

CITY OF CEDAR RAPIDS POSITION PROFILE	JOB CODE #/TITLE: NB421 Information Security Analyst II
POSITION #/TITLE: 2487, 2488 Information Security Analyst II	Adopted: 02-08
	Revised: 01-09

POSITION DESCRIPTION

Dept: Information Technology	Manager Level: Non-Manager
Salary Plan/Description: NBU/Non-Bargaining Unit	Salary Grade: 13
Reports To Position #/Job Code #/JC Title: 2485/NB424/Information Security Manager	Dotted-line Reports To Position #/Job Code #/JC Title:
FLSA Status: Exempt	City Overtime Status (Employee Type): Exempt (Salaried)
Physical Demand Rating: Medium	Work Environment: Controlled
Pre-employment Testing: Drug and health screening after contingent offer.	Position Testing: Job fit assessment, knowledge test, skills test
Personal Protective Equipment: None	

General Statement of Duties

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

Distinguishing Features of the Class

Considerable leeway is granted for the exercise of independent judgement and initiative. This position may serve as the lead IT Security representative at times.

Examples of Essential Work (Illustrative Only)

Performs random security audits of all City Information Technology assets and escalates findings to the Information Security Manager for consideration of further investigation;

Performs hardware configuration, detailed analysis, management reviews, policy reviews, repair and maintenance of all IT security related physical devices including but not limited to firewalls, routers, switches, HIDS/NIDS, IDS/IPS, Servers, PC's and any other device connecting to or protecting City IT assets in coordination with the Operations section;

Participates on 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;

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 Applications Design and Development section;

Troubleshoots all problem areas associated with security related applications and computer operations and reports findings to the Information Security Manager for further action;

Installs computer hardware components and all relevant software and hardware as needed;

Develops 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;
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 XP Workstation and Microsoft Office Professional);
Good knowledge of the functions and operations of the Information Technology Division;
Good knowledge in information security, system architecture and risk management in an Information Technology environment;
Good knowledge in security risk assessment and mitigation;
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, institute 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 and 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 maintain 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 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 ISACA CISA, CISM or equivalent (Minimum).
Certification in CompTia A+, Network+, or Server+, SANS training desirable.
Must possess or attain a higher level of IT Security certification within 2 years of employment.
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.