CITY OF FONTANA
(IT) NETWORK/SECURITY ADMINISTRATOR

DEFINITION: The Network/Security Administrator is responsible for all IT infrastructure services, IT security and integrating physical security systems and networks. This position also serves as backup to the Database Administrator and the Systems Administrator. Successful incumbents will also conduct themselves in a professional and ethical manner, enjoy keeping their technology skills updated and posses a positive and enthusiastic attitude.

EXAMPLES OF DUTIES: Under general supervision, incumbents assigned to this classification are expected to perform the full range of work assigned to this class and are expected to work independently.

ESSENTIAL FUNCTIONS: The incumbent must have the ability to:

- Manage infrastructure and security projects.
- Serve as department liaison on city construction projects for IT infrastructure needs.
- Participate in disaster planning and recovery.
- Design, configure, maintain and monitor the city's network infrastructure.
- Evaluate the cable plant and recommend strategies for optimization.
- Ensure that network equipment is adequately maintained, covered under appropriate support agreements, and replaced on the appropriate lifecycle schedule.
- Design and implement LAN/WAN topology to meet connectivity requirements.
- Diagnose and resolve LAN/WAN connectivity problems.
- Monitor network bandwidth usage and tune for optimal performance.
- Investigate and resolve IT security breaches.
- Support the city's Identity Management, Access Control, Intrusion Detection, and Video Surveillance systems.
- Configure, support and evaluate security tools.
- Conduct security audits and provide recommendations to mitigate risks.
- Configure and support Firewalls, Content Engines, and Intrusion Detection / Prevention Systems.
- Represent the information security function in the IT change management process to ensure security concerns are addressed.
- Participate in the evaluation of vendor proposals, new and existing security designs, and emerging security technologies and systems.
- Supervise the configuration and support of anti-virus software.
- Supervise the server and desktop patch management function.
- Provide backup support for the Systems Administrator and Database Administrator.

THE ABOVE LIST OF ESSENTIAL FUNCTIONS IS NOT EXHAUSTIVE AND MAY BE SUPPLEMENTED AS NECESSARY BY THE EMPLOYER.

WORKING CONDITIONS: In the performance of daily activities, this position requires prolonged sitting, standing, walking, reaching, twisting, turning, kneeling, and bending; the ability to push, pull, drag and/or lift up to 25 pounds; normal manual dexterity and hand/eye coordination; repetitive hand movement using a computer keyboard and mouse; corrected vision to normal range; acute hearing; written and oral

communication; use of standard office equipment such as computers, telephones, printers, and copiers; frequent contact with other staff.

EXPERIENCE AND TRAINING GUIDELINES: A combination of experience and training that would provide the required knowledge is qualifying. The incumbent must have knowledge and background in the following:

- Experience configuring and securing routers, switches, firewalls, VPN appliances, and other network equipment.
- Intermediate to expert knowledge of common protocols such as SNMP, HTTP, HTTPS, SMTP, NTP, LDAP, KERBEROS, RADIUS and FTP.
- Knowledge of disaster recovery and business continuity practices.
- Intermediate to expert knowledge of operating systems and enterprise patch management.
- Intermediate to expert knowledge of Active Directory security.
- Intermediate to expert knowledge of database security.
- Intermediate knowledge and experience with MS SQL Server.
- Intermediate to expert knowledge of software-based security applications (anti-virus, SPAM filters, web content filters, etc.).
- Intermediate to expert knowledge of Intrusion Detection / Prevention.
- Knowledge of CCTV system configuration and operation.
- A basic understanding of security policies.
- A basic understanding of risk assessments and audits.
- A working knowledge of IT Infrastructure Library (ITIL) processes.
- Excellent problem-solving and communication skills.
- Basic project management skills.
- Employee supervision and evaluation skills.

EXPERIENCE AND EDUCATION: A minimum of four years experience in Network Administration and Security Administration, three years experience with Microsoft server and UNIX operating systems, a Bachelor’s Degree from an accredited college or university with major coursework in Computer Science or a closely related field.

DESIRED CERTIFICATIONS:

- CISSP, SANS OR GIAC
- Any Cisco certification
- Any Microsoft server or network certification

LICENSES AND/OR CERTIFICATIONS: Possession of, and continuously throughout employment, a valid California Class “C” Driver's License.

SUPPLEMENTAL INFORMATION: Successful candidates will be required to pass a drug screening, fingerprint screening, physical examination and a background investigation.