CITY OF HOUSTON

JOB DESCRIPTION

Job Code: 457.7

Job Title: **IT MANAGER - SECURITY**

Pay Grade: 32

GENERAL SUMMARY:

The purpose of this position is to manage compliance with IT security plans, policies, and operational procedures. Promotes and supports the city's IT security framework to *identify* the IT assets and data that must be protected, *detect* cyber incidents, *protect* IT assets from intentional or unintentional compromise or destruction, *respond* and *recover* from cyber incidents.

RESPONSIBILITIES:

MANAGEMENT: Accomplishes staff results by communicating job expectations; planning, monitoring, and appraising job results; coaching, mentoring, and disciplining team members; developing, coordinating and enforcing systems, policies, procedures, and productivity standards. Maintains high performing staff by recruiting, selecting, orienting, and training team members; maintaining a safe, secure, and discrimination-free work environment; developing personal growth opportunities. Accomplishes financial objectives by forecasting requirements; preparing an annual budget; scheduling expenditures; analyzing variances; initiating corrective action for variances. Establishes strategic goals that support organizational objectives by gathering pertinent business, financial, service, and operations information; identifying and evaluating trends and options; choosing a course of action; defining objectives; evaluating outcomes.

OPERATIONS: Manages the development and delivery of IT security standards, best practices, architecture and systems to ensure information system security across one or more departments. Implements processes and methods for auditing and addressing non-compliance to information security standards; facilitates migration of non-compliant environments to compliant environments. Conducts studies within and outside the organization to ensure compliance with standards and currency with industry security norms. Manages and participates in the planning and implementation of security administration for all IT projects. Responsible for evaluation and selection of security applications and systems. Makes recommendations and assists in the implementation of changes to work methods and procedures to make them more effective or to strengthen security measures. Safeguards IT assets by monitoring tools that detect security vulnerabilities and incidents. Manages incident response and business continuity procedures to respond and recover from IT security incidents.

CUSTOMER SERVICE: Functions as business partner; builds business relationships with stakeholder representatives and frequently interacts with to discuss IT security risks, incident response, policies, controls and training. Aligns IT security operational tasks to the priorities established by the business stakeholders. Analyzes KPI's to maintain quality standards for IT security service delivery.

TEAM EFFORT: Contributes to team effort by accomplishing related results and performing related responsibilities as needed.

SPECIFICATIONS:

KNOWLEDGE:
Bachelor's degree in Computer Science, Management and Information Systems (MIS), Business or a related field. Requires CISM, CISSP, or equivalent broad security certification.

EXPERIENCE: At least 3 years of technology experience implementing IT Security plans and controls of a department or enterprise IT environment that includes two (2) years supervising a technology team.

COMPLEXITY: Work is non-standardized, complex and varied, and requires interpretation of technical and detailed guidelines, policies and procedures in combination. Advanced analytic ability is needed to gather and interpret data where answers can be found only after detailed analysis of many facts.

IMPACT OF ACTIONS: Errors in work lead to significant costs and problems, and may have minor impact on the short- term performance of the department. The incumbent generally receives general direction, working from broad goals and policies only. The individual may participate heavily in setting his/her own work objectives. Ability to pass and maintain federal security clearances may be required.

SUPERVISION EXERCISED:

Direct Supervision: Involves scheduling, supervision and evaluation of work, recommends personnel actions, such as hiring, terminations, pay changes of non-supervisory personnel.

Indirect Supervision: May include two or more indirect reports. May involve supervision and evaluation of work as a division manager or the equivalent.

CONTACTS:

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

External Contacts: Level of external contact is primarily with prominent persons such as community leaders, business and industry leaders as well as officials of government and financial agencies, media representatives and professional contacts with affiliated organizations. Interaction involves considerable explanation and persuasion leading to decision, agreement or rejection on complex issues that requires diplomacy; e.g., important contacts involving difficult matters of agreements, negotiations and controversies.

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. Ability to pass and maintain federal security clearances.

PHYSICAL SKILL: Requires the ability to make coordinated gross motor movements in response to changing external stimuli within minor demanding tolerances; or the ability to make simple eye/hand movements on a patterned response space within very low tolerance demands.

MISCELLANEOUS: Performs related work as required.

JOB FAMILY: Information Technology – Security

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

Effective: November 4, 2015
Revised September 2017