ACTIVITIES</u>:

- Installs, programs, repairs and upgrades county network hardware/software equipment;
- Manages physical server infrastructure of the network;
- Participates in the development and implementation of data access security safeguards and protective measures to ensure the safekeeping and protection of computer data;
- Develops and maintains various auditing routines and reporting systems to isolate and identify occurrences of illegal or unauthorized access;
- Identifies, analyzes and resolves security and system problems relating to data access security;
- Develops and recommends data access security related standards, policies, procedures and guidelines and monitors compliance;
- Tests, evaluates and recommends new and/or revised systems, applications, programs and features related to information security;
- Investigates all incidences of data access violations and data corruption or loss, reports findings and takes appropriate action;
- Interacts with Information Technology staff, providing consultation on measures implemented to meet security policy requirements;
- Reviews and approves the acquisition and deployment of special-purpose security software or devices (e.g. digital certificates, 2-factor authentication tokens, etc.);
- Maintains various systems including email system, camera security system, door control, telephonic system and timeclock;
- Monitors news and events in the security marketplace as well as relevant laws and regulations that may affect the security posture of the organization;
- Makes recommendations for future need of hardware equipment and software for network environment;
- Uses computer applications or other automated systems such as spreadsheets, word processing, calendar, email and database software in performing work assignments;

- Establishes standards for networking and computer functions;
- Researches changing technology using trade journals and other forms of media to provide suggestions and input for future needs;
- Acts as project leader to direct and coordinate the activities of staff for work involving networking;
- Establishes standards for networking, hosts and servers and advocates for adoption of such standards;
- Performs a variety of computer/network hardware and software installation, configuration and training on the network;
- Assures coordination and compatibility of hardware/software systems and performs necessary stages of research and maintenance;
- Travels to various work locations to perform the above tasks.

FULL PERFORMANCE KNOWLEDGES, SKILLS, ABILITIES, AND PERSONAL CHARACTERISTICS: Thorough knowledge of state-of-the-art computer security; thorough knowledge of internal computer logic, programs and facilities; thorough knowledge of the operation and use of internally stored programmed computer with magnetic storage media; thorough knowledge of computer performance monitoring techniques; thorough knowledge of organization structure and its relation to work flow; thorough knowledge of requirements and capabilities of County hardware and related peripheral equipment; ability to comprehend and integrate complex computer technology, facilities and software into a working system of Data Access Security on a countywide basis; ability to read, interpret and apply technical information; ability to analyze and resolve security problems quickly and efficiently; ability to communicate effectively both orally and in writing; ability to analyze and evaluate security data; ability to plan, organize and supervise the work of others; ability to train and evaluate technical staff; ability to effectively use computer applications such as spreadsheets, word processing, calendar, email and database software; initiative; tact; and good judgment.

MINIMUM QUALIFICATIONS: Graduation from high school or possession of a high school equivalency diploma and either:

A) Graduation from a regionally accredited or New York State registered college or university with at least a bachelor's degree including or supplemented by eighteen (18) credit hours in management information systems, information technology security and risk analysis, technology integration, or closely related field, and three (3) years of experience developing and maintaining policies and procedures for computer security in a large integrated data processing environment;

<div align="center">OR</div>

B) Graduation from a regionally accredited or New York State registered college or university with at least an associate's degree including or supplemented by nine (9) credit hours in management information systems, information technology, security and risk analysis, technology integration, or closely related field, and five (5) years of experience in information systems security, security and risk analysis, information systems management, computer programming, network administration or closely related field including three (3) years of experience developing and maintaining policies and procedures for computer security in a large integrated data processing environment;

OR

C) Seven (7) years of experience in information systems security, security and risk analysis, information systems management, computer programming, network administration or closely related field including three (3) years of experience developing and maintaining policies and procedures for computer security in a large integrated data processing environment;

OR

D) An equalivant combination of the above mentioned training and experience.

SPECIAL REQUIREMENT: Candidates must possess a valid New York State Driver's license at time of appointment and throughout the duration of employment. Certain assignments made to employees in this class will require reasonable access to transportation to meet field work requirements made in the ordinary course of business in a timely and efficient manner.

CATTARAUGUS COUNTY CIVIL SERVICE

Adopted: 4/6/22