|  |
| --- |
| **الجمهورية اللبنانية**  **وزارة الأشغال العامة والنقل**  **مصلحة استثمار مرفأ طرابلس** |

**لائحة الأسعار لأعمال " حماية الأمن السبراني في مرفأ طرابلس "**

يجب أن تنفذ أعمال الإشراف وفقاً لدفتر الشروط الفنية، وعلى أن تشمل أعمال الأمن السبراني، الإجراءات والسياسات والتقنيات والممارسات التي تهدف لحماية الأنظمة المعلوماتية والشبكات (ويقصد الشبكات السلكية واللاسلكية والفايبر أوبتيك) والبيانات من التهديدات السبرانية والهجمات والإختراقات الإلكترونية. كما تهدف إلى توفير سرية وسلامة البيانات وفقاً للبنود التالية:

1. يدفع ثمن الشهر الواحد بدل أعمال إشراف مهندس أمن سبراني، على أن تشمل:

* Protecting computer systems, networks, and data from cyber threats.
* Designing and implementing security measures: This involves creating and deploying systems and protocols to safeguard digital assets against unauthorized access, data breaches, and cyber attacks.
* Monitoring and detecting security breaches: Cybersecurity engineers continuously monitor networks and systems for any signs of suspicious activity or potential security breaches. They use various tools and technologies to identify and analyze security incidents.
* Responding to security incidents: When security breaches occur, cybersecurity engineers investigate the incidents, contain the damage, and implement remediation measures to mitigate the impact and prevent future occurrences.
* Conducting security assessments and audits: They perform regular assessments and