

CLASS SPECIFICATION
County of Fairfax, Virginia

CLASS CODE: 1838

TITLE: INFORMATION SECURITY ANALYST IV

GRADE: S-31

DEFINITION:

Under limited supervision, enacts the directives of the Chief Information Security Officer across divisional boundaries and enterprise agencies. Serves as the lead for implementing major Information Security Office (ISO) projects and programs and liaison between ISO and Department of Information Technology technical support groups; develops information security architecture and systems; develops and enforces security policies and procedures; leads and manages security management services, forensic analysis, cybercrime investigations and incident response; supervises subordinate Information Security Analyst positions; and performs related work as required.

DISTINGUISHING CHARACTERISTICS OF THE CLASS:

This advanced/supervisory information security analysis work is distinguished from the Information Security Analyst III in that the Information Security Analyst IV performs work that includes a leadership role with project management and supervisory responsibility, policy creation and enforcement recommendations, and forensic investigation and analysis; whereas the Security Analyst III performs work that focuses on the operational and design activities involving cross-environment security architecture and complex management systems integration, performance of highly complex analyses and technical tasks, and deployment of protective processes. The classes are further distinguished by the portion of time spent interfacing with individuals or groups outside the functional area(s) of primary responsibility.

ILLUSTRATIVE DUTIES:

(The illustrative duties listed in this specification are representative of the class but are not an all inclusive list. A complete list of position duties and unique physical requirements can be found in the position description.)

Manages operational activities implementing the enterprise-wide information security program and develops related procedures and performance metrics;
Reviews and contributes to the improvement and standardization of the security administration process across all business units;
Develops IT security architecture and system design guidelines, and evaluates and/or assists IT system designs to ensure appropriate controls and protections are included;
Plans, organizes, coordinates, assigns and evaluates the work of security analysts, technical team members and vendor staff;
Conducts forensic analysis, cyber-crime investigations and incident response as directed by the Chief Information Security Officer;
Interacts with county agency management and staff to guide security policies and procedures;
Ensures enterprise IT architecture is compliant with federal health, privacy and financial regulations and manages quarterly risk assessment program;
Analyzes and evaluates system generated security incident reports and information security notices issued by information system vendors, government agencies, universities, professional

CLASS CODE: 1838

TITLE: INFORMATION SECURITY ANALYST IV

GRADE: S-31

Page 2

associations, and other organizations, and advises senior management on appropriate safeguards for adoption;

Advises internal and external government partners, professional IT analysts and management on security requirements supporting inter-agency and regional interoperability initiatives;

Identifies process functions, risk security weaknesses and controls;

Presents security challenges and resolutions to management;

Researches and deploys new technologies, and manages transition to operational service;

Provides leadership on security projects which involve a wide range of issues including secure architectures, secure electronic data traffic, network security, platform and data security and privacy;

Works with senior management to determine acceptable levels of risk for enterprise computing platforms and discusses security implications of new information technology uses being considered;

Represents and promotes the county' IT security program at conferences and other speaking engagements, and pursues and writes award recognition;

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES:

(The knowledge, skills and abilities listed in this specification are representative of the class but are not an all inclusive list.)

Thorough knowledge of the cyber-security industry issues and related regulatory and compliance matters, information security standards, guidelines, applied procedures, and risk mitigation;

Excellent analytical and problem solving skills;

Extensive knowledge of IT security architecture design, processes and controls, data security and access control systems, identification and authentication, access control encryption and related matters;

Knowledge of all areas of technology platforms, applications, servers, operating systems, database, network architecture, and data;

Knowledge of system and network exploitation, attack pathologies and intrusion techniques, i.e., denial of services, malicious code, password cracking, etc;

Knowledge of all pertinent federal and state regulations and associated accreditations and/or certifications regarding information protection (e.g., Virginia Freedom of Information Act, E-Discovery, HIPAA, PCI, COPA, etc.);

Ability to conduct digital forensics investigations, secure evidence and formulate conclusions;

Ability to interact with law enforcement officials and legal counsel;

Ability to plan, organizes, coordinate, assign and evaluate the work of subordinate staff;

Ability to interface with individuals at all levels of the organization and to establish effective working relationships;

Ability to communicate effectively, both orally and in writing;

Ability to present and discuss technical information in a way that establishes rapport, persuades others, and gains understanding;

Ability to maintain the highest level of ethics and integrity in handling sensitive and classified matters.

CLASS CODE: 1838

TITLE: INFORMATION SECURITY ANALYST IV

GRADE: S-31

Page 3

EMPLOYMENT STANDARDS:

Any combination of education, experience, and training equivalent to the following:

Possession of a bachelor's degree in information systems, computer science, telecommunications management, business or public administration; PLUS

Five years of information security systems experience, including leadership and supervisory experience; OR

Combination of seven years related work experience and two years professional training with possession of information security specific certifications (e.g., CISSP, GIAC, Security+, Forensics, etc.) may be substituted for four year degree requirement.

CERTIFICATES AND LICENSES REQUIRED:

Possession of one of the following certifications:

Certified Information Systems Security Professional (CISSP)

Global Information Assurance Certification (GIAC)

ESTABLISHED: October 14, 2009