CLASS TITLE: CHIEF INFORMATION SECURITY OFFICER

Class Code: 02705700
Pay Grade: 38
EO: A

CLASS DEFINITION:

GENERAL STATEMENT OF DUTIES: Under administrative direction, performs highly responsible and complex administrative work directing the information technology (IT) security service functions of the state including all physical locations and digital systems such as voice, data, wireless networks and other similar applications, as well as, all technical security staff engaged in performing such activities; to be responsible for establishing, developing, implementing, and improving information security systems and functions across the enterprise and within the various state agencies for the purpose of promoting more effective and efficient security administration; to direct the development of security systems and procedures, and assure the maximum usage of information security systems, personnel, and equipment; to audit and control security policies and procedures to insure cost-effective use of enterprise information security resources to enable state agencies to carry out their appointed functions; and to do related work as required.

SUPERVISION RECEIVED: Works under the administrative direction of a superior with wide latitude for the exercise of initiative and independent judgment in network security development functions; work is subject to review upon completion for results obtained and conformance with agency policies and objectives.

SUPERVISION EXERCISED: Plans, coordinates, directs and reviews the work of IT security technical staff. As required, supervises private IT security specialists contracted by the state for specific projects.

ILLUSTRATIVE EXAMPLES OF WORK PERFORMED:

Under administrative direction, performs highly responsible and complex administrative work directing the information technology (IT) security service functions of the state including all physical locations and digital systems such as voice, data, wireless networks and other similar applications, as well as, all technical security staff engaged in performing such activities.

To be responsible for establishing, developing, implementing, and improving information security systems and functions across the enterprise and within the various state agencies for the purpose of promoting more effective and efficient security administration.

To direct the development of security systems and procedures, and assure the maximum usage of information security systems, personnel, and equipment; to audit and control security policies and procedures to insure cost-effective use of enterprise information security resources to enable state agencies to carry out their appointed functions.

To provide regulatory oversight for information technology to insure compliance with Federal and State laws, regulations, and guidelines, and sound IT security and privacy security.

To develop, implement and maintain all statewide information security standards, procedures, and guidelines, including compliance monitoring procedures.

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

To be responsible for establishing workload priorities, assigning tasks, and instructing and directing employees within the division and to ensure that all new technology projects are appropriately monitored for security risks and appropriate risk mitigation requirements are efficiently set forth and appropriately designed and delivered with the newly developed production system.

To develop work plans to assure efficient use of staff resources and to direct the development of IT plans to respond to the goals established by the department and division.

To directly conduct IT security vulnerability assessments and investigate any violation of security policy and report such violations to a superior.

To provide leadership, guidance, and assistance in information security systems analysis; to review 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.

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

To review all information security equipment, services, and personnel requisitions and to recommend approval or disapproval.

To establish annual objectives based upon the organization and analysis of resources in order to maximize the output of divisional goals and objectives and to ensure their efficiency and effectiveness.

To coordinate regular reviews of system and platform access and develop a risk-analysis and rating of all current and future systems and platforms.

To supervise staff and oversee vendors who safeguard the states assets, intellectual property and computer systems.

To ensure that operational requirements are conducive to effective business operations as reflected in the state’s security policy.

To maintain a common and uniform architecture for security protection to maximize interoperability of component agency information systems.

To develop training plans for staff to assure the necessary level of staff competency and backup for major applications.

To ensure the confidentiality of sensitive information processed by, stored in, and moved through information systems and applications.

To ensure the integrity of the information such that decisions and actions taken based upon the data processed by, stored in, and moved through information systems can be made with the assurance that the information has not been manipulated, the information is not subject to repudiation and the source of the changes to information can be verified.

To oversee the maintenance and updating of incident response plans.

To ensure the availability of information systems and applications during routine operations and in crisis situations.

To perform information security-related strategic and tactical planning, budget preparation, initiative and project planning.

To provide information security and privacy services to state agencies

To do related work as required.

REQUIRED QUALIFICATIONS FOR APPOINTMENT:

KNOWLEDGES, SKILLS AND CAPACITIES: A thorough knowledge of the principles, practices and procedures used in the development and direction of IT security systems and their design as it relates to the development, operation, and maintenance of automated systems; a thorough knowledge of current and emerging information technology systems, hardware, software and best practices; a thorough knowledge of management principles, practices, and techniques, including organization, structure, staffing patterns, and administrative control; a working knowledge of the principles and practices of the administration of state government and the ability to apply such knowledge in directing the state's information technology (IT) security service functions; the ability to provide comprehensive leadership in the area of IT system security to support the state's goals and objectives; the ability to analyze administrative problems and to interpret and apply general policies in specific situations; the ability to make decisions and assume responsibility for these decisions; the ability to plan, organize, direct, and coordinate the work of a staff; the ability to delegate authority, fix responsibility, and evaluate staff work; the ability to identify efficient uses of technology and analyze and evaluate the effectiveness of management information services and resources in direct relation to IT security systems; the ability to develop, manage, and make recommendations for the budgeting of cost-effective IT security solutions, acquisitions, and maintenance; the ability to establish effective relationships with agency senior staff, program officials, vendors, consultants, and representatives of other state departments and agencies; and related capacities and abilities.

EDUCATION AND EXPERIENCE:

Education: Such as may have been gained through: graduation from a college of recognized standing with Bachelor's Degree in Computer Information Systems, Computer Science; or a closely related information technology field; professional designation of Certified Protection Professional (CPP), Certified Information Systems Auditor (CISA) or Certification for the Information Systems Security Professional (CISSP) is preferred; and

Experience: Such as may have been gained through: a minimum of 7 years employment in a highly responsible management position with responsibility for directing an information technology security operation within a large federal agency, state department or in a large private organization including planning, coordinating, supervising and reviewing the work of professional and technical IT security staff.

Or, any combination of education and experience that shall be substantially equivalent to the above education and experience.

Class Created: March 19, 2006