ASSOCIATE SECURITY ANALYST TRAINEE

DISTINGUISHING FEATURES OF THE CLASS: The incumbent assigned to this position has responsibility to learn and assist in performing both technical and administrative work involving policy and procedure development with regards to data security and infrastructure and system security. The work is performed under direct supervision of the Associate Security Analyst or the Information Security Analyst, in accordance with the Broome County computer systems security policy. Does related work as required.

TYPICAL WORK ACTIVITIES:

Learns to and 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;

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

Learns to and assists in auditing and monitoring both electronic and physical security of IT systems and networks;

Leans to and assists in **c**reating and maintaining a County Incident Response Plan;

Learns to and 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;

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

Learns to and assists in conducting county-wide data classification assessment and security audits and recommends remediation plans;

Keeps abreast of latest security issues;

Learns to and assists in conducting and documenting both internal and external intrusion testing;

Learns to and assists in the auditing and monitoring of security policies for workstations and servers;

Learns to and assists in coordinating the reporting of security issues;

Learns to and assists in creating, managing and maintaining user security awareness;

Learns to and 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:

Working knowledge of NIST and the most efficient practices pertaining to information technology security;

Working 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;

Working knowledge of firewall management;

Working knowledge of networking, network protocols, and network management;

Working 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 closely related field; 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 two (2) 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 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

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

SUBSTITUTION: Certification in the following may be substituted for one year of the required experience:

1) ISC2 Systems Security Certified Practitioner (SSCP)
2) CompTIA Advanced Security Practitioner (CASP+)
3) Fortinet Certified Professional in Network Security (FCP-NS)
4) Cisco Certified Network Associate (CCNA)
5) Microsoft Certified Identity and Access Administrator Associate (SC-300)

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.

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.