GEM
COMPANIES INC
DBA GEM NETWORK SOLUTIONS

Position Description

JOB TITLE: IT Security Engineer

Primary Location: Colorado Springs

Summary:

Provide subject matter expertise and capability to consult/troubleshoot security related matters for enterprise information system and network architectures, access problems and implementation of security policies and procedures. Ensures security access and protects against unauthorized access, modification, or destruction. Demonstrate a familiarity with a variety of security concepts, practices, and procedures. Relies on extensive experience and judgment to plan and accomplish goals. May lead and direct the work of others. A wide degree of creativity and latitude is expected. The Information Technology (IT) Security Engineer reports to the Mission Support Manager.

Responsibilities:

Apply solid knowledge of information security principles and practices. Manage and maintain the security integrity of all IT systems and network architectures. Ensure systems are operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the security plan. Ensure all users have the requisite security clearances, authorization, and are aware of their security responsibilities before granting access systems. Other facets of the IT Security Engineer responsibilities include the following:

- Provide daily, ongoing security oversight of assigned systems as to the security impact of proposed modifications, additions, and technology refresh evolutions.
- Advise users of the security features and procedures used in their ISs
- Evaluate and develop approach to solutions while proactively assess items of risk and opportunities of vulnerability in the network.
- Provide vulnerability remediation and mitigation recommendations.
- Work directly with internal IT staff and customer to establish and enforce IT security best practices, protection objectives, process improvements and effective IT security controls.
- Perform system vulnerability scanning using approved software tools.
- Assist with the software installation, monitoring, troubleshooting, account management, and overall efforts to minimize system downtime.
- Assist in the administration of critical server infrastructure, including e-mail, backup and recovery, file servers and web servers.

Provide documentation on security practices and vulnerability mitigation reports. Support network accreditation activities. Participate in system reviews to include hardware and software, in-house development and provide recommendations for securing these systems.
Assist in IT security incident response and documentation. Provide security administration for all IT Security applications and associated accounts. Perform regularly scheduled security reviews (e.g., technology, operations and personnel). Participate in designing and managing IT Security strategy including both infrastructure and applications. Lead security and compliance based projects. Perform regularly scheduled software upgrades/updates. Consult with users to determine requirements, and provide security solutions to meet needs. Assist with projects involving database and security issues and requirements. Monitor network to ensure network availability to all system users and perform necessary maintenance to support network availability. Work w/ various technologies including servers, printers, network peripherals, & network infrastructure. Installing, maintaining and troubleshooting Windows 2003/2008 server, networking Infrastructure (hardware and security).

Minimum Qualifications:

- CISSP certification
- 7+ years experience as a Security Engineer supporting software architecture development environments
- Expert on security directives, policies, publications and regulations
- Strong experience in creating System Security Plans
- Strong experience in IT security certifications (CIPP. CompTIA Security, CPP, PSP and alarm/badge system
- Posses clear understanding of security protocols and standards and have experience with software and security architectures.
- Understand how to design and implement security tests in accordance with stated criteria
- Experience with security practices of Intranet and Extranet
- Experience with packet analyzers
- Experience with Linux/UNIX/AIX and Windows servers 2003 & 2008
- Expert understanding of protocols, such as, SSL/TLS, CIFS, HTTP/S, DHCP, SMTP, LDAP/S and DNS
- Experience in networking concepts and services, such as, VPNs, IPSec, PKI and TCP/IP
- Expertise with the accreditation process in support of such programs as DIACAP

Preferred Qualifications:

- 7 to 10 years of experience in IT security field
- Able to work independently or within a team

- Ability to work with minimal direction on a variety, sometime ambiguous, requirements
- Strong communication skills, both oral and written
- Organized, responsive and highly thorough problem solver
- Familiar with security controls of Federal Information Systems

Education/Certification Requirement:

A Bachelor's degree or equivalent in Computer Science, Information Systems Management, Information Technology or other related discipline with 7 or more years related professional experience..

Clearance:

Minimum Active DoD Secret

Working Hours:

Day, 8AM – 5PM, Some on call

Relocation authorized: None