New York State Department of Civil Service
DIVISION OF CLASSIFICATION & COMPENSATION

Classification Standard

Occ. Code 0815350

Information Technology Specialist 2 (Information Security), Grade 18 0815350
Information Technology Specialist 3 (Information Security), Grade 23 0815450
Information Technology Specialist 4 (Information Security), Grade 25 0815550

Brief Description of Class Series

Information Technology Specialists (Information Security) perform cyber security activities to protect New York State's assets (data, systems and infrastructure); and collaborate with State and federal entities to identify and respond to threats and risks to New York State.

Distinguishing Characteristics

All positions are in the non-competitive jurisdictional class.

Information Technology Specialists (Information Security) at various levels perform similar duties with positions distinguished by level of responsibility, depth and breadth of IT programs and systems supported, and supervision. Incumbents coordinate with control agencies which have oversight of information technology on the direction and management of an agency information security compliance program; manage and resolve security threats to agency information systems; conduct first- and second-level analysis, remediation, and escalation of cyber events; and conduct digital forensic and threat detection/prevention analysis. The breadth and depth of the program they support or administer dictates the level classified.

*Information Technology Specialist 2 (Information Security)***:** entry level; performs a variety of information security duties with detailed instructions and guidance provided by either an Information Technology Specialist 3 (Information Security) or higher-level security position; may supervise student assistants or support staff.

*Information Technology Specialist 3 (Information Security)***:** full performance level; under the general direction of a higher-level security position, independently performs a broad variety of information security duties with less instruction or works on more technically complex analysis; may supervise student assistants, support staff or Information Technology Specialist 2 (Information Security).

*Information Technology Specialist 4 (Information Security)***:** supervisory level; under the general direction of a higher-level security position, performs a variety of

information security duties with little to no instruction and/or works on more technically complex cases, and supervises Information Technology Specialists 2 and 3 (Information Security) or equivalent contract staff.

Related Classes

Information Technology Specialists perform or assist in performing technical and agency program support IT activities related to network and system design, configuration, maintenance, and security; customer support; business/systems analysis and design which may include web site development and administration of a transactional, dynamic, or interactive web site; and the design, development and administration of database systems.

Intelligence Analysts (Information Systems) are assigned to the New York State Intelligence Center (NYSIC) within the Cyber Analysis Unit at the Division of State Police. Incumbents engage in activities to protect New York State's infrastructures and analyze threats and risks to the State. Incumbents collaborate with the Division of Homeland Security and Emergency Services to identify and review ongoing intrusion activities and threats to New York State.

Illustrative Tasks

Information Technology Specialist 2 (Information Security)

Implements information security and compliance programs.

- Participates in the development, interpretation, review and communication of information security policies, procedures and standards.
- Monitors information security compliance and recommends improvements.
- Supports the implementation of information security procedures and protocols and participates in security risk reviews and remediation activity including producing written reports.
- Works with internal and external partners on information security issues.
- Plans and conducts outreach programs and activities to increase cyber security awareness.
- Builds/maintains Business Continuity and Disaster Recovery documentation.
- Tracks and reports out on all security related project portfolio tasks.

- Administers or verifies training to agency employees, contractors, and third parties, as appropriate, on their responsibilities to protect agency IT and information assets.

- Develops and champions information security awareness activities.

Supports the management and resolution of security threats to agency information systems.

- Participates in information security risk analysis and risk management processes with business and IT units.

- Performs vulnerability scanning and analysis to help determine scope of risk and prioritization of remediation.

- Collects and maintains risk register, including reporting and tracking of remediation.

- Monitors external data sources to maintain currency of threat condition and potential impact on enterprise.

- Participates in the identification and modeling of new threat scenarios to provide proactive defensive measures to technical teams for mitigation of risk.

- Disseminates threat and vulnerability intelligence products.

- Characterizes and analyzes network traffic to identify anomalous activity and potential threats to network resources.

- Participates in the continuous monitoring and protection of technology resources and determines events that require investigation and response.

Participates in cyber incident response.

- Supports the implementation and improvement of information security incident response plans and reports.

