8266

DIRECTOR OF INFORMATION SECURITY, COMPLIANCE AND INTERNAL CONTROLS

NATURE OF WORK

Under administrative direction performs highly responsible and complex administrative work directing the information security, compliance and internal controls functions of the state. Responsible for an organization to establish, develop, implement, and improve information security systems, compliance and controls functions across the enterprise and within the various state agencies for the purpose of promoting more effective and efficient security administration, compliance and controls. The Director of Information Security will work with the Chief Privacy Officer to mutually support the Executive Branch Privacy and Information Security Programs. Additional responsibility includes the development and enforcing of policies and procedures to adequately insure that compliance and internal controls exist across the Executive Branch agencies. Administrative responsibilities include: policy leadership; directing development of security systems and procedures, and assuring the maximum usage of information security systems, personnel, and equipment; audit and control of security policies and procedures to insure cost-effective use of enterprise information security resources to enable state agencies to carry out their appointed functions. The incumbent shall have wide latitude in performance of duties within the framework of rules and general policies. Performs related work as required.

EXAMPLES OF WORK PERFORMED

Identifies information security and privacy goals and objectives consistent with state strategic plans.

Oversees information security and collaborates with privacy official efforts and provides direction for information security staff.

Encourages increased recognition of the role of information security systems, procedures, and analysis through the development and administration of enterprise-wide information security education and awareness programs.

Provides leadership, guidance, and assistance in information security systems analysis, reviewing all proposed revisions of systems and services to assure the security of the application, its economic justification, proper design, and suitability of security-related equipment.

Supports the mission of the Chief Privacy Officer to assure best practices are followed in the electronic storage and transmission of protected and sensitive information.

Coordinates development and maintenance of disaster recovery and business continuity security plans and procedures for the timely recovery of critical business functions.

Reviews all information security equipment, services, and personnel requisitions and recommends approval or disapproval.

Performs information security-related strategic and tactical planning, budget preparation, initiative and project planning.
Provides information security services to state agencies.

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES
Knowledge of current and emerging information technology systems, hardware, software and best practices.
Knowledge of management principles and supervisory techniques.
Knowledge of the principles and practices of the administration of state government, preferably West Virginia.
Ability to analyze administrative problems and to interpret and apply general policies in specific situations.
Ability to make decisions and assume responsibility for these decisions.
Ability to plan, organize, direct, and coordinate the work of others.
Ability to delegate authority, fix responsibility, and evaluate staff work.
Ability to plan and conduct a professional staff development program.
Ability to establish and maintain effective working relationships with a wide range of executive, departmental and public representative.

MINIMUM QUALIFICATIONS
Training:
Bachelor's degree from a regionally accredited four-year college or university and a CISSP certification.
Substitution:
Associate Degree from a regionally accredited college or university in information technology, information security, business administration, public administration, computer science/management, or related field, plus two years of supervisory experience in an information technology/security environment and CISSP certification may be substituted for the required training.
Experience:
Ten years of full-time or equivalent part-time paid experience including five years administrative or staff employment in government or in private industry at a management level in a capacity in which the individual worked with and gained extensive knowledge of the principles and practices of government. Three years of the required experience must have been in an administrative capacity involving information technology and information security responsibilities.
Substitution:
Graduate training in an appropriate field may be substituted for the required non-administrative experience on a year-for-year basis.

Establish: 7/21/05
Title Change: 10/22/2008, 11/21/2012
Revised: 1/04/2007, 10/22/2008, 11/21/2012
Effective: 11/21/2012