CITY OF HOUSTON

JOB DESCRIPTION

Job Code: 457.5

Job Title: **IT EXPERT - SECURITY**

Pay Grade: 33

GENERAL SUMMARY:

The purpose of this position is to function as technical expert and platform strategist for specific IT security systems or applications. This individual contributor is a position that is very highly specialized; may be nationally recognized as a leader in the specialized field and may speak at industry forums; contributes to the body of knowledge within a particular area of expertise. Represents the highest level of technical knowledge in a specialized field; usually reserved for a single individual within a particular area of expertise.

RESPONSIBILITIES:

TECHNICAL EXPERT: Preeminent technical expertise with multiple technical certifications. Proactively resolves highly complex IT security operational problems by providing deep technical expertise, such as the ability to reverse engineer malware, perform extensive digital forensics, perform incident triage to include determining scope, urgency, and potential impact; and make recommendations that enable expeditious remediation; perform analysis of SIEM data from a variety of sources to identify trends and possible threats to IT security. Serves as the highest level of specialized technical expertise internally.

STRATEGY: Directs strategy for IT security system architecture, design, and platform evolution using current and emerging technologies. Develops counter-measures and defense-in-depth solutions to emerging threats. Evaluates and recommends new products, and maintains knowledge of emerging policy or regulatory requirements. Drives innovation and strategic solutions by providing value propositions; adapts plans and priorities to address business requirements and long-term platform requirements. Serves as liaison between senior leadership, project teams, development teams and other stakeholders to discuss IT security risks to business processes, systems and data.

SYSTEMS ANALYSIS & PROGRAMMING: Performs complex analysis of data and events from a variety of sources, including correlation and anomaly rules. Provides guidance and instruction on daily use of the SIEM and other security tools to the Incident Response Team and other security and operational personnel. Identifies potential intrusions, and provides highly specialized support in mission critical troubleshooting or design activities. Plans and recommends security architecture and platform evolution. Approves and modifies application design and architecture to ensure compliance. Monitors overall operational security health, and is proactive in assessing and making recommendations for improvement.

TEAM EFFORT: Contributes to team effort by accomplishing business results through proactive strategy, planning, and deep technical expertise for highly specialized technical systems.

SPECIFICATIONS:

KNOWLEDGE: Bachelor's degree in Computer Science, Management and Information Systems (MIS), Engineering or a related field.

EXPERIENCE: At least 4 years of progressively responsible IT experience, two (2) years of which must have included progressively specialized IT security responsibilities.

COMPLEXITY: Individual contributor and acknowledged expert in IT security. Works independently; routinely coaches other professionals on technical issues. Ability to execute highly complex or specialized projects; develops new solutions to complex problems.

IMPACT OF ACTIONS: Errors in work typically lead to significant business risks and costs. The incumbent functions autonomously and as an advisor to senior business and technical leadership. Ability to pass and maintain federal security clearances may be required.

SUPERVISION EXERCISED: No direct report employees. No indirect reports.

Direct Supervision:

Indirect Supervision:

CONTACTS:

Internal Contacts: Level of internal contact is primarily with managers, Assistant Directors, and Deputy Directors. Interaction involves considerable explanation and persuasion leading to decision, agreement or rejection on complex issues; diplomacy is required; problem-solving discussions regarding responsibilities, finance or work flow or to facilitate change.

External Contacts: Level of external contact is primarily with senior-level representatives of government agencies, guests, vendors and professional contacts with affiliated organizations. Interaction requires substantial sensitivity and persuasion leading to resolution of complex issues, e.g., project coordination and higher-level problem resolution

PHYSICAL EFFORT: The position is physically comfortable; the individual has discretion about walking, standing, etc. Operates a motor vehicle.

WORK ENVIRONMENT: There are no major sources of discomfort, i.e., essentially normal office environment with acceptable lighting, temperature and air conditions. Significant time spent using computer display, keyboard, and mouse.

PHYSICAL SKILL: Requires the ability to make closely coordinated eye/hand movements within very fine tolerance and/or calibration demands. Operates a motor vehicle.

MISCELLANEOUS: Performs related work as required.

JOB FAMILY: Information Technology – IT Security

Technical Track:	**Management Track:**
IT Intern	--
IT Associate – IT Security	--
IT Specialist – IT Security	--
IT Professional – IT Security	IT Lead -- IT Security
IT Sr. Professional – IT Security	IT Manager -- IT Security
IT Security Professional – Expert	Information Security Officer (ISO)
--	Chief Information Security Officer (CISO)

Effective: November 4, 2015
Revised: June 9, 2017