CHIEF INFORMATION SECURITY OFFICER

JOB DESCRIPTION

Classification Responsibilities: The Chief Information Security Officer (CISO) assists the Chief Information Officer in overseeing information risk management for the organization. The CISO is responsible for establishing and maintaining the enterprise vision, strategy, and security program to ensure information assets and technologies are adequately protected. The CISO directs staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and Information Technology (IT) risks. Duties include: managing the development, implementation, and maintenance of the City's information security and privacy policies, standards, guidelines, baselines, processes, and procedures in compliance with state and federal regulations and standards; developing and leading the City's incident response and investigation procedures and processes; assisting in the development of disaster recovery and business continuity plans and procedures; serving as a member of the leadership team and communicating security related concepts to a broad range of technical and non-technical employees; overseeing the City's Information Security Program; monitoring and reporting on information security activities and compliance across all City departments; performing security assessments on the acquisitions of technology products, tools, and services; providing guidance and advocacy of security issues regarding prioritization of infrastructure investments that impact information security; monitoring information security trends and keeping the City's senior management informed about security related issues and activities affecting the City of Mesa; understanding potential threats, vulnerability, and control techniques; serving as liaison to local, state, and federal law enforcement and other related government agencies on information security related issues; and developing and administering a Citywide information security training and awareness program. The CISO also responds to security incidents, establishes appropriate standards and controls, manages security technologies, directs the establishment and implementation of security policies and procedures, maintains information-related compliance, and performs related duties as required.

Distinguishing Features: This classification has been designated as a non-classified, non-merit system, at-will position. Excellent communication skills are essential in dealing with both internal and external parties. Incumbents must possess sufficient communication skills and business and technical knowledge in order to communicate meanings and impact using both business and technical terminology. Incumbents work independently and with initiative in performing day-to-day responsibilities to meet the continuous demands associated with the completion of simultaneous projects and requests for a variety of resources. Work is performed under the general direction of the Chief Information Officer, but considerable freedom is given to exercise independent judgment and initiative. Employees in this class are required to be available on a 24-hour basis to cover emergency situations. This class is FLSA exempt-administrative.

QUALIFICATIONS

Employee Values: All employees of the City of Mesa are expected to uphold and exhibit the City's shared employee values of Knowledge, Respect, and Integrity.

Minimum Qualifications Required. Any combination of training, education, and experience equivalent to graduation from an accredited college or university with a Bachelor's Degree. Extensive (5+ years) of progressively responsible

professional experience in information security and privacy for a large enterprise. Considerable (3 – 5 years) experience in managing and/or supervising staff.

Special Requirements. Must possess a valid Class D Arizona Driver's License by hire date. For this position, an individual receiving a conditional offer of employment from the City of Mesa must pass a background investigation through the City of Mesa Police Department, the Arizona Department of Public Safety, and Federal Bureau of Investigation prior to commencing employment with the City of Mesa.

Substance Abuse Testing. None.

Preferred/Desirable Qualifications. Graduation from an accredited college or university with a Master's Degree in Computer Science, Information Systems, or a related field is preferred. Experience with presentations, project management, team facilitation, budgeting, and training are highly desirable. Experience or training in customer service techniques is also desirable. Certified Information Systems Security Professional (CISSP) or other related security accreditation/certification is highly desirable.

ESSENTIAL FUNCTIONS

Communication: Communicates with the general public, other City employees, vendors, management, contractors and public officials in order to reduce information and information technology risks. Serves as the City's designated Security Officer. Establishes an information security program, systems, policies and procedures and advises senior management regarding technology risks. Instructs and trains subordinates and City staff on information security and awareness. Prepares written documents, including reports, memos, forms, manuals, etc., with clearly organized thoughts and using proper sentence construction and grammar.

Manual/Physical: Operates a motor vehicle requiring a standard Arizona Driver's License to travel to various locations to attend meetings, conferences, and seminars to discuss and share cyber information. Ensures services are delivered in a secure and efficient manner. Operates a variety of standard office equipment such as a personal computer (PC), printer, copier, and telephone. Meets scheduling and attendance requirements.

Mental: Plans, organizes, and directs the activities of the security group. Develops and monitors section budget and determines which programs take priority. Conducts research and analyzes data to monitor and report on information security activities and compliance across the City. Resolves procedural, operational, and other work-related problems related to area of responsibility. Coordinates work activities, program functions with other City departments, and cities and agencies related to cyber/information security. Develops departmental policies and procedures and short and long-term objectives for the City's cybersecurity program. Supervises, assigns, and evaluates the work of subordinate personnel.

Knowledge and Abilities:

Knowledge of:

security principles and practices;
safeguards, building secure systems and security procedures for information systems;
City of Mesa organization, corporate/industry security information, goals, objectives, and policies and procedures;
laws and regulations related to Health Insurance Portability Accountability Act (HIPAA), Gramm-Leach Bliley (GLB) Act, Communications Assistance for Law Enforcement Act (CALEA), and Payment Card Industry (PCI);
current and developing information technology services, industry information technology, impact on processes, business continuity planning, auditing, and risk management requirements in a large organization;
vendor and contract negotiations;
general functions of City departments, including departmental needs and requirements;
laws, policies, and regulations governing the purchase of commodities and services for the City; and
principles, practices, and procedures of employee supervision, including hiring, evaluating, and training.

Ability to:

evaluate and resolve security related problems and issues;
effectively communicate with a wide range of individuals and constituencies in a diverse community;
present information both orally and in writing;
effectively present information and respond to questions from top management, groups of managers, clients, customers, and the general public;
communicate with individuals and groups in a face-to-face, one-on-one setting, or by telephone on technical and nontechnical issues;
analyze and evaluate feasibility and suitability of division projects;
produce technical and nontechnical written documents with clearly organized thoughts using proper sentence construction, punctuation, and grammar;
exercise a broad range of supervisory responsibility over others;
coordinate work assignments;
comprehend and make references from written material;
explain complicated and technical information in simple, non-technical language;
negotiate and facilitate conflict resolutions;
develop policies and strategic plans for immediate and future security needs in Information Technology;
direct and assess security risk and vulnerability testing of networks, operating systems, and applications and associated databases;
understand and apply state-of-the-art security technologies in computer systems, networking, and telecommunication to the needs of a complex organization with multiple locations and large number of users of enterprise applications; and
establish and maintain effective working relationships with staff, management, and the general public.

The duties listed above are intended only as general illustrations of the various types of work that may be performed. Specific statements of duties not included does not exclude them from the position if the work is similar, related, or a logical assignment to the position. Job descriptions are subject to change by the City as the needs of the City and requirements of the job change.

Revised 3/20
NF/co/kc
CS5912
EEO-O/A
JOB FCTN-INT
INCREMENTS 5-200

PAY GRADE 61
IND-9410
SWORN-No