TECHNOLOGY COMPLIANCE SPECIALIST

DISTINGUISHING FEATURES OF THE CLASS: This 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 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. Responsibilities include developing and enforcing data access security related standards and guidelines, supervising and participating in the design and implementation of security safeguards, and developing and maintaining security auditing and reporting systems to ensure data integrity, confidentiality, reliability and availability. The work is performed under general direction of the Director of Information Services or his/her designee, with wide leeway allowed for the exercise of independent judgment in carrying out the details of the work. A Technology Compliance Specialist does related work as required.

TYPICAL WORK ACTIVITIES:

- 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.);
- Monitors news and events in the security marketplace as well as relevant laws and regulations that may affect the security posture of the organization;
- Uses computer applications or other automated systems such as spreadsheets, word processing, calendar, email and database software in performing work assignments;

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; physical condition sufficient to perform the essential functions of the position.

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 two (2) years of experience developing and maintaining policies and procedures for computer security in a large integrated data processing environment;

OR

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 four (4 years of experience in information systems security, security and risk analysis, information systems management, computer programming, or closely related field including two (2) years of experience developing and maintaining policies and procedures for computer security in a large integrated data processing environment;

OR

C) Six (6) years of experience in information systems security, security and risk analysis, information systems management, computer programming, or closely related field including two (2) 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 foregoing training and experience.

CATTARAUGUS COUNTY CIVIL SERVICE

Adopted: 7/25/2013