8243

INFORMATION SECURITY OFFICER 3

NATURE OF WORK

Under general direction, performs advanced and expert level professional/technical work in the Office of Technology by developing, implementing, and maintaining information security policies, standards, and controls throughout the enterprise. Directs audits and assessments to identify and analyze threats/ vulnerabilities posing risks to data, personnel, applications, systems, and other resources. Leads activities to define, establish, and maintain resource ownership/stewardship responsibilities, such as data classification, account management, access controls, monitoring activities, and other internal controls. Issues managements reports recommending internal controls and risk management strategies to reduce risks and ensure compliance with policy and regulations. Responsible for the planning, development, implementation, reporting for, and ongoing management of two to three Office of Information Security and Controls (OISC) programs. Manages the scope, schedule, budget, personnel, and other resources required to deploy the OISC programs across the Executive Branch. Mentors others with the OISC, as well as within the Office of Technology. Travel may be required. Performs related work as required.

DISTINGUISHING CHARACTERISTICS

The Information Security Officer 3 leads or serves as a subject matter expert for initiatives or projects of significant complexity with enterprise-wide scope and extended duration. Such initiatives or projects are highly visible and have significant impact on the enterprise and/or Office of Technology operations and goals. When in charge of information security projects, this position leads personnel from other units, departments, and agencies; may assume management responsibilities on a temporary or permanent basis. The position performs both functional and technical work, as well as evaluates different perspectives and alternatives to deliver effective information security solutions. Requires excellent customer service skills. Responds to a wide variety of security requests, problem reports, questions, and incident reports. Then, takes action to resolve the questions, problems, or issues. The Information Security Officer 3 has a broad, highly advanced level of knowledge and experience to direct work and projects related to complex: (1) controls, such as, access controls, auditing, authorization, segregation of duties, monitoring, policies, and training; (2) processes, such as, account management, data management and classification, technology resource lifecycles, incident management, disaster recovery, and investigations; and/or, (3) technologies, such as, applications, databases, data centers/facilities, network components, operating systems, servers, computers, 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.)**

Serves as an information security subject matter expert to all Office of Technology divisions during technical projects to assure that security requirements are defined early in the project, proper security testing is conducted, and security issues are resolved before implementation. Provides project consulting services by reviewing the requirements, design, and accreditation/certification processes to assure that adequate administrative/technical security controls are included/embedded, and standards are achieved before the implementation of an application, system, or service.

INFORMATION SECURITY OFFICER 3 (CONT'D)

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.)**

Architects technical information security solutions, including research, analysis, and design activities to implement advanced technical security solutions. Reviews, evaluates, and recommends hardware, software, and other technology acquisitions for consistency with policy and best practices, technical feasibility, potential to increase operational efficiencies, and the ability to provide secure services.

Leads technical/control installation, integration, process/procedure development, training, etc. utilizing advanced institutional knowledge of the State's information technology architecture and/or advanced technical expertise to integrate advanced information security solutions with the existing technology to enhance the strategic security posture.

Manages security operations (e.g., intrusion detection/prevention, vulnerability analysis, and Web filtering) to continually monitor and analyze the environment for security threats, vulnerabilities, and unauthorized access to the Office of Technology resources. Recommends corrective actions, and then, follows-up on corrective actions to ensure that threats and vulnerabilities are addressed.

Leads risk management activities to identify, evaluate, and address processes and operations posing security threats or significant vulnerabilities to data, personnel, systems, and other technology resources. Advises management on the prioritization of risks, consequences of selecting a specific risk management strategy, and the effectiveness of specific security risk management strategies.

Directs audit and assessment projects to continually analyze and evaluate the effectiveness of controls, regulatory and policy compliance, security monitoring tools, etc. within the Executive Branch.

Issues formal recommendations, in the form of reports and presentations, to provide management with guidance and alternatives to mitigate risks, achieve policy and regulatory compliance, and strengthen internal controls.

Directs forensic examinations to ensure proper containment and preservation of evidence (e.g., data, media, equipment, etc.), precise tracking of forensic events, accurate maintenance of the chain of custody, and other related tasks.

Leads incident management activities to establish a central point of contact for reporting incidents and provides consulting services throughout all phases of the incident handling process.

Leads the work of other staff as they train for the support of information security administrative and technical controls, including the mentoring of the Information Security Associate, Information Security Officer 1, and/or Information Security Officer 2 in the best practices associated with all the OISC strategic initiatives.

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 WV OT information security polices, standards, and procedures as approved by the executive management.

Directs the development or acquisition of new, relevant information security training content, security communications, and content for Web pages, news articles, flyers, and other distribution vehicles. Leads activities to evaluate the effectiveness of information security awareness training activities to ensure that the content is relevant, appropriate, and effectively influencing the behavior of Executive Branch personnel.

INFORMATION SECURITY OFFICER 3 (CONT'D)

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.)**

Prepares and presents briefings, training, and seminars for/to the Governor's Cabinet, Governor's Executive Information Security Team (GEIST), the Security Audit Committee, the Chief Technology Officer, the Chief Information Security Officer, management, audit clients, and others.

Leads clients seeking to obtain third-party information security related services, through the development of information security specifications, and the evaluation of vendor responses to ensure that engagement objectives are clearly articulated and the appropriate vendor is selected.

Oversees third-party Information security engagements to ensure that (1) third-parties 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.

KNOWLEDGE, SKILLS, AND ABILITIES:

Knowledge of all 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 lifecycle methodologies (e.g., requirements, acquisition, development, implementation, testing, certification and accreditation, maintenance, conversion, retirement, etc.) for data, applications, hardware, and other technology resources.

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

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 direct and manage diverse teams or groups on projects, of moderate to long duration, that impact numerous operations and processes, and require substantial changes in culture and business practices.

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.

INFORMATION SECURITY OFFICER 3 (CONT'D)

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: Ten 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.

Special Requirement: Must acquire **o**ne professional information security certification 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 professional certifications at the discretion of the Office of Technology Chief Information Security Officer. **OR** Must acquire two technical/specialist information security related certifications, such as Systems Security Certified Practitioner (SSCP®), A+ Certification, Network + Certification, Computer Hacking Forensic Investigator (CHFI), FBI Computer Analysis Response Team (CART) Field Examiner Certification, or other technical certification at the discretion of the Office of Technology Chief Information Security Officer.

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