- Participates in the investigation of alleged information security violations, follows agency procedures for referring the investigation to other investigatory entities (e.g., law enforcement, and State and federal oversight agencies), and responds to requests for information from external investigators.

- Performs analysis (e.g., logs, packet capture, reverse engineering) during cyber investigations to establish root cause and provides remediation recommendations.

- Collects, seizes, handles and analyzes digital evidence, identifies elements discovered during investigations for their potential use as evidence in criminal or other investigations, and produces forensic reports with findings documented.

Serves as information security expert and evaluates systems and contracts for alignment with agency and State information security policies.

- Reviews contract, service level agreement, memorandum of understanding language and other documents to verify that they meet information security needs and requirements and align with agency and State information security policies.

- Provides information security expertise, advice and recommendations to agency executives on a broad range of information security matters.

- Acts as information security lead on projects and initiatives to ensure security by design through implementation of the Secure Systems Development Lifecycle (SSDLC).

Monitors information security trends, tools and techniques.

- Keeps abreast of relevant laws and regulations that could affect the security controls and classification of information assets and communicates legal and regulatory requirements.

- Researches, administers and utilizes specialized cyber security tools, techniques, and procedures.

- Represents the agency at internal and external information security meetings and conferences to maintain awareness and evaluates the applicability of the latest information security techniques and tools to the agency's security program.

- Participates in creation and maintenance of dashboard and reports that present information security data in an intuitive manner.

Information Technology Specialist 3 (Information Security)

Performs the above duties with considerable independence, and in addition may supervise student assistants, support staff or provide guidance to Information Technology Specialist 2 (Information Security).

Information Technology Specialist 4 (Information Security)

Performs the above duties, and in addition supervises a team of Information Technology Specialists 2 and 3 (Information Security) or equivalent contract staff.

Serves as a subject matter expert in multiple areas of cyber security such as incident response, digital forensics, risk assessments, digital identity management, federal compliance requirements.

Supervises staff and assigns work, writes performance and probationary evaluations, conducts interviews, and hires staff.

Supervision Exercised

Information Technology Specialist 2 and 3 (Information Security) are typically non-supervisory. Positions may supervise student assistants, support staff or provide guidance on information security policy and procedures to co-workers.

Information Technology Specialist 4 (Information Security) typically supervises lower-level information security staff assigned to an information security unit. Supervision includes providing technical direction on specific tasks, ensure adherence to information security policies and procedures, and administrative supervisory duties such as approving time off; signing timecards; and completing performance evaluations.

In smaller units, positions may coordinate staff from different business units and may not be responsible for the regular supervision of these individuals but contribute to the employee's performance evaluation. In larger units, Information Technology Specialists 4 (Information Security) directly supervise information security staff, and direct and coordinate staff from different business units to ensure adherence to information security policies and procedures.

Minimum Qualifications

Information Technology Specialist 2 (Information Security)

Non-competitive: bachelor's degree* with at least 15 credit hours in cyber security, information assurance, or information technology.

Information Technology Specialist 3 (Information Security)

Non-competitive: bachelor's degree* with at least 15 credit hours in cyber security, information assurance, or information technology; and two years of information technology experience, including one year of information security or information assurance experience**.

Information Technology Specialist 4 (Information Security)

Non-competitive: bachelor’s degree* with at least 15 credit hours in cyber security, information assurance, or information technology; and three years of information technology experience, including two years of information security or information assurance experience**.

*Substitution: bachelor's degree candidates without at least 15 course credits in cyber security, information assurance, or information technology require an additional year of general information technology experience to qualify. Appropriate information security or information assurance experience may substitute for the bachelor's degree on a year-for-year basis; an associate's degree requires an additional two years of general information technology experience.

**Experience solely in information security or information assurance may substitute for the general information technology experience.

Note: Classification Standards illustrate the nature, extent, and scope of duties and responsibilities of the classes they describe. Standards cannot and do not include all of the work that might be appropriately performed by a class. The minimum qualifications above are those which were required for appointment at the time the Classification Standard was written. Please contact the Division of Staffing Services for current information on minimum requirements for appointment or examination.

Date: 3/2021

CM