



CITY OF HOUSTON

JOB DESCRIPTION

Job Code: 457.6

Job Title: **IT LEAD – SECURITY**

Pay Grade: 30

GENERAL SUMMARY:

The purpose of this position is to lead a team of IT security personnel responsible one or more functional areas within the IT Security group. Leads day-to-day operations, organizes and monitors work processes, and deploys resources; provides technical support and direction.

RESPONSIBILITIES:

SUPERVISION: Functions as technical lead with limited supervisory responsibilities. Plans, organizes and assigns work for the team. Accomplishes staff results by communicating job expectations and providing technical guidance; coaching, mentoring. Provides input to manager regarding team member performance evaluations and disciplinary action. Contributes to the development of policies, procedures, and productivity standards. Assists manager with recruiting, selecting, orienting, and training team members; maintains a safe, secure, and discrimination-free work environment; developing team member personal growth opportunities. Establishes team 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: Completes operations by developing team schedules, assigning and monitoring work; gathering resources; analyzes KPI's; analyzes security threat data; resolves operational problems; maintaining reference on-line manuals and implements new procedures and processes. Controls expenditures by gathering and submitting budget information; schedules expenditures; monitoring variances; implementing corrective actions. Delivers high performance by enforcing performance, quality, and customer service standards.

CUSTOMER SERVICE: Maintains customer service standard by monitoring impact of IT security incidents, as well as business impact related to IT security policies or controls.

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

SPECIFICATIONS:

KNOWLEDGE:

Associate's degree in Computer Science, Management and Information Systems (MIS), Business or a related field. System-specific technical certifications may be considered a substitution for Associate's degree. CISM, CISSP, or equivalent broad security certifications may be considered for substitution of up to two (2) years of the education requirement.

Experience in IT security, infrastructure or applications may be substituted for the education requirement on a year-for-year basis.

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

COMPLEXITY: Team leader that is fully proficient in applying established standards; knowledge base acquired from several years of experience in a particular area. Coaches team members on technical issues as well as training, interpersonal skills, decision making, problem resolution, career development, etc. Ability to execute moderately complex or specialized projects; adopts precedent and may make significant departures from traditional approaches to develop solutions. Security system or application specific technical training and/or certifications will often be required (post-hire).

IMPACT OF ACTIONS: Errors in work typically lead to moderate inconvenience, risk and costs. The incumbent functions autonomously on technical matters, but relies on manager for final approval of personnel-related matters for the team. Ability to pass and maintain federal security clearances may be required.

SUPERVISION EXERCISED:

Direct Supervision: Involves scheduling, limited supervision and evaluation of team and individual performance. Makes recommendations to manager regarding personnel actions such as team member performance evaluations, hiring, terminations, disciplinary action, and pay changes of non-supervisory team members.

Indirect Supervision: No indirect reports.

CONTACTS:

Internal Contacts: Level of internal contact is primarily with professionals, managers and Assistant Directors. Interaction requires substantial sensitivity and cooperation; e.g., basic project interaction.

External Contacts: Level of external contact is primarily with citizens, visitors and/or mid-level representatives of government agencies, guests, vendors and professional contacts with allied organizations. Interaction requires substantial sensitivity and cooperation; e.g., lower-level problem resolution, providing information to citizens who from time to time may be irate.

PHYSICAL EFFORT: There are occasional minor discomforts from exposure to less-than-optimal temperature and air conditions. The position may involve dealing with modestly unpleasant situations, as with occasional exposure to office chemicals and/or extensive use of a video display terminal

WORK ENVIRONMENT: There are no major sources of discomfort, i.e., essentially normal office environment with acceptable lighting, temperature and air conditions. Skilled technician in a hands-on environment and may have on-call responsibilities and rotating shifts. Ability to pass and maintain federal security clearances.

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 – Security

Technical Track:

IT Intern
IT Associate – Security
IT Specialist – Security
IT Professional – Security
IT Sr. Professional – Security
Information Security Professional – Expert
--

Management Track:

--
--
--
IT Lead -- Security
IT Manager -- Security
Information Security Officer
Chief Information Security Officer

Effective: November 4, 2015

Revised: June 9, 2017

|