IT Deputy Chief of Information Security #03141
City of Virginia Beach – Job Description
Date of Last Revision: 03/21/2019

FLSA Status: Exempt  Pay Plan: Administrative  Grade: 20

City of Virginia Beach Organizational Mission & Values

The City of Virginia Beach exists to enhance the economic, educational, social and physical quality of the community and provide sustainable municipal services which are valued by its citizens. The City of Virginia Beach organization is based upon a belief in the democratic process of government. This belief provides meaningful ways for citizens, reflecting the diversity of our City, to contribute to the development of public policy. This process is enhanced by organizational values which guide member performance within the Virginia Beach Quality Service System. These Values define our desired organizational culture. We value quality customer service; teamwork; leadership and learning; integrity; commitment; and inclusion and diversity.

Summary Position Description

The work of the IT Deputy Chief positions emphasize the management, coordination and planning of all functions of a major organizational unit of the Information Technology Department. IT Deputy Chiefs have responsibility for activities that contribute to planning, creating and implementing an IT vision and strategy aligned with the City's strategic business plan within their area of assignment. In cooperation with the Chief Information Officer (CIO), they oversee the development of City IT standards, technology architecture, technology services and the strategic direction of IT. They manage teams of people responsible for developing and delivering IT solutions for the City and citizens.

IT Deputy Chiefs are also responsible for analyzing trends in technology, assessing the impact of emerging technologies on the business, providing solutions to address technology and business issues, and managing financial resources while ensuring the development of high-quality technology solutions.

Deputy Chief of Information Security (DCIS) is responsible for aligning security initiatives with enterprise programs and business objectives; ensuring that information assets and technologies are adequately protected. The DCIS's role is to identify, develop, implement and maintain a proactive security-related program with associated processes that reduce the organization's operational risks. The DCIS will oversee the City's Computer Security Incident Response Team. This division will be accountable for: establishing and implementing security-related policies; overseeing regulatory compliance; ensuring data privacy; securing identity and access management; establishing and overseeing the organization's security architecture; and conducting electronic discovery and digital forensic investigations.

The DCIS will work closely with high-level IT and City executives to establish disaster recovery (DR) and business continuity plans.

Job Functions

Plans, organizes, directs, and coordinates the activities of a major IT service area (multiple functional areas) of the Information Technology Department; provides leadership, direction, and guidance for development and operational activities to achieve the long and short range goals and business objectives.
Assists the CIO in formulating and implementing policies, programs, procedures, and standards for activities of the department.

Exercises considerable independent judgment to analyze, develop, and recommend plans and solutions to operational, management, business process, and utilizes effective leadership skills to implement such plans and recommendations.

In compliance with City policies, recruits, interviews, selects and evaluates staff; assigns and reviews projects to determine progress and work priorities; ensures adherence to standards and procedures; identifies, recommends and initiates training plans for staff within areas of assignment.

Directs managers, information technology staff, customer support teams, etc. to provide liaison with departments throughout the City to affect resolution of issues, accomplish work requests, and recommend viable technical improvements to business processes.

Coordinates and identifies objectives, plans, and methods to satisfy business requirements and negotiates service level agreements (SLA) in support of these requirements.

Develops budgets and recommends IT spending. Tracks budget and ensures that budgets are not exceeded. Oversees and provides high-level advice and counsel to the vendor relationship decision-making and contract development processes.

Identifies opportunities to develop and market systems that will enhance operational efficiencies and; evaluates and recommends new tools and methodologies that will expedite or enhance the development process.

Acts on behalf of the CIO in his/her absence as directed.

Perform other job duties requiring skills, knowledge and physical requirements as demanded by those duties described or less. Individual assignments will be determined by the supervisor based on then current workloads and department needs.

**Minimum Qualifications**

Bachelor's Degree in Computer Science, Information Technology, or related field; AND ten (10) years of progressively responsible professional experience providing architecture design and deployment, systems lifecycle management and infrastructure planning and operations, with at least three (3) years of leadership experience in managing multiple, large cross-functional teams or projects, and influencing senior level management and key stakeholders; OR an equivalent combination of education, training and experience.

Must have demonstrated experience managing teams and building relationships with people at a variety of levels and the ability to launch and deliver one or more IT project(s), process(s), or service(s) on time and within budget.

**Preferred Qualifications**

Master's degree in Computer Science, Information Systems, or closely related field. Entrepreneurial leadership experience, vision, and commitment to an organization with multiple diverse missions, programs, and service deliveries for the community. Professional certifications related to information security or privacy, network infrastructure, and VMware (SDN) that could include: Certified Information

This description is intended to indicate the kinds of tasks and levels of work difficulty that will be required of positions that will be given this title and shall not be construed as declaring what the specific duties and responsibilities of any particular position shall be. It is not intended to limit or in any way modify the right of any supervisor to assign, direct, and control the work of employees under his or her supervision. The use of a particular expression or illustration describing duties shall not be held to exclude other duties not mentioned that are of similar kind or level of difficulty.
Security Manager (CISM); Certified Information Systems Security Professional (CISSP); GIAC Security Leadership Certification (GLC); Global Information Assurance Certifications (GIAC); Certified Information Privacy Professional (CIPP); Cisco Certified Internetwork Expert Security (CCIE Security); VMware Certified Professional 6 – Network Virtualization (VCPE-NV); and/or Microsoft Certified Solutions Expert (MCSE).

