Information Security Administrator

Definition:

Under the direction of the Kern County Deputy Chief Information Technology Officer, or designee, oversees the day-to-day operations of the in-place security solutions and works with other Security Team personnel; ensure the secure operation of the in-house computer systems, servers, and network connections. This includes checking server and firewall logs, scrutinizing network traffic, establishing and updating virus scans, and troubleshooting. This person will also analyze and resolve security incidents and vulnerability issues in a timely and accurate fashion.

This position is an Administrative level position. Duties may include, but are not limited to, the implementation of new security solutions, assist with the creation and or maintenance of policies, standards, baselines, guidelines, and procedures as well as conducting vulnerability audits and assessments. The Information Security Administrator is expected to be fully aware of and participate in establishing the enterprise's security goals as established by its stated policies, procedures, and guidelines and to actively work towards upholding those goals. The Information Security Administrator is distinguished from the Information Security Analyst by the formers responsibility to assist in the deployment, management, and maintenance of all security systems and their corresponding or associated software.

Essential Functions:

- Assist in the deployment, management, and maintenance of all security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and anti-virus software.
- Manage connection security for local area networks, the company web site, the company intranet, and e-mail communications.
- Manage and ensure security of databases and ensure data in transit is protected as appropriate for classification and compliancy regulations.
- Under general guidance of the Deputy Chief Information Technology Officer, perform vulnerability assessments of all systems to identify system vulnerabilities.
- Assist in a team lead role for incident response efforts and the remediation of threats and vulnerabilities.
- Design, implement, and report on security system and end user activity audits.
- Download and test new security software and/or technologies.
- Provide on-call security support to end-users.
- Manage and/or provide guidance to junior members of the team.
- Recommend, schedule, and perform security improvements, and/or upgrades.
- Maintain up-to-date knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes, and the development of new attacks and threat vectors.
- Assist in the planning and design of enterprise security architecture.
- Assist in the creation of enterprise security documents (policies, standards, baselines, guidelines, and procedures).
- Assist in the planning and design of an enterprise business continuity plan and disaster recovery plan.
- Performs other job-related duties as required.

Employment Standards:

A bachelor's degree from an accredited college or university, in computer science or information technology related field AND three (3) years of experience in the administration of networks and/or security systems environments for a department or organization.

OR

Completion of an accredited trade or vocational school training program in computer repair, computer science or information systems AND five (5) years of experience in the administration of networks and/or security systems environments for a department or organization.

OR

Completion sixty (60) semester or ninety (90) quarter units from an accredited college or university, in computer science or information technology related field AND five (5) years of experience in the administration of networks and/or security systems environments for a department or organization.

OR

Seven (7) years of experience in the administration of networks and/or security systems environments for a department or organization.

Qualifying experience must have been within the last eight (8) years.

A valid Class "C" California Driver's License is required at the time of appointment.

Knowledge of: firewalls, intrusion detection systems, anti-virus software, data encryption, and other industry-standard techniques and practices; In-depth technical knowledge of network, PC, and platform operating systems; antivirus and end-point management practices and techniques; working technical knowledge of the Microsoft Defender suite; strong understanding of IP, TCP/IP, and other network protocols; hands-on experience with devices such as hubs, switches, and routers; familiarity with Microsoft Sentinel, Tanium, PRTG, and other monitoring systems.

Ability to: conduct windows server administration; understand and utilize Microsoft Azure cloud environments; work with PowerShell and other scripting languages.

A background check may be conducted for this classification.

All Kern County employees are designated "Disaster Service Workers" through state and local laws (CA Government Code Sec.3100-3109 and Ordinance Code Title 2-Administration, Ch. 2.66 Emergency Services). As Disaster Service Workers, all County employees are expected to remain at work, or to report for work as soon as practicable, following a significant emergency or disaster.