CITY OF AURORA
POSITION DESCRIPTION

JOB CODE: 24237
SALARY GRADE: 18
EFFECTIVE: 12/21/2022

CHIEF INFORMATION SECURITY OFFICER

Definition

Reporting to the Chief Information Officer, this position requires the ability to understand business issues and articulate the business context of projects and processes to facilitate strategy, planning, and best practice sharing with senior business and IT executives, customers and industry leaders. The CISO is familiar with the principles and techniques of security risk analysis and must demonstrate an understanding of the management issues involved in implementing security processes and a security-aware culture in a large environment. Interactions require the ability to influence and persuade other senior leaders regarding complex and/or controversial situations. Responsible for planning, coordinating, implementing, conducting research and maintain information and cyber security policies for the City of Aurora, and works collaboratively across departments to increase security awareness, initiate business practice changes, perform risk assessments, develop mitigation plans and reach consensus regarding the need for security measures. This role will work in direct collaboration with the Director Cyber & Technology Risk.

Equipment/Job Location

Works in an office environment. Operates office equipment. Works with computer hardware and software. May work in confined areas and climb ladders.

Essential Functions of the Job

1. Perform highly responsible technical assistance and analysis for upper level management in the Information Technology Department.
2. Provide guidance and advocacy regarding the selection and prioritization of security infrastructure and other investments that impact information technology security.
3. Provide information technology security direction and oversight for all IT related systems and projects from acquisition through implementation.
4. Identify critical IT security needs.
5. Assists department heads with resource planning, prioritize and budget for security related items on IT.
6. Facilitates the development of subordinate plans for providing adequate IT security for networks, facilities and systems or groups of information systems.
7. Maintain understanding of relevant policies such as; Health Insurance Portability Accountability Act (HIPAA), Gramm–Leach–Bliley Act, Criminal Justice Information

Services (CJIS) Security Policy, Payment Card Industry Data Security Standard (PCI DSS), and State and Federal document retention.

8. Maintain awareness of potential cyber threats to the systems; provide timely reports to management that allow quick response as required to mitigate the threats.
9. Install, configure, and maintain information security equipment including firewalls, intrusion protection systems, routers, switches and other miscellaneous security appliances at the City.
10. Monitor and audit security equipment logs.
11. Coordinate and participate in security audits, vulnerability assessments, network scans, and penetration tests.
12. Work with other departments to coordinate information technology security activities and create a broad-based IT security conscious culture within the organization.
13. Work with staff in conducting cyber security investigations following the compromise of critical systems.
14. Preserve forensic evidence collected during information or cyber security investigations to prevent loss of evidentiary value.
15. Continue to develop skill and knowledge in the area of information systems security. Move this. Conduct routine hardware and software audits to ensure information and cyber security compliance with established standards, policies, procedures, and requirements.
16. Compile and analyze data and make recommendations on the formation of IT policies, procedures, and organizational services.
17. Responsible for the local operation and maintenance of security tools & processes, and adherence to policies that defend, detect, and respond to threats.
18. Collaborates with city departments to assess business requirements and develop strategies for securing of City information assets and processes.
19. Analyze and prepare statistical and monthly security reports, prepare special reports relating the progress of specified security activities.
20. Performs other related duties as assigned.

<u>Required Knowledge and Abilities</u>

1. Requires extensive knowledge and technical expertise with common software applications, computer cabling, and networks.
2. Requires the ability to think logically, analyze and interpret abstract and complex systems and application programming problems with efficiency and precision.
3. Requires training and instructional ability.
4. Requires the ability to communicate effectively orally and in writing.
5. Requires the ability to install, move, and repair equipment in confined or isolated areas.
6. Understand all aspects of the City’s networks, operating systems, hardware and software platforms, and protocols as they relate to information security.
7. Requires thorough knowledge of Federal, State and Local laws, as well as all Aurora Police Policies and Procedures.
8. Requires the ability to establish and maintain good working relationships with City

personnel, other agencies and vendor support personnel.

9. Requires ability to lift and carry hardware equipment.
10. Requires ability to sit for extended periods of time.
11. Requires ability to climb ladders.
12. Requires ability to work on weekends and second/third shifts on occasion.
13. Requires a valid Illinois driver's license and ability to operate city vehicles in a safe manner.

Qualifications for Hire

Experience:

- 5-10 years executive management experience working with C-Level executives and customers.
- 10-15 years of proven experience and demonstrated success in technology leadership and management, with an emphasis on information security, infrastructure services, portfolio management, business systems, IT architecture, and application development
- 8 years of experience managing a global enterprise information security function preferably in the software/high technology industry
- Experience in information security program administration and enforcement.
- Must have experience in the installation, setup and operation of network routers, switches, firewalls, data encryption devices and intrusion protection devices.
- Significant understanding of IT Infrastructure technologies including network, server, end-point, mobile, storage and how security relates to the overall IT environment
- Experience implementing regulatory and industry standard information security compliance strategies.
- Experience in information or cyber security incident response and forensics
- Any combination of education, training and experience which provides the required knowledge, skills and abilities to perform the essential functions of the job.

Education:

- Equivalent to a Bachelor’s degree from an accredited college or university or equivalent combination of education and experience CCNA or CCNP, CISM, CISSP (Preferred)
- Must complete required National Incident Management System (NIMS) Training Program within first six months of hire.