**Special Requirements**
Alpha I Status: Positions within this class have been designated as Alpha I positions requiring employees to work during inclement weather, regardless of the City's operational status.

All employees may be expected to work hours in excess of their normally scheduled hours in response to short-term department needs and/or City-wide emergencies.

**Knowledge-Skills-Abilities Required to Perform Satisfactorily**

A. Knowledge
1. Knowledge and understanding of IT security program strategy and management
2. Expert Knowledge of IT Security policies, practices and regulations
3. Expert Knowledge of intrusion detection and intrusion prevention systems and practices
4. Knowledge of IT infrastructure to include networks, servers, and data centers, (on premise, cloud, and hybrid systems), etc.
5. Excellent knowledge and understanding of project management principles.
6. Advanced knowledge of systems networking, databases, application management, web development, and user support; in order to successfully execute security responsibilities
7. In-depth knowledge of multiple enterprise-wide complex systems and operations and the integration of those systems to maximize the efficiency and effectiveness of businesses, services, and operations in a conglomerate-like environment
8. In-depth knowledge of applicable laws and regulations as they relate to technology issues
9. Working knowledge of business theory, business processes, management, budgeting, and business office operations
10. Knowledge of IT industry standard metrics, reporting and analysis necessary to demonstrate service value, service reliability, and to support service change recommendations

B. Skills
1. Skill in analyzing IT system designs for security vulnerabilities and to correct the designs to support the IT security strategy
2. Skill in analyzing complex security logs, incidents, threats, and data to project vulnerabilities, determine risk of occurrence, identify cost / benefit of corrective action(s), and implement mitigation program
3. Skill in leading IT Incident Response Teams and building rapid incident identification, source, mitigation, and recovery protocols
4. Skill in defining functional priorities and balancing resources to ensure critical business projects are delivered while maintaining a high level of ongoing IT support to customers
5. Skill in developing, implementing and ensuring compliance to IT Operation's policies, standards, and procedures
6. Skill in analyzing metrics and reports to communicate service value, service reliability, and to make service change recommendations
7. Skill in researching, analyzing and evaluating advanced technologies to address evolving business needs and changing requirements
8. Skill in ensure IT solutions meet organizational needs and are scalable

This description is intended to indicate the kinds of tasks and levels of work difficulty that will be required of positions that will be given this title and shall not be construed as declaring what the specific duties and responsibilities of any particular position shall be. It is not intended to limit or in any way modify the right of any supervisor to assign, direct, and control the work of employees under his or her supervision. The use of a particular expression or illustration describing duties shall not be held to exclude other duties not mentioned that are of similar kind or level of difficulty.
9. Skill in developing proactive solutions with a holistic plan that supports the current business and will enable future growth
10. Strong tactical skills.
11. Excellent interpersonal skills.

C. Abilities
1. Ability to communicate IT Security Risk and mitigation plans to executive level organizational and/or customer groups
2. Ability to create and manage an enterprise IT security strategy and program
3. Ability to conduct and/or oversee a enterprise level Security Risk Assessment/Audit and its resulting mitigation plan
4. Ability to assist IT architects in finalizing and adapting enterprise architecture standards as it relates to IT security
5. Proven leadership ability
6. Demonstrated ability to interact effectively with all levels of decision makers
7. Ability to set and manage priorities judiciously
8. Excellent verbal and written communications abilities including presentation facilitation
9. Ability to articulate ideas to both technical and non-technical addressees
10. Demonstrated ability in self-motivation and self-direction
11. Keen ability in attention to detail
12. Superior analytical, evaluative, and problem-solving abilities
13. Exceptional service orientation ability
14. Ability to motivate in a team-oriented, collaborative environment
15. Ability to design, implement, and manage best in class Cybersecurity Programs

Working Conditions
The below stated working conditions are intended to provide a general overview of the environmental conditions inherent in the job setting, as well as the physical, mental, and sensory requirements necessary to perform the essential functions of positions in the noted job title. A more detailed description will be made available at the position (PCN) level.

NOTE: Per HR Policy 6.19, Americans with Disabilities, the City follows the requirements of the Americans with Disabilities Act (ADA) in all hiring and employment decisions. The City shall not discriminate on the basis of disability in its hiring and employment practices. The City shall make reasonable accommodations for the known physical or mental limitations of a qualified applicant or employee with a disability upon request unless the accommodation would cause an undue hardship on the operation of the City’s business.

Physical Requirements: Physical refers to the requirement for physical exertion and coordination of limb and body movement.
Requires sedentary work that involves walking or standing some of the time and involves exerting up to 10 pounds of force on a regular and recurring basis and routine keyboard operations.

Mental Requirements: Mental refers to the degree that the job involves cognitive activities, and use of mental processes
Performs advanced professional level work in the analysis or interpretation of methods of a scientific, engineering, fiscal, legal, or other nature and formulates recommendations on the basis of such analysis; applies creativity and resourcefulness in the analysis and solution of complex problems; requires sustained, intense concentration for accurate results or continuous exposure to unusual pressure.
**Environmental Conditions:** Environmental refers to job conditions inherent to the job setting, including those that may lead to injury or health hazards even though precautions have been taken. This job involves a risk of limited to no exposure to any environmental hazards.

**Sensory Requirements:** Sensory refers to hearing, sight, touch, taste, and smell required by the job. The job requires normal visual acuity, and field of vision, hearing and speaking.