8241

INFORMATION SECURITY OFFICER 1

NATURE OF WORK

Under general 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. Assists with 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, and ongoing management of at least one Office of Information Security and Controls (OISC) program. Manages the scope, schedule, and other resources that are required to deploy the OISC program throughout the Executive Branch. Travel may be required. Performs related work as required.

DISTINGUISHING CHARACTERISTICS

The Information Security Officer 1 is typically involved in, and frequently leads security initiatives or projects of limited complexity, scope, and duration. Projects at this level may have an impact on enterprise and/or departmental operations. An incumbent works independently on routine assignments such as running security monitoring tools, preparing presentation materials, and compiling audit documentation. Works under the direction of more senior personnel for assignments of increasing complexity, such as regulatory audits, detailed technical testing, and performance of forensic investigations. The Information Security Officer 1 has a general background in information security enabling the individual to contribute effectively to projects involving 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, Web applications, mobile devices, and personal computers.

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 security requests, problem reports, questions, and incident reports; recommends or takes corrective action and follows-up on corrective actions to ensure that threats and vulnerabilities are addressed.

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

8241

INFORMATION SECURITY OFFICER 1 (CONT'D)

ESSENTIAL JOB FUNCTIONS (cont'd):

Provides assistance with the definition, implementation, maintenance and monitoring of information security requirements for applications, systems and other technology resources.

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.

Assists in planning and performing audits and assessments of processes, employee practices, network operations and components, servers, telecommunications, applications, and other technology resources for policy and regulatory compliance, threats and vulnerabilities, and weak or missing controls. Supports technology tools typically used in audits, assessments, monitoring, analysis, presentations, reporting, and other OISC activities.

Assists in the preparation and presentation of audit and assessment findings, as well as recommendations of options to mitigate risks, achieve policy and regulatory compliance, 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.

Contributes to the communication and enforcement of the West Virginia Office of Technology information security policies, standards, and procedures, as approved by the executive management.

Assists in the planning and delivery of policy training and information security awareness training rollout across the Executive Branch.

Provides support for information security training and awareness activities. Responds to questions and resolves problems related to the on-line Information Security Training Program. Coordinates requests for, and develops, customized information security 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.

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.

Makes recommendations and provides consulting services on the development of procurement instruments and the routine procurement of information security products and/or services.

8241

INFORMATION SECURITY OFFICER 1 (CONT'D)

ESSENTIAL JOB FUNCTIONS (cont'd):

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.

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 and develops information security knowledge and skills by researching technical literature and attending classes, seminars, and conferences.

KNOWLEDGE, SKILLS, AND ABILITIES:

Knowledge of at least three (3) 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.

Basic knowledge of information technology software, hardware, terminology, and concepts.

Basic knowledge of information technology forensic investigations involving the recovery of evidence from computers and other storage media, preservation of evidence, and regulations governing forensic investigations, e-Discovery, etc.

Ability to develop skills to use tools and technologies to assess, monitor, and document the security state of applications, systems, media, and other technology resources.

Ability to read, understand, interpret, compile, and apply technical information.

Ability to communicate effectively, both verbally and in writing.

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: Six 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.

8241

INFORMATION SECURITY OFFICER 1 (CONT'D)

MINIMUM QUALIFICATIONS (Cont'd):

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