ASSOCIATE SECURITY ANALYST

DISTINGUISHING FEATURES OF THE CLASS: This position has responsibility for assisting in performing both technical and administrative work involving policy and procedure development with regards to data integrity and infrastructure and system security. The incumbent assists in monitoring security systems and software to ensure the safekeeping and protection of data from unauthorized modification or destruction, Responsibilities also include assisting in the monitoring, assessing, and modifying the disaster recovery program, performing network intrusion testing, application vulnerability assessment scans, and risk assessment reviews. The work is performed under the general supervision of the Information Security Analyst win accordance with the County computer systems security policy. Does related work as required.

TYPICAL WORK ACTIVITIES:

Assists in the monitoring and advising on information security issues related to both systems and workflow to ensure that internal security controls for the county are appropriate and operating as intended;

Assists in making sure security appliances such as IPS, firewall, antivirus, antimalware, web filters and spam filters are kept up to date;

Assists in auditing and monitoring both electronic and physical security of IT systems and networks;

Assists in **c**reating and maintaining a County Incident Response Plan;

Assists in response team for information security incidents, including conducting the initial investigation to determine the type and scale of the incident, supervising any other technical teams to gather information;

Assists in developing information security policies, procedures, standards and guidelines based on knowledge of best practices and compliance requirements;

Assists in conducting county-wide data classification assessment and security audits and recommends remediation plans;

Keeps abreast of latest security issues;

Assists in conducting and documenting both internal and external intrusion testing;

Assists in the auditing and monitoring of security policies for workstations and servers;

Assists in coordinating the reporting of security issues;

ASSOCIATE SECURITY ANALYST–cont'd

Assists in creating, managing and maintaining user security awareness;
Assists in preparing and maintaining information security documentation, including department policies and procedures, county-wide notifications, Web content, and ITS alerts.

FULL PERFORMANCE KNOWLEDGE, SKILLS, ABILITIES AND PERSONAL CHARACTERISTICS:

Good knowledge of NIST and the most efficient practices pertaining to information technology security;
Good knowledge of the principles and practices of computer system security administration; Thorough knowledge of accepted information technology practices with regard to data integrity and security;
Good knowledge of firewall management;
Good knowledge of networking, network protocols, and network management;
Good knowledge of web filtering software and hardware;
Working knowledge of logical operations of data communications devices;
Working knowledge of local and wide area network administration;
Working knowledge of data processing methodology and techniques including documentation of data security;
Ability to communicate effectively, both orally and in writing;
Ability to understand and interpret complex technical material; Ability to prepare written material, especially system security documentation;
Ability to define and recommend computer documentation of data security;
Ability to establish and maintain effective working relationships;
Ability to deduce problems logically;
Ability to share and communicate relevant information in a timely fashion;
Strong attention to detail.

;.
MINIMUM QUALIFICATIONS:

A) Possession of a Bachelor's degree or higher in computer science, computer technology, data processing, management information systems, information resource management, or related field, and two (2) years' experience in security systems

administration and/or network administration, one year of which included network management and security as a primary function of the job; OR

B) Possession of an Associate's degree in computer science, computer technology, data processing, management information systems, information resource management, or related field, and four (4) years of experience in security systems administration and/or network administration, one year of which included network management and security as a primary function of the job; OR

C) Graduation from high-school or possession of an equivalency diploma and six (6) years of experience in security systems administration and/or network administration, one year of which included network management and security as a primary function of the job; OR

D) An equivalent combination of training and experience as indicated between the limits of A), B), and C) above.

NOTE: Your degree 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.

NOTES:
1) Certification as a Microsoft Network Administrator or Cisco Network Engineer may be substituted for one-year experience in security systems administration and/or network administration.
2) Two years of education in the specific field is equivalent to one year of experience in security systems administration and/or network administration.
3) There is no substitution for the required one-year experience in network management and security.

SPECIAL REQUIREMENT: Possession of a valid license to operate a motor vehicle in the State of New York will be required at time of appointment and maintain same while in the title.

SPECIAL NOTE: Because of the radical evolution of technology in this field, qualifying experience must have been gained within the last five years.