VIRGINIA BEACH CITY PUBLIC SCHOOLS
CHARTING THE COURSE

INFORMATION SECURITY MANAGER

GENERAL RESPONSIBILITIES

Under the leadership of the Chief Information Officer (CIO), the position is responsible for planning, developing, implementing and maintaining security programs, policies, and procedures that address risk and security requirements for the division.

ESSENTIAL TASKS

(These are intended only as illustrations of the various types of work performed. The omission of specific duties does not exclude them from the position if the work is similar, related, or a logical assignment to the position.)

- Provide leadership, direction and guidance in assessing and evaluating information security risks and monitor compliance with security standards and appropriate policies.
- Create the framework for information security governance and compliance in consultation with all the leadership team and other stakeholders
- Assist the CIO in the development of the budget and short and long-range goals and objectives, as required.
- Develop and maintain computer related policies and procedures; propose changes to existing policies and procedures to ensure operating efficiency and compliance.
- Perform risk assessments/audits and execute tests of data processing system to ensure functioning of data processing activities and security measures.
- Assess, evaluate and make recommendations to the CIO regarding the adequacy of the security controls.
- Develop disaster recovery/contingency plan and security plan; document computer security and emergency measures policies, procedures, and tests.
- Monitor and report on violations of computer security procedures; discuss enforcement procedures with the CIO to ensure violations are not repeated.
- Monitor, maintain and update virus protection software.
- Maintain Internet filtering software.
- Monitor Internet usage and firewall activity.
- Confer with users to discuss issues such as computer data access needs, security violations, and programming changes.
- Train users and promote security awareness to ensure system security and to improve server and network efficiency.
- Research, evaluate, design, test, recommend or plan the implementation of new or updated information security hardware or software; analyze its impact on the existing environment; provide technical and managerial expertise for the administration of security tools.
- Consult with Department of Technology (DOT) staff to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications and software.
- Coordinate and maintain software licensing agreements.
- Keep abreast of information security issues and regulatory changes.
- Engage in professional development to maintain continual growth in professional skills and knowledge essential to the position.
- Perform related work as required.

KNOWLEDGE, SKILLS AND ABILITIES

Thorough knowledge of microcomputer hardware and software and local and wide area networks; demonstrates an understanding of the job tasks and demonstrates good communication and human relations skills. Knowledge of business and management principles involved in strategic planning and leadership. Skilled in performing risk assessments and defining solutions and analyzing security requirements to develop appropriate controls. Must have the ability to work effectively with school officials, community groups, and other staff members; ensure that oral and written communications are clear, accurate, and grammatically correct; respect the confidential nature of professional information; submit reports accurately and punctually; and comply with administrative directives and school board policy; demonstrate good work habits to include punctual and regular attendance and efficient use of time; demonstrate self-control in interactions with the school community.

EDUCATION AND EXPERIENCE

Bachelor's Degree in Information Systems or equivalent with a minimum of 5 years of experience in computer related security required. A M.B.A. or M.S. in Information Security is preferred. Documented successful completion of a computer security course. Considerable experience in general computer operations and computer security (private or military sector) preferred.
A comparable amount of training and experience may be substituted for the minimum qualifications.

PHYSICAL REQUIREMENTS

Some standing, walking, moving, climbing, carrying, bending, kneeling, crawling, reaching, handling, pushing, and pulling. Ability to lift and carry items weighing up to fifty (50) pounds.
Reasonable accommodations may be made to enable individuals with disabilities to perform the essential tasks

SPECIAL REQUIREMENTS

Certified Information Systems Auditor (CISA) preferred.
Information Systems Audit and Control Association (ISACA).
Possession of a valid driver's license.

FLSA status: Exempt	Description: 12/2016