CARROLLTON
TEXAS

DATE	11/1/2022
JOB CODE	
FLSA	EXEMPT ADMINISTRATIVE
EEO	

JOB TITLE: Security Engineer
DEPARTMENT/DIVISION: Information Technology
REPORTS TO: Infrastructure & Security Officer

SUMMARY: Responsible for the security of the organization's computer systems and networks. This position will design, implement, and maintain security solutions as well as actively participate in the development of standards and information security policies and procedures.

ESSENTIAL JOB FUNCTIONS:

- Develop, execute, and track the performance of security measures to protect information and network infrastructure and computer systems.
- Design computer security strategy and engineer comprehensive cybersecurity architecture.
- Identify, define, and document system security requirements and recommend solutions to management.
- Configure, troubleshoot, and maintain security infrastructure software and hardware including, but not limited to, firewalls, IPS/IDS, Anti-virus, etc.
- Install software that monitors systems and networks for security breaches and intrusions.
- Monitor systems for irregular behavior and set up preventive measures.
- Plan, develop, implement, and update the City's information security strategy.
- Educate and train staff on information system security best practices.
- Oversight of disaster recovery operations and record backups when required.
- Maintain compliance with external regulatory controls such as HIPAA, PCI-DSS, and CJIS.
- Participates in a variety of special projects in support of departmental operations, which may include performing special studies; providing guidance and recommendations to departments to ensure organizational sustainability and maximize organizational efficiency, effectiveness, and performance; recommending cost- conscious decisions and actions; and/or, performing other related activities.
- Performs other duties as assigned, which may involve irregular work hours, including evenings and weekends.

KNOWLEDGE, SKILLS, AND ABILITIES:

- Ability to work in high-risk environments;
- Exceptionally creative problem-solving skills;
- Ability to gauge potential cyber security threats;
- Ability to work within and across teams;

- Excellent written and verbal communication skills;
- Willingness to learn and improve;
- Knowledge of various programming languages (ie. C, C++, SQL, Powershell, Ruby, Shell Scripting, Python, etc)
- Knowledge of networking (ie. Subnetting, routing protocols, VoIP, DNS, VPN, encryption techniques, secure network architecture, etc)
- Knowledge of web application and browser security;
- Knowledge of security assessments and penetration testing techniques and procedures;
- Knowledge of incident response and forensics;
- Knowledge of project management and team management methodologies;

MINIMUM QUALIFICATIONS:

- 3-5 years of progressive experience in IT operations, policy development, and governance
- Security+ certification and an ISC2 cybersecurity certification or equivalent upon management approval within 6 months of employment
- Hold one or more of the following certifications (or substantially similar) or the ability to obtain within 12 months of employment:
  - Cisco Certified Network Professional Security (CCNP Security)
  - Palo Alto Networks Certified Network Security Administrator (PCNSA)
  - Certified Ethical Hacker (CEH) v10 or higher
  - CompTIA Advanced Security Practitioner (CASP+)
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Systems Security Certified Professional (SSCP)
  - Certified Information Systems Security Professional (CISSP)
- Hold two or more valid and current industry recognized certifications in current enterprise technology areas outside of security field.
- Must qualify for and maintain compliance with Criminal Justice Information Systems access requirements
- Must possess or be able to obtain and maintain a valid Texas driver’s license

PREFERENCES:

- 4-5 years experience designing, configuring, administering, and maintaining a complex network and server environment with an emphasis on security
- Hold two or more of the following certifications (or substantially similar):
  - Cisco Certified Network Professional Security (CCNP Security)
  - Palo Alto Networks Certified Network Security Administrator (PCNSA)
  - Certified Ethical Hacker (CEH) v10 or higher
  - CompTIA Advanced Security Practitioner (CASP+)
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Systems Security Certified Professional (SSCP)
  - Certified Information Systems Security Professional (CISSP)

WORKING CONDITIONS:

- Frequent sitting, talking, seeing, hearing, and manual dexterity.
- Occasional lifting and carrying up to 50 pounds.
- Work is typically performed in a standard office environment.
- Work may be performed in a data center environment involving loud noise and temperature irregularity
- Work both indoors and outdoors and are exposed to cold and hot temperatures, constant noise, fume/odor hazards, road hazards, heights, and mechanical and electrical hazards

CONDITIONS OF EMPLOYMENT:

- Must pass pre-employment drug test.
- Must pass criminal history check.
- Must pass motor vehicle records check.