INFORMATION SYSTEMS SECURITY ANALYST

DISTINGUISHING FEATURES OF THE CLASS: Under general supervision, an incumbent of this class is responsible for assisting in the organization and control of system security administration activities to ensure the safekeeping and protection of data and system assets from illegal, intentional or unauthorized disclosure, use, modification or destruction. Responsibilities include granting and monitoring computer access capabilities for various system users on a County-wide or agency-wide basis; interfacing with departmental coordinators to discuss and/or resolve security issues and problems, and performing analyses of data security systems to keep management informed of system utilization patterns. While supervision is not a function of this title, guidance and instruction may be provided to other information systems personnel regarding security-related best practices. Does related work as required.

EXAMPLES OF WORK: (Illustrative Only)

Assists in the implementation of data access security measures by identifying, analyzing and resolving cyber security and system problems relating to data security access, for applications, network, and computer programs;

Investigates security incidents concerning data access violations, breaches and data loss prevention of sensitive data. Reports findings to supervisor for direction or resolution;

Maintains the information security systems by joining or separating users to various system applications; coordinates the registration of users to the system and respective access levels with departmental coordinators;

Monitors and audits the information security systems to isolate and identify occurrences of illegal or unauthorized access; prepares reports and/or memoranda recommending corrective action;

Configures and maintains network and host-based security platforms;

Investigates and corrects cyber security related vulnerabilities and problems to ensure data information system integrity and a secure environment;

Performs analyses of data security systems to keep management informed of system security risks;

Assists in the development and maintenance of security tools, documentation and procedures to reduce cyber security risks in the environment;

Audits, tests and evaluates commercial and proprietary security software fixes, patches and runs to improve system performance and efficiency;

Conducts forensic investigations as required;

EXAMPLES OF WORK: (Cont'd)

Conducts periodic audits of user privileges to determine authorized access to systems and manage any discrepancies;

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

Uses computer and security applications or other automated tools such as spread sheets, word documents, calendar, e-mail, and various database software in performing work assignments;

May perform other incidental tasks, as needed;

FULL PERFORMANCE 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 logic, thorough knowledge of computer performance monitoring techniques; thorough knowledge of TCP/IP and OSI Model networking concepts; thorough knowledge of best practices regarding malware, emerging threats, attack vectors, and vulnerability management; good knowledge of organization structure and its relation to work flow; good knowledge of requirements and capabilities of County or Medical Center hardware and software related equipment; working knowledge of network and security analytical tools and applications such as Wireshark, SolarWinds, SNORT, Kali Linux, Gigamon, etc. in performing work assignments; ability to comprehend and integrate complex computer technology, facilities and software into a working system of Data Access Security; ability to read, interpret and apply technical information; ability to analyze and identify security problems quickly and efficiently coupled with an ability to recommend appropriate resolutions to same; ability to communicate complex solutions and concepts effectively to technical and non-technical audiences both orally and in writing; ability to analyze and evaluate operational data; ability to establish and maintain effective working relationships with associates, users and vendors; ability to read, write, speak, understand, and communicate in English sufficiently to perform the essential duties of the position; resourcefulness; initiative; tact; physical condition commensurate with the demands of the position.

MINIMUM ACCEPTABLE TRAINING AND EXPERIENCE: Current certification as a Certified Information Systems Security Professional (CISSP).

NOTE: Employee must:

1. maintain CISSP certification while in the title.
2. be licensed to drive a motor vehicle in New York State at time of appointment and maintain same while in the title.