Security and Systems Manager (Supervisor of Elections)
Pinellas County, FL

Location: 13001 Starkey Road, Largo, FL 33773

The 2020 election year is upon us and the Security and Systems Manager position will play a key role in maintaining the cybersecurity within the trusted reputation of the Pinellas County Supervisor of Elections. If you have a background in information systems security, vulnerability management, and incident response planning, this position may be the ideal opportunity for you.

This is a specialized and technical work supervising a staff providing information technology (IT) operational, technical, and applications support for the Supervisor of Election's local and wide area networks. This position provides system analysis and design, installation, configuration and maintenance of new and existing office networked data processing systems, as well as connectivity between the office's computer network and any other computer network. Assignments and activities to support operations require the incumbent to exercise considerable independent action, initiative, and judgment completing day-to-day assignments and activities to support operations. The incumbent reports to the Elections Technology Administrator or designee.

Position Specific Qualifications

Experience – professional experience as a Systems Administrator with an emphasis on information systems security including lead worker experience or supervisory training.

Education – degree in computer science or related field.

- 6 years of experience as described above; or
- Associate degree as described above and 4 years of experience as described above; or
- Bachelor's degree as described above and 2 years of experience as described above; or
- Master's degree as described above and some experience as described above.

Additional Requirements

- Must be able to work additional hours, including holidays and weekends, as needed during election cycles.
- Assignment to work a variety of work schedules including compulsory work periods in special, emergency, and/or disaster situations.

Highly Desirable

- Bachelor's Degree in Computer Science or related field.
- Experience with Cybersecurity Standards and Frameworks such as NIST and ISO/IEC.
- Certifications such as CISSP, CISM, CEH, CASP+, CySA+, PenTest+
- GSEC: GIAC Security Essentials Certification
- ECSA: EC-Council Certified Security Analyst

Illustrative Tasks

- Coordinates the security, design, installation, maintenance, and support of all hardware and related network components as well as the installation and maintenance of all operating software within the office's local and wide area networks.
- Develops the design specifications of computer systems, programs and operating systems, with the following core competencies: Security Analysis, Design, Business Process Improvement, Data

Modeling, Development, Planning, Implementation, Test Script Development, Monitoring/Controls, Troubleshooting/Problem Solving, Documentation and Service Motivation.
- Develops and implements Internet/intranet configuration solutions and technological solutions within the office's network environment.
- Solicits, compiles, analyzes and summarizes data and information; distinguishes between relevant and irrelevant information in order to make immediate logical decisions; provides appropriate and necessary solutions.
- Coordinates deployment of new and enhanced applications throughout the office or within single divisions or workgroups as appropriate; trains employees on the applications as necessary.
- Serves as liaison to external agencies and entities with regard to the security, implementation, distribution, connection of shared information systems, network resources, hardware resources, operating system resources, the purchase of equipment, and problem resolution.
- Coordinates technical support and trains office staff work groups and divisions.
- Develops and maintains network and support staff documentation.
- Additional duties may be assigned and not included in the above listing.

Knowledge, Skills and Abilities

- Knowledge and skills in using Windows Server 2016, SQL Server 2016, Splunk, Microsoft Advanced Threat Protection.
- Knowledge and skills in using Windows 10, Microsoft Office 365, MapInfo, ESRI, VoterFocus, Adobe Creative Cloud.
- Knowledge of computer operating systems, network operating systems and network protocols.
- Knowledge of system analysis and design techniques.
- Knowledge of advanced-level Cyber Security concepts and methodology.
- Knowledge of industry standards and practices relating to data communications, office automation and computer systems in the development of policy, direction and standards.
- Knowledge of implementing anti-malware, anti-virus, web filtering, application control, and data leakage protection.
- Knowledge of application protection technologies and secure development concepts.
- Knowledge of performing risk assessments and IT audits.
- Knowledge of security best practices such as the CIS Benchmarks, security awareness, incident response, enterprise security monitoring, compliance and auditing.
- Knowledge of creating security policies and best practices, security program management, vulnerability management, risk management.
- Ability to present oral and written reports clearly and concisely.
- Ability to conduct tests, analyze test results, detect design and configuration errors and take appropriate corrective steps.

Salary: $70,000.00 - $75,000.00

Apply by: December 13, 2019

To apply visit:
https://chu.tbe.taleo.net/chu04/ats/careers/v2/viewRequisition?org=PCG&cws=47&rid=3195

EOE/AA/ADA/DFW/VP

Certain servicemembers and veterans, and the spouses and family members of the servicemembers and veterans, receive preference and priority in employment by the state and are encouraged to apply for the positions being filled.