INFORMATION SECURITY ANALYST

DISTINGUISHING FEATURES OF THE CLASS: This position performs both technical and administrative work involving policy and procedure development with regards to data integrity and security. The incumbent monitors security systems and software to ensure the safekeeping and protection of data from unauthorized modification or destruction. The position also monitors, assesses, and modifies the disaster recovery program, performs network intrusion testing, application vulnerability assessment scans, and risk assessment reviews. The incumbent will lead the County Incident Response team, as well as set policies and provide education. The work is performed under the supervision of Information Technology management in accordance with the county computer systems security policy. Does related work as required.

TYPICAL WORK ACTIVITIES:

Monitors and advises 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;
Makes sure security appliances such as IPS, firewall, antivirus, antimalware, web filters and spam filters are kept up to date;
Audits and monitors both electronic and physical security of IT systems and networks;
Creates and maintains a County Incident Response Plan;
Leads the 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;
Works with the Information Technology Management on developing information security policies, procedures, standards and guidelines based on knowledge of best practices and compliance requirements;
Provides education on security related matters;
Conducts county-wide data classification assessment and security audits and recommends remediation plans;
Keeps abreast of latest security issues;
Conducts and documents both internal and external intrusion testing;
Audits and monitors security policies for workstations and servers;
Coordinates the reporting of security issues;

INFORMATION SECURITY ANALYST-cont'd

Collaborates with IT management, the Law department, the Security Division, and law enforcement agencies to manage security vulnerabilities;
Creates, manages and maintains user security awareness;
Prepares and maintains information security documentation, including department policies and procedures, county-wide notifications, Web content, and ITS alerts.

FULL PERFORMANCE KNOWLEDGE, SKILLS, ABILITIES AND PERSONAL CHARACTERISTICS:

Thorough knowledge of NIST and the most efficient practices pertaining to information technology security;
Thorough 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;
Thorough knowledge of firewall management;
Thorough knowledge of networking, network protocols, and network management;
Thorough knowledge of web filtering software and hardware;
Good knowledge of logical operations of data communications devices;
Good knowledge of local and wide area network administration;
Working knowledge of data processing methodology and techniques including documentation of data security;
Ability to implement and maintain computer security policies and procedures;
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.

MINIMUM QUALIFICATIONS:

A) Graduation from a regionally accredited or New York State registered four-year college or university with a Bachelor's degree or higher in computer science, computer technology, data processing, management information systems, information resource management, or related field, and three (3) 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) Graduation from a regionally accredited or New York State registered college or university with an Associate's degree in computer science, computer technology, data processing, management information systems, information resource management, or related field, and five (5) 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 seven (7) 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.

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.

"**BACKGROUND INVESTIGATION AND ADDITIONAL SCREENINGS:** Each candidate is subject to a thorough background investigation to comply with requirements related to security, data types and supported systems. A conviction at any time may bar appointment to this position, result in termination and/or require additional screening at the discretion of the employer."