CITY OF HOUSTON

JOB DESCRIPTION

Job Code: 457.8

Job Title: **INFORMATION SECURITY OFFICER (ISO) (EXE LVL)**

Pay Grade: 34

GENERAL SUMMARY:

The purpose of this position is to develop the IT security strategy, policy and operational procedures for one or more city departments. Advises department leadership regarding cyber-security related vulnerabilities, and facilitates business-focused evaluation and prioritization of risks.

RESPONSIBILITIES:

STRATEGY: May participate in development of overall business strategy for the department or enterprise. Develops department IT security strategy and business plan. Translates risk mitigation requirements into projects and operating procedures.

MANAGEMENT: Accomplishes business results by aligning technical staff goals to business plan objectives. Generally manages other managers or senior technical professionals. Communicates job expectations; plans, monitors, and appraises job results; coaches, mentors, and disciplines team members; develops, coordinates and enforces systems, policies, procedures, and productivity standards. Maintains high performing staff by recruiting, selecting, orienting, and training team members; maintains a safe, secure, and discrimination-free work environment; develops personal growth opportunities. Develops key performance indicators (KPI's) to measure effectiveness of IT security program.

OPERATIONS: Facilitates the development and delivery of IT security plans, standards, procedures, architecture and system requirements to protect city systems and data from unauthorized access. Ensures department compliance with COH Executive Orders, Administrative Procedures, and department information security policies and procedures. Facilitate information systems security assessments. Manages Governance, Risk & Compliance and other assessment tools to document reported security weaknesses. Actively works with information system owners to ensure that the weaknesses and deficiencies are corrected and the vulnerabilities are mitigated. Leads cross-functional incident response teams to remediate IT security breaches and document lessons learned. Leads cross-functional vulnerability management teams identify and implement appropriate controls and countermeasures to maintain acceptable risk tolerance levels.

CUSTOMER SERVICE: Functions as business partner; builds business relationships with stakeholder representatives and frequently interacts with to discuss technology services and assess customer satisfaction.

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

SPECIFICATIONS:

KNOWLEDGE: B.A. or B.S. degree in Management and Information Systems (MIS), Computer Science, Engineering or a closely related field.

EXPERIENCE: At least 5 years of experience implementing IT Security plans and controls of a department or enterprise IT environment that includes three (3) years managing a technology team. Strong understanding of the department's core business functions and business strategy.

COMPLEXITY: Work is non-standardized, highly 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, and acts as an advisor to senior business leaders and CIO /Deputy CIO / CTO. 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 management and senior technical personnel.

Indirect Supervision: Often manages indirect reports associated with multi-discipline project teams and consultants.

CONTACTS:

Internal Contacts: Level of internal contact is primarily with Managers, Assistant Directors, Deputy Directors, and occasionally Department 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 – IT Security

Technical Track:
IT Intern
IT Associate – IT Security
IT Specialist – IT Security
IT Professional – IT Security
IT Sr. Professional – IT Security
IT Security Professional – Expert
--

Management Track:
--
--
--
IT Lead -- IT Security
IT Manager -- IT Security
Information Security Officer (ISO)
Chief Information Security Officer (CISO)

Effective: November 2015
Revised: February 2016
Revised: June 9, 2017
Revised May 2019