

## IT Security Associate

### Job Description

#### ***Company Overview***

Partners Enterprise Capital LLC (PEC) is a registered investment advisor with more than \$20 billion of assets under management through long-term private equity investments in real estate operating companies throughout the United States. PEC primarily focuses on the industrial, residential, and retail sectors.

PEC maintains a mission-driven business model with an established track record of strong performance that incorporates elements of venture capital, private equity, and real estate investment management. The approach is strategic and relationship-driven, with a long-term view that is centered on business building. PEC's flat organizational structure and entrepreneurial culture allow for all roles to be broad and dynamic with significant opportunity for learning and development. A substantial foundation of organizational resources and capital is in place to facilitate the company's continued growth.

#### ***Position Overview***

PEC is seeking an IT Security Associate to join its team in Chicago. This is an exciting opportunity to contribute to and be part of a key team at PEC. The position will be based in PEC's Fulton Market office. PEC operates in a hybrid work model, with a majority of days in the office. In-person collaboration and learning are integral to PEC's culture and success in this role.

The IT Security Associate will be responsible for tasks related to identifying, analyzing, and resolving complex information technology and cybersecurity issues. The individual in this role will manage, monitor, and ensure compliance with cybersecurity controls and procedures and develop and implement processes to facilitate continual improvements and evolution. The IT Security Associate will ensure proper technology maintenance and operations so that end users can accomplish daily business tasks. Problem resolution may involve the use of diagnostic and help request tracking tools, as well as hands-on help at the desktop level with response by email and telephone, as needed.

#### ***Primary Responsibilities***

- Analyze, remediate, and respond to user submitted phishing messages
- Triage or resolve incidents raised by our cybersecurity tools
- Assist in incident response procedures as needed
- Participate in vulnerability remediation tasks
- Work with other teams to remediate vulnerabilities
- Assist in the deployment and configuration of security solutions
- Produce documentation and curate existing documentation
- Take part in security policy audits
- Monitor and review logging of user data
- Perform malware investigations as needed
- Respond to escalated IT and security tickets
- Assign training for security and communicate results
- Manage phishing and new hire security programs
- Understand and assess risks regarding data and technology issues throughout the organization

- Monitor and maintain the health of IT systems, networks, and servers
- Provide first-line technical support to end-users, addressing hardware and software issues promptly and effectively
- Assist with the setup, configuration, and maintenance of end-user devices
- Respond to and resolve IT incidents in a timely manner, ensuring minimal disruption to business operations
- Identify opportunities for process improvement and automation within IT operations and support

***Preferred Skills, Capabilities, and Experience***

- Bachelor's degree from an accredited academic institution with a focus in one of the following: Cybersecurity, Business, Information Security, Information Technology, or Computer Science with a cybersecurity concentration preferred
- 2+ years of experience in information technology and cybersecurity
- Experience with Cloud Security (Azure/O365)
- Excellent communication and teamwork skills
- Proven problem-solving and analytical abilities
- Project management skills
- High degree of sensitivity to confidential matters required
- Strong interpersonal skills
- Ability to work in a fast-paced environment, in both team and independent settings
- Consistently delivers on commitments, deadlines, and objectives while remaining in scope and leveraging appropriate tools, methods, frameworks, and professional standards
- Ability to build trust and credibility with business partners and leadership while recommending initiatives and identifying gaps and potential issues
- IT/Cyber certification(s) preferred, but not required

***To Apply***

Please submit a resume to [careers@pec1999.com](mailto:careers@pec1999.com)

PEC is an equal opportunity employer and makes employment decisions based on merit. Company policy prohibits unlawful discrimination based on genetic characteristics or information, race, color, creed, sex, gender, gender identity, religion, marital status, partnership status, age, national origin or ancestry, alienage, physical or mental disability, medical condition, veteran status, sexual orientation, or any other consideration made unlawful by federal, state, or local laws.