INFORMATION SYSTEMS SECURITY SUPERVISOR

DISTINGUISHING FEATURES OF THE CLASS: Under general supervision of the 2nd Deputy Chief Information Officer, an incumbent in this class, located in the Department of Information Technology, is responsible for safekeeping and protecting 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. Supervision is exercised over technical staff. Doe related work as required.

EXAMPLES OF WORK: (Illustrative Only)

Supervises and participates in the development and implementation of data access security safeguards and protective measures to ensure the safekeeping and protection of computer data;

Directs the activities of technical staff by establishing, assigning and reviewing daily and long-term projects, establishing goals and objectives, training new employees and evaluating work performance;

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;

EXAMPLES OF WORK: (Illustrative Only) (Cont'd.)

Uses computer applications or other automated systems such as spreadsheets, word processing, calendar, email and database software in performing work assignments;

May perform other incidental tasks, as needed.

REQUIRED KNOWLEDGE, SKILLS, ABILITIES AND ATTRIBUTES: 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 maintain effective working relationships with associates, users and vendors; resourcefulness; ability to read, write, speak, understand and communicate in English sufficiently to perform the essential duties of the position; ability to effectively use computer applications such as spreadsheets, word processing, calendar, email and database software; initiative; tact; physical condition commensurate with the demands of the position.

MINIMUM ACCEPTABLE TRAINING AND EXPERIENCE: Possession of a high school diploma or equivalency and either: (a) Bachelor's Degree* and five years experience in the computer field, three years of which must have included experience developing and maintaining policies and procedures for computer security in a large integrated data processing environment; or (b) ten years of experience as described in (a), including the three years of specialized experience; or (c) an equivalent combination of the foregoing training and experience.

SUBSTITUTIONS: Satisfactory completion of college level coursework* may be substituted at the rate of 30 credits per year of experience for up two years of experience, but candidates must possess the three years of specialized experience. Satisfactory completion of the CISSP security certification, or its industry equivalent, may be substituted for one year of the specialized experience.

*SPECIAL NOTE: Education beyond the secondary level must be from an institution recognized or accredited by the Board of Regents of the New York State Department of Education as a post secondary degree granting institution.

NOTE: Unless otherwise noted, only experience gained after attaining the minimum education level indicated in the minimum qualifications will be considered in evaluating experience.