STATE OF NEBRASKA CLASS SPECIFICATION EST: 02/08 – REV: 09/12
STATE INFORMATION SECURITY OFFICER CLASS CODE: G07620

DESCRIPTION: Under administrative direction, coordinates, facilitates, implements, and monitors the statewide information security program ensuring the security, integrity, and privacy of the State government enterprise-wide network and agency information networks; performs related work assigned.

DISTINGUISHING CHARACTERISTICS: (A position is assigned to this class based on the scope and level of work performed as outlined below.)

This is a single position classification where the incumbent works within the Office of the CIO. The position develops, recommends, implements, and monitors the effectiveness of information technology security policy and procedure at a state government enterprise-wide level. Serves as a liaison and resource for agency level staff assigned information security duties. Indirectly controls and manages information security policy and procedure where there may be divergent viewpoints among stakeholders.

EXAMPLES OF WORK: (A position may not be assigned all the duties listed, nor do the listed examples include all the duties that may be assigned.)

Serves as the information security expert for State Government enterprise-wide and agency information technology security issues such as policy questions, incident responses, education, and strategic planning. Facilitates and coordinates discussions with agency or political subdivision information technology staff and management relating to security policy and procedure to develop, execute, and review enterprise information security policies, procedures, standards, and guidelines.

Coordinates and conducts agency and enterprise-level information security risk assessments. Monitors State enterprise-level networks, hardware, and software for security vulnerabilities and breaches such as email traffic, firewall violations, unauthorized intrusions, SPAM, viruses, worms, Trojan horses, and policy violations. Confers with, coordinates, and advises outside consultants and vendors as appropriate for independent security audits.

Advocates for information security practices that protect the State's resources and assets against unauthorized modification, destruction, or disclosure. Coordinates and facilities information security workgroups, including working with individual agency staff who are delegated information security duties at the agency level.

Leads the Security Architecture Work Group for the State Government Council, and advises and represents the Nebraska Information Technology Commission (NITC) Technical Panel, and other NITC committees on security issues. Serves as Homeland Security information security point of contact. Notifies agencies when known breaches occur; serves as a resource and provides direction to agencies when breaches occur. Represents State government on National boards or organizations relating to security.

Oversees the investigation of security breaches and assists with law enforcement and legal matters associated with breaches as necessary. Assists in information recovery and architecture redesign following security breaches.

Coordinates and develops information security awareness and security training programs to promote information security awareness and best practices.

KNOWLEDGE, SKILLS, AND ABILITIES REQUIRED: (These are needed at entry level to perform the work assigned.)

Knowledge of: existing and emerging information technology; client relations; business methods; policy development; collaboration and facilitation techniques; computer operating systems; information systems and telecommunication systems and associated hardware and software; information security practices and procedures such as firewalls, intrusion detection devices, and encryption techniques; network administration practices; technical, security, operational, and policy aspects of information technology administration.

Skill in: active listening; active learning; analytical and critical thinking; influencing and communicating with others; solving complex problems; providing customer service; deductive and inductive reasoning; developing objectives and strategies; evaluating information against standards; identifying causal factors; identifying desired and undesired consequences; implementation planning; information organizing; exercising initiative and innovation; applying judgment and making decisions; oral and written comprehension and expression; planning and prioritizing action steps and goals; persuading others; providing consultation and advice to others; resolving conflict and negotiating with others; appraising solutions; conducting system evaluations; managing time.

Ability to: persuade others; facilitate groups of all levels; influence policy-making and administer, develop, and implement strategic plans within a large organization; interpret and apply state and federal laws, rules, and regulations, labor contracts, and agency rules and regulations; make sound technical, operational, and policy determinations; manage technical staff.

MINIMUM QUALIFICATIONS: (Applicants will be screened for possession of these qualifications. Applicants who need accommodation in the selection process should request this in advance.)

Bachelor's degree in computer science, information systems management, computer engineering, or a related technical field and ten years of recent progressively responsible experience with enterprise-wide information security technologies, information security methods, information security risk management practices, or information security programs. Additional years of experience in the fields described above may substitute for the required education on a year-for-year basis.

OR

Bachelor's degree in computer science, information systems management, computer engineering, or a related technical field, and five years of recent highly responsible experience managing an enterprise-wide information security program. Additional years of experience in the fields described above may substitute for the required education on a year-for-year basis.

SPECIAL NOTE:

State agencies are responsible to evaluate each of their positions to determine their individual overtime eligibility status as required by the Fair Labor Standards Act (FLSA).