



Salt Lake County Job Description

Associate Division Director, Information Security Officer

DEPARTMENT: Administrative Services

DIVISION: Information Services/6050

JOB CODE: 221 **GRADE:** 22

FLSA STATUS: Exempt

SALARY PLAN: TRD

EFFECTIVE DATE: 12/6/2016

SAFETY SENSITIVE No

JOB SUMMARY

Manages the design, development, implementation, operation and maintenance of Salt Lake County's Information Technology (IT) security programs. Designs a comprehensive security program, an accountable culture, and a security infrastructure. Provides countywide strategic and operational IT leadership.

MINIMUM QUALIFICATIONS

Bachelor's degree from an accredited college or university in Information Technology field or business, or other closely related field, plus eight (8) years of related experience, of which two (2) years must have been supervisory or administrative; OR an equivalent combination of related education and experience. Education may not be substituted for the required supervisory experience.

Professional certification in Information Systems Security Professional (CISSP) and/or Certified Information Security Manager (CISM) preferred.

Due to the nature of this position, the successful applicant must pass a required pre-employment background check and subsequent mandatory background checks in accordance with current County Human Resources policy requirements.

ESSENTIAL FUNCTIONS

The following duties and responsibilities are intended to be representative of the work performed by the incumbent(s) in this position and are not all-inclusive. The omission of specific duties and responsibilities will not preclude it from the position.

Applicants must be prepared to demonstrate the ability to perform the essential functions of the job with or without a reasonable accommodation.

- Stays current with technical knowledge in information systems, uses appropriate security controls and methods.
- Directs the preparation of Information Security plans, short-term and long-term strategies for the IT organization and the County as a whole.
- Develops, manages and integrates IT security and privacy related programs designed to protect the County's systems, applications and data.
- Identifies security issues, their impact on the IT organization and the County and executes successful solutions while tracking and achieving measurable results.
- Formulates and promotes all IT security policies, processes, procedures and best practices.

- Establishes and maintains positive business relationships with managers countywide to actively market and educate them on importance of User community cooperation and compliance.
- Designs, develops and implements a countywide information security awareness program for the County's employees.
- Designs, develops, and implements information security systems and controls.
- Documents processes and monitoring systems that report on the effectiveness of said systems and controls necessary to protect the County's information technology systems, assets, and interests.
- Monitors compliance with the organization's information security policies and procedures among employees, contractors, partners, and other third parties and resolves potential issues as needed.
- Performs information security risk assessments and serves as information security consultant to the IT organization and countywide customers.
- Manages the response to information security incidents and follows up to ensure that proper protection and corrective measures have been successfully taken.
- Manages forensic investigations and audits, and leads a team of forensics investigators to document root cause and create effective solutions to eradicate security breaches.
- Exercises strong organizational and team leadership skills to achieve interdepartmental compliance and to ensure that departmental information security staff adopts and fully integrates appropriate security and privacy practices.
- Manages the IT disaster recovery plan (IT DRP) including assigning tasks across the IT organization in the event of a disaster in order to restore all systems, programs, hardware, software applications and data in time to meet the needs of the County's business recovery.
- Represents the County's information security interests to State and Federal agencies and regulatory bodies.
- Designs and implements the security controls for systems that process credit card and health data.
- Works with budget committee to identify annual operational and capital budgets for assigned group and the IT organization as a whole. Matches appropriations for specific programs with appropriations for broader programs, including items for emergency funds.
- Develops IT cost metrics for budgeting and employee headcount analysis, current and projected.
- Prepares projections on IT capital budget and monitors expenditure levels.
- Evaluates IT key performance indicators. Analyzes monthly department budgeting and accounting reports to maintain expenditure.
- Leads and influences peers, customers and staff in executing the goals of the County.
- Fosters an innovative, collaborative, success-oriented team environment.
- Develops and maintains effective working relationships with customers, vendors, peers, subordinates, support personnel and team members.
- Manages, directs, and coordinates activities through managers and supervisors, which includes hiring, firing, promoting, orienting, training, assigning and reviewing work performance, annual work performance appraisal and discipline.
- Encourages innovation while weighing cost against benefit of information technology investments.
- Oversees PCI-DSS, HIPAA and other compliance.

KNOWLEDGE, SKILLS AND ABILITIES (KSA)

Knowledge of:

- Security concepts, principles and best practices for voice and data networks; applications and architecture; design and testing; hosting and cloud based services; Internet/Intranet technology and mobile devices
- Information security architecture, information security technologies, tools, practices and controls
- Operations, services, concepts, terms and activities common to a comprehensive, state-of-the-art information systems security program and current regulatory requirements

- Current and emerging security technologies including by not limited to: Firewalls (Fortinet, Cisco), Remote Access (Juniper, Net Motion), Email Security (Cisco, IronPort), Encryption (Dell Data, Credent), Vulnerability (Rapid 7 Nexpose and Tenable/Nessus), Traffic Management (F5 BIG-IP), Security Event Information Management (Nitro Security, Intel, ARCSight), End Point Security (IBM BigFix, Tivoli Endpoint Manager), Authentication (Active Directory, FortiNet, OpenLDAP), Anti-Virus, Citrix Xenapp Hosting
- Methods and techniques of evaluating information security and developing appropriate resolutions
- Project management principles and techniques including project budgeting, quality assessment and control, and resource management
- Organizing and prioritizing projects and work assignments and review, establish, and maintain project schedules

Skills and Abilities to:

- Communicate effectively both verbally and in writing
- Ensure IT requirements are in compliance and support customer specific needs, countywide policy, standards, infrastructure, business processes, and state and federal mandates
- Establish and maintain effective partnerships, through collaboration and teamwork, to assure effective use of information technology in support of the County's business needs
- Develop clear requirements for internal information technology staff and third-party vendors
- Implement and then act as an advocate for best practices and technology awareness
- Lead the IT organization where change is frequent and the demand for effective technological solutions is high
- Market new concepts and champion change
- Produce results within a large, decentralized organization
- Effectively analyze and solve problems under pressure
- Exercise professionalism, discretion and confidentiality in all matters

WORKING CONDITIONS AND PHYSICAL REQUIREMENTS

IMPORTANT INFORMATION REGARDING THIS POSITION

May be required to work holidays, nights, and weekends as needed.

Revised Date/Consultant's Initials: 12/2/2016/HA