CITY OF ROSEVILLE

SECURITY ARCHITECT

DEFINITION

To perform a variety of high-level professional, technical, and analytical project management duties involving the design, development, testing, implementation, evaluation, administration, troubleshooting and management of security systems and solutions; and to perform advanced level threat detection and prevention, education, risk assessment, compliance, governance, business recovery, forensics and incident response.

DISTINGUISHING CHARACTERISTICS

The Security Architect is the advanced journey level in the Security Analyst class series. Positions at this level are distinguished from other classes within the series by the provision of the highest level of technical expertise and knowledge in the performance of duties. Incumbents are the recognized experts in their field including possessing extensive experience designing and architecting complex information technology and security solutions, as well as demonstrating successful technical project management and by the advanced level of knowledge and experience required. Positions do not provide technical and functional supervision on a day-to-day basis but rather on a project basis.

SUPERVISION RECEIVED AND EXERCISED

Receives general direction from the Information Security Administrator.

Exercises technical and functional supervision over professional and technical personnel for assigned projects.

EXAMPLES OF ESSENTIAL DUTIES - Duties may include, but are not limited to, the following:

Plan and manage complex information technology projects including directing project teams, developing schedules, project plans, proposals, budgets and status reports applying cost benefit methodologies to monitor progress and success and managing projects to completion.

Develop and participate in the development of Requests for Proposal, Quote, or Information; participate in the selection and oversight of vendors and consultants.

Perform highly complex work to architect, implement, maintain, and troubleshoot the City's business continuity plan as it relates to redundant, systems and secure enterprise infrastructure.

Coordinate with Data Center SMEs to provide secure, fault tolerant, and highly available systems and networking infrastructure.

Investigate, analyze, produce reports, and remediate security incidents occurring on all City systems and applications, both on-premises as well as in the cloud.

Prepare and maintain system security-related policies, procedures, design documents, diagrams, drawings, and related documentation; monitor systems and network resources; maintain and administer security systems and methodologies.

Perform risk assessments and execute tests of network and information systems to ensure technology processes are secure

Confer with users to discuss issues such as computer data access needs, security violations, and system changes.

Review violations of computer and network security protocols and discuss procedures with violators to ensure violations are not repeated.

Stay up to date on evolving security threats and trends; regularly review security alerts and reports from Federal, State and commercial security sources.

Review technology governance concept papers and proposals and provide input regarding security aspects of proposed projects, applications, and systems

Ensure systems and procedures are compliant with relevant industry requirements and government regulations, e.g. PCI-DSS, CJIS, NERC CIP, etc.

Participate in strategic planning efforts with respect to improving information technology service delivery.

Stay abreast of relevant business and technology trends, internal and external to the City in order to evaluate new/future information system capabilities.

Develop and promote standardization and best practices including standardized architectures and governance processes; prepare and maintain procedures to ensure consistent work processes.

Coordinate and remediate trouble tickets escalated to Tier 2 support from other IT staff.

Prepare technical and administrative reports; review, prepare, and update internal system documentation and end user training instructional materials; conduct mentoring, cross-training, and end user training on group or individual basis as needed; develop policies and procedures.

Participate in budget preparation and administration for assigned projects.

Build and maintain positive working relationships with co-workers, other City employees, vendors, other public agencies and the public using principles of good customer service.

Perform related duties as assigned.

MINIMUM QUALIFICATIONS

Knowledge of:

Computer operating systems, local area networks, data communications software and hardware and network technologies, architectures, and environment.

NIST 800-series cyber security standards, CIS Top-20 Critical Security Controls, Payment Card Industry Data Security Standards (PCI-DSS), and Criminal Justice Information Security (CJIS) requirements.

Principles and practices of securing cloud-hosted systems and applications.

Current hacker techniques, exploits, active defense detection and prevention measures, penetration testing tools, tactics, techniques, and procedures (TTPs).

Unified threat management (UTM) firewalls and associated components including, but not limited to, URL/Content filtering, file scanning and blocking, DNS sinkholing, and data leakage prevention (DLP).

Endpoint detection and response (EDR) platform deployment, monitoring and management,

Business continuity planning, documentation, and testing best practices.

Computer and network forensic tools, techniques and analysis including root cause and comprehensive cause and effect analysis of cyber attacks and breaches.

eDiscovery processes and techniques for messaging and other social media platforms

Network monitoring tools and techniques used to perform security troubleshooting including packet capture and protocol analysis tools.

Network routing and switching protocols (BGP, EIGRP, OSPF, RIP, VLANs, STP, VTP, IOS, NX-OS, HSRP, CDP, LLDP).

File storage technologies, file structures, and file systems.

Methods of application integration.

Principles and practices of complex operating system design, analysis, and documentation.

System licensing, auditing and compliance.

Advanced project management methodologies.

Principles and practices of customer service.

Ability to:

Oversee and participate in complex projects involving the implementation and maintenance of compliance with all required information security rules, regulations, mandates, standards, and best practices.

On a continuous basis, know and understand all aspects of the job. Intermittently analyze work papers, reports and special projects; identify and interpret technical and numerical information; observe and problem solve operational and technical policy and procedures.

On a continuous basis, sit at desk for long periods of time. Intermittently twist to reach equipment surrounding desk; perform simple grasping and fine manipulation; intermittently climb stairs and/or ladders to rooftops and walk rooftops perimeter; use telephone, and write or use a keyboard to communicate through written means; and lift or carry weight of 50 pounds or less.

Design, document, and implement secure network, system, and application architectures.

Perform and/or work with professional service providers to conduct risk assessments and/or ethical hacking/penetration testing against city systems to determine and mitigate vulnerabilities and other security issues

Conduct various security awareness programs such as citywide cyber security training campaigns, phishing testing, and periodic targeted training initiatives.

Manage multiple projects concurrently.

Analyze, design, integrate, program, and manage highly technical and complex computer programs.

Analyze and develop logical solutions and alternatives to complex problems.

Develop scope of work for consultants and manage the consultant services procurement process.

Prepare a variety of reports and maintain accurate records and files.

Plan and support processes and adhere to best practices.

Maintain confidentiality as necessary.

Work weekends and evenings as required.

Communicate clearly and concisely, both orally and in writing.

Establish and maintain effective working relationships with those contacted in the course of work.

Experience and Training

Experience:

Two years of responsible experience performing duties similar to that of a Security

Analyst II with the City of Roseville.

AND

Training:

A Bachelor's degree from an accredited college or university, preferably with major course work in computer science, information systems, business management, business information systems, or a related field.

License or Certificate

Possession of a valid California driver's license by date of appointment.

04-09-22 Security Architect