MAJOR FUNCTION

The Information Systems Security Manager is responsible for the organization's Security Program including but not limited to daily operations of the information technology security program, oversight of the annual and ongoing risk assessment and penetration process, and maintenance of policies and procedures. The Information Systems Security Manager must identify organizational protection goals and objectives, ensuring they're consistent with the organizations' strategic plans. Work is performed with considerable independence and is reviewed through conferences and written reports for achievement of desired objectives.

ESSENTIAL AND OTHER IMPORTANT JOB DUTIES

Essential Duties

Plans, organizes, and implements security policies, procedures and processes. Builds a strategic and comprehensive information security program that defines, develops, maintains and implements policies and processes that enable consistent, effective information security practices which minimize risk and ensure the integrity, confidentiality and availability of information that is owned, controlled and processed within the organization. Establishes and maintains data security for computer systems. Ensures information security policies, standards, and procedures are up to date. Ensures that the disaster recovery, business continuity, risk management and access controls needs of the organization are addressed. Evaluates security trends, threats, risks and vulnerabilities and applies tools to mitigate risk as necessary. Responsible for periodic information security risk assessments, mitigation and remediation. Responsible for the development and implementation of a security risk management plan. Manages and responds to security incidents and events. Establishes and administers a process for investigating and acting on security incidents. Develops and coordinates initial and ongoing security training to the organization. Initiates, facilitates and promotes activities to foster information security awareness within the organization.

Other Important Duties

Initiates, facilitates, and promotes activities to foster information security awareness within the organization. Analyze a wide variety of highly technical materials and develop appropriate recommendations. Consult with and train other employees in best security practices/procedures. Perform related work as assigned and required.

DESIRABLE QUALIFICATIONS

Knowledge, Abilities and Skills

Thorough knowledge of security standards, processes, industry trends, principles and practices. Knowledge of modern security tools/software. Knowledge and experience in state and federal information security laws. Demonstrated skills in collaboration, teamwork, and problem-solving to achieve goals. Demonstrated skills in listening. Ability to communicate effectively, clearly, and concisely both verbally and written. A high level of integrity and trust.

Minimum Training and Experience

Possession of a bachelor’s degree in data processing, information systems, computer science, business or public administration, or a related field and three years of technical or professional experience that includes development and implementation of a security program and policies; or an equivalent combination of training and experience.

Necessary Special Requirements

Must possess a valid Class E State driver's license at the time of appointment.

This position includes a variety of responsibilities and requires a high degree of sensitivity to confidential matters. The selected applicant must successfully complete a criminal background check including fingerprints. Must obtain Criminal Justice Information Systems (CJIS) certification within 30 days of employment required.

Established: 11-02-15
Revised: 07-20-26