INFORMATION / NETWORK SECURITY OFFICER 50-K

DISTINGUISHING FEATURES OF THE CLASS: This position, located in the Information Technology Services Department, involves overall responsibility for safekeeping and protecting computer data from illegal or unauthorized access, disclosure, modification or destruction by directing data security activities, monitoring security threats and communicating associated risks. The incumbent also performs routine maintenance and administration tasks on the County's Local Area (LAN), Wide Area (WAN) and Voice Network infrastructure. This position will perform LAN/WAN security procedures, including implementing login requests, and acts as liaison support between the PC/LAN team, vendors, and User Support staff as needed. The incumbent administers various systems and applications as they apply to data risk management and security policy formulation and provides guidance and supervision to Information Technology Services staff on issues relating to data access security, data protection, backup and recovery. The incumbent may, as directed by the CIO, participate in the investigative process surrounding information security incidents (e.g., forensics, evidence collection and preservation, log analysis, interviewing, etc.). Work is performed under the direct supervision of the Chief Information Officer with wide leeway for performing the duties of the position. Does related work as required.

TYPICAL WORK ACTIVITIES: *(The typical work activities listed below, while providing representative examples of the variety of work assignments in the title, do not describe any individual position. Incumbents in this title may perform some or all of the following, as well as other related activities not described.)*

Recognizes, researches, isolates and resolves network security problems;

Makes recommendations on various hardware and software products;

Documents all existing technology on the County's LAN/WAN network;

Utilizes approved policies and procedures to monitor, secure and maintain the County's network infrastructure;

Installs, troubleshoots and maintains racks, wire bridles, wall plates, patch panels, cable risers, network cabling, cross connections, routers, switches, etc.;

Performs daily or other periodic procedures to create backup, recovery files for all network configuration data contained on the network;

Provides technical advice and assistance to PC Technicians and Users in support of their use of network resources;

Develops and monitors LAN/WAN performance and utilization statistics and prepares reports for management summarizing network status;

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;

Develops and maintains various auditing routines and reporting systems to isolate and identify occurrences of illegal or unauthorized access;

Develops and recommends data access security related standards, policies, procedures and guidelines and monitors compliance;

Investigates all incidences of data access violations and data corruption or loss, reports finding and takes appropriate action;

Reviews the acquisition and deployment plans for special-purpose security software or devices (e.g. digital certificates, 2-factor authentication tokens, etc.);

Accesses protected health information (PHI) in accordance with departmental assignments and guidelines defining levels of access (i.e. incidental vs. extensive);

Develop, in collaboration with County Departments, the Chief Information Officer and the County Administration, a business continuity and a contingency plan to ensure protection of all confidential data during and after an emergency or disruption of security procedures;

Facilitates project team meetings, assigns responsibilities for project deliverables and coordinates workflow analysis and re-design;

Coordinates training on new security applications;

Coordinates security related software interface builds;

Serves as back-up to system administrator(s) for various security software applications;

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.

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 breach notification regulations and assist County in reporting and managing any breach of protected data; thorough knowledge of the operation and use of internally stored programmed computer with magnetic storage media; thorough knowledge of computer performance monitoring techniques; good knowledge of organization structure and its relation to work flow; ability to comprehend and integrate complex computer technology, facilities and software into a working system of Data Access Security on a countywide basis; high interpersonal and interviewing skills; strong ability to work independently and autonomously; strong organizational skills, including the ability to manage large projects; strong communication skills; strong ability to analyze and redesign workflows to support the implementation and meaningful use of County confidential data managed in software or technology systems; ability to effectively use computer applications such as spreadsheets, word processing, calendar, email and database software; ability to read, interpret and apply technical information; ability to analyze and resolve security problems quickly and efficiently; ability to present ideas clearly, 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; and ability to maintain effective working relationships with associates, users and vendors.

MINIMUM QUALIFICATIONS: Either:

(A)   Graduation from a regionally accredited college or university or one accredited by the New York State Board of Regents to grant degrees with a Bachelor's Degree or higher in Computer Sciences or a related field and six (6) years of network security experience in a large enterprise environment, 100 or more workstations connected to the network, with specific knowledge of network security software; or

(B)   Graduation from a regionally accredited college or university or one accredited by the New York State Board of Regents to grant degrees with an Associate's Degree and eight (8) years of experience as described in (A) above; or

(C)   Graduation from high school or possession of a high school equivalency diploma with ten (10) years of experience as described in (A) above.

SPECIAL REQUIREMENTS FOR APPOINTMENT: Must possess and maintain a valid driver's license; ability to safely lift and carry fifty (50) pounds.

SPECIAL NOTE: Each Special Industry Recognized Certifications, such as Microsoft Certified Systems Engineer, may be substituted for experience based on one certification equals two (2) years of experience.

Experience in the performance of basic keyboarding functions and/or experience with the use of specific software products (such as MS Word, Access, or Excel or other software products) is not considered to be qualifying experience. Experience in the operation of personal computers implies familiarity with hardware components, the ability to install basic hardware, the ability to connect wires and cables and the performance of basic repair and maintenance functions.

NOTE: Your degree or credits 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. If your degree or credits were awarded by an educational institution outside of the United States and its territories, you must provide independent verification of equivalency. A list of acceptable companies who provide this service can be found on the Internet at: https://www.cs.ny.gov/jobseeker/degrees.cfm. You must pay the required evaluation fee.

_____