

<b>CITY OF CEDAR RAPIDS POSITION PROFILE</b>	<b>JOB CODE #/TITLE:</b> NB424 Information Security Manager
<b>POSITION #/TITLE:</b> 2486 Information Security Manager	<b>Adopted:</b> 02-08
	<b>Revised:</b> 03-15

<b>POSITION DESCRIPTION</b>
-----------------------------

<b>Dept:</b> Information Technology	<b>Manager Level:</b> Manager
<b>Salary Plan/Description:</b> NBU/Non-Bargaining Unit	<b>Salary Grade:</b> 15
<b>Reports To Position #/Job Code #/JC Title:</b> 1252/NB343/Chief Information Officer	<b>Dotted-line Reports To Position #/Job Code #/JC Title:</b>
<b>FLSA Status:</b> Exempt	<b>City Overtime Status (Employee Type):</b> Exempt (Salaried)
<b>Physical Demand Rating:</b> Light	<b>Work Environment:</b> Controlled
<b>Pre-employment Testing:</b> Drug and health screening after contingent offer.	<b>Position Testing:</b> Job fit assessment, knowledge test, skills test
<b>Personal Protective Equipment:</b> None	

<b>General Statement of Duties</b>
------------------------------------

Facilitates and makes recommendations to the Chief Information Officer on the performance of hardware configuration, detailed analysis, management reviews, policy reviews, audits, repair and maintenance of all Information Technology security related physical devices including but not limited to firewalls, routers, switches, HIDS/NIDS, IDS/IPS, anti-virus, Servers, PC's and any other device connecting to or protecting City IT assets. Performs related duties as assigned.

<b>Distinguishing Features of the Class</b>
---

Considerable leeway is granted for the exercise of independent judgement and initiative. The Information Security Program Manager serves as the lead Information Technology Security representative.

<b>Examples of Essential Work (Illustrative Only)</b>
---

Performs random security audits of all City Information Technology assets;  
Coordinates with technical and business teams in the development and continuous improvement of security risk assessment, and the adoption of risk-based testing, remediation and project prioritization;  
Recommends architecture governance for compliance solutions;  
Facilitates the risk assessment compliance effort and interaction with internal and external auditors;  
Develops the plans for the City to be secure which will be implemented by the Infrastructure Team.  
Audits the implementation of security management to ensure compliance;  
Develops and implements security practices, procedures and policies in cooperation with the Chief Information Officer;  
Assists with internal and external investigations involving forensics, chain of custody, etc.;  
Performs software configuration, detailed analysis, management reviews, port assignments, software security testing, development practices of all software including but not limited to internal and external applications such as COTS, APPS, DBs, Web development, Documents, Forms, and any other intangible asset operating, connecting to or protecting City Information Technology assets in cooperation with the Enterprise Applications Solutions division;  
Troubleshoots all problem areas associated with security related applications and computer operations;

Installs computer hardware components and all relevant software and hardware as needed;  
Assists in the development of database inquiries, reports and other software applications as needed for the support of specialized security investigations, analysis or support;  
Maintains all appropriate records on departmental computer operations and security related activities;  
Trains and assists other employees in the use of the various computer applications and troubleshoots operational problems as requested;  
Serves as the technical project lead for IT for JCN Fiber management, SCADA network and Traffic network;  
Performs all work duties and activities in accordance with City policies, procedures and safety practices;  
Attends work regularly at the designated place and time;  
Supports continuous process improvement initiatives;  
Performs related work as required.

### **Required Knowledge and Abilities**

Thorough knowledge of software, hardware and computer operating systems (specifically Microsoft Windows products and Microsoft Office products);  
Thorough knowledge of the functions and operations of the Information Technology Department;  
Thorough knowledge in information security, system architecture and risk management in an Information Technology environment;  
Thorough knowledge in security risk assessment and mitigation;  
Ability to manage Information Technology security across departmental lines horizontally and vertically to insure the Confidentiality, Integrity, Availability, Non-repudiation and lowest possible risk exposure with the least amount of business impact and cost according to a security ontology developed internally;  
Ability to take complex legal regulations, have detailed knowledge of the technical infrastructure and understand business implications to develop an enterprise-wide security risk assessment;  
Ability to drive the adoption of assessment results in remediation efforts, scope and frequency of testing and project prioritization across functional and regional boundaries;  
Ability to effectively conduct random security audits, coordinate process and audit controls, develop security policies based on industry standards to protect the data, information, assets, identities and employees of the organization;  
Ability to evaluate, develop and make recommendations to improve all defense in depth security measures, practices, policies, procedures, manuals, workflows, and all other processes which can or will disaffect Information Technology security;  
Ability to contribute to an enterprise Disaster Recovery/Business Continuity (DR/BC) plan;  
Ability to train others in the use of computer operations and software applications;  
Ability to install new computers, hardware and software;  
Ability to recognize departmental needs and design automated data systems;  
Ability to work cooperatively and to maintain effective working relationships to accomplish job responsibilities;  
Ability to quickly learn and put to use new skills and knowledge brought about by rapidly changing information and/or technology;  
Ingenuity and inventiveness in the performance of assigned tasks.

### **Acceptable Experience and Training**

Graduation from an accredited college or university with a Bachelor's Degree in Information Services, Computer Science or a closely related field; and  
Considerable experience working with computer software, hardware and operations systems related to IT security administration; or  
Any equivalent combination of experience, training and certification which provides the knowledge, skills and abilities necessary to perform the work.

### **Required Special Qualifications**

Valid Iowa Driver's License.

Certification in SANS GIAC or equivalent (Minimum).

Certification in CISA, CISM CompTia A+, Network+, or Server+, additional training desirable.

May be required to obtain Iowa NCIC certification based on work assignment.

### **Essential Physical Abilities**

Requires the following, with or without reasonable accommodation:

Clarity of speech and hearing which permits the employee to communicate effectively;

Sufficient vision which permits the employee to operate equipment and tools;

Sufficient manual dexterity which permits the employee to operate equipment;

Sufficient personal mobility which permits the employee to visit various and other work stations in the City.