8242

INFORMATION SECURITY OFFICER 2

NATURE OF WORK

Under limited supervision, at the full-performance level, performs professional/technical work in the Office of Technology in developing, implementing, and maintaining information security policies, standards, and controls throughout the enterprise. Performs audits and assessments to identify and analyze threats/vulnerabilities posing risks to data, personnel, applications, systems, and other resources. Performs duties necessary to define, establish, and maintain resource ownership/stewardship responsibilities, such as data classification, account management, access controls, monitoring activities, and other internal controls. Recommends internal controls and risk management strategies to reduce risks and ensure compliance with policy and regulations. Assumes lead responsibility for the planning, development, implementation, reporting, and ongoing management of one or more Office of Information Security and Controls (OISC) programs. Manages the scope, schedule, and other resources required to deploy the OISC programs throughout the Executive Branch. Travel may be required. Performs related work as required.

DISTINGUISHING CHARACTERISTICS

The Information Security Officer 2 serves as team lead or provides information security guidance for security projects of moderate complexity, moderate scope, and limited duration. Projects at this level have a significant impact on enterprise and/or Office of Technology operations. Provides advanced support to senior personnel on projects of significant complexity and enterprise-wide scope. An incumbent works independently on assignments of moderate complexity. The Information Security Officer 2 has a broad background in information security enabling the individual to contribute or to lead projects related to various: (1) controls, such as, access controls, auditing, monitoring, policies, and training; (2) processes, such as, account management, data management and classification, incident management, disaster recovery, and investigations; and/or, (3) technologies, such as, network components, operating systems, servers, personal computers, mobile devices, and telecommunications.

ESSENTIAL JOB FUNCTIONS: **(Any specific position in this class may not include all of the duties listed, nor do the examples listed cover all of the duties which may be assigned.)**

Supports security operations (e.g., intrusion detection/prevention, Web filtering, and vulnerability scans) to continually monitor the technology resources and analyze the environment for security threats/vulnerabilities and unauthorized access to the Office of Technology network. Responds to moderately complex security requests, problem reports, questions, and incident reports; takes corrective action and follows-up on corrective actions to ensure that threats and vulnerabilities are addressed.

Coordinates and performs forensic examinations to ensure proper containment and preservation of evidence, precise tracking of forensic events, accurate maintenance of the chain of custody, and other related tasks.

Guides risk assessment exercises to identify, evaluate, and address the Executive Branch processes and operations posing security threats or significant vulnerabilities to data, personnel, systems, and other technology resources.

ESSENTIAL JOB FUNCTIONS (cont'd):

Performs and may manage moderate audits or portions of large scope audits and assessments to analyze and evaluate the effectiveness of controls, policy and regulatory compliance, security monitoring tools, etc. and makes recommendations to strengthen those controls and/or achieve necessary compliance.

Prepare and presents audit and assessment findings, as well as recommendations of options to mitigate risks, achieve compliance, address threats/vulnerabilities and strengthen controls.

Recommends, drafts, and contributes to the development of information technology and information security policies, procedures, and standards to govern information technology usage and optimize operations across the Executive Branch.

Communicates and enforces the West Virginia Office of Technology information security policies, standards, and procedures as approved by the executive management.

Assists with and may lead components of the planning and delivery of information security awareness and training throughout the Executive Branch. Responds to questions and resolves problems related to the Information Security Awareness Training Program. Develops and presents customized information security awareness training.

Monitors employee compliance with information security training policies. Works with OISC training leader, personnel, training units, supervisors, and others to ensure that employees are successfully completing information security awareness and refresher training.

Develops or acquires content for information security courses, articles, bulletins, flyers, Web postings, and other distribution vehicles.

Manages and responds to service desk problem tickets to ensure appropriate resolution of issues; analyzes problem tickets to identify issues, patterns, etc. that pose security threats to Office of Technology systems and data.

Contributes to the preparation and presentation of formal information security briefings, seminars, and self-assessment exercises for various parties, such as the Governor's Executive Information Security Team (GEIST), the Security Audit Committee, the Chief Technology Officer, the Chief Information Security Officer, management, Office of Technology Directors, audit clients, and others.

Provides technology resource life-cycle support by performing duties necessary to define, implement, and maintain information security requirements for applications, systems and other technology resources.

Coordinates and assists in the management of third-party information security engagements to ensure that (1) third-parties have access to, and ultimately obtain accurate and complete information, (2) engagement objectives are achieved, (3) deliverables comply with contract specifications, and (4) costs are controlled by avoiding duplicate or out-of-scope work.

Reviews, evaluates, and recommends hardware, software, and other information security related procurement requests for consistency with policy and best practices, technical feasibility, potential to enhance operational efficiencies, and the ability to provide secure services. Recommends security products, services, and /or procedures to enhance security and deliver operational efficiencies.

ESSENTIAL JOB FUNCTIONS (cont'd):

Assists with, and may lead incident management activities to establish a central point of contact for reporting incidents and provide consulting services and support throughout all phases of the incident handling process.

Collaborates with and provides security expertise to the West Virginia Privacy Office and State Privacy Officers to assure that privacy concerns are properly addressed.

Represents the Office of Technology OISC with other governmental agencies, other Office of Technology work groups, professional associations, and community organizations.

Maintains advances skills and knowledge of information security and technology by researching technical literature, serving on professional association committees or boards, and attending classes, seminars, and conferences.

KNOWLEDGE, SKILLS, AND ABILITIES:

Knowledge of at least five (5) of the ten (10) recognized information security domains: (1) access controls, (2) application security, (3) business continuity and disaster recovery, (4) cryptography, (5) risk management, (6) regulations, compliance and investigations, (7) operations security, (8) physical security, (9) security architecture, and (10) telecommunications.

Knowledge of information technology architectures, applications, data management, databases and other data repositories, software, hardware, information processing, data center/system operations, networks, telecommunications, terminology, and concepts.

Knowledge of programming languages and concepts.

Knowledge of information technology forensic investigations involving the containment, recovery, and preservation of evidence, as well as, regulations governing forensic investigations, e-Discovery, etc.

Knowledge of project management principles and practices, such as resource management, tasks and work breakdown structure, schedules, milestones, reporting, and issue tracking.

Skilled in the use of tools and technologies to assess, monitor, evaluate, document, and report on the security state of applications, systems, media, and other technology resources.

Ability to analyze and evaluate various work environment and processes to specify security requirements, determine testing criteria, and recommend monitoring techniques.

Ability to make decisions and use independent judgment, especially when resolving complex, challenging issues associated with information security work, projects or operations.

Ability to read, understand, evaluate, interpret, compile, and apply complex technical information (e.g., technical diagrams, program code, technical manuals, regulations, and standards).

Ability to communicate effectively, both verbally and in writing, to diverse groups, including those serving in management, professional, technical, and staff positions.

Ability to establish and maintain effective working relationships with subordinates, superiors, and the user community.

MINIMUM QUALIFICATIONS:

Training: Bachelor's Degree from a regionally accredited four-year college or university.

Substitution: Up to two years experience as described below may substitute for the required training on a year-for-year basis.

Experience: Eight years of full-time or equivalent part-time paid experience in computer science, information security, software engineering, information technology auditing, network administration, or other related information technology field.

Substitution: (1) Master's Degree from a regionally accredited college or university may substitute for two (2) years of the required experience. (2) Each professional information security certification or license from a nationally recognized professional organization, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Auditor (CISA), or Certified Information Security Manager (CISM), or other technical certifications at the discretion of the Office of Technology Chief Information Security Officer may be substituted for one year of work experience. (3) Each technical or specialist certification, such as Systems Security Certified Practitioner (SSCP), Network + Certification, FBI Computer Analysis Response Team (CART) Field Examiner Certification, Computer Hacking Forensic Investigator (CHFI), or other technical certifications at the discretion of the Office of Information Technology Chief Information Security Officer may be substituted for six months of work experience. (4) Successful completion of twenty-four (24) semester credits or 384 hours of industry recognized/authorized/certified information security training/seminars, related to ISO job duties may be substituted for one (1) year of the required experience. Semester hours must be supported by transcripts and equivalent industry training must be supported by records from the organization hosting the training/seminar.

Established: 9/30/08
Effective: 11/1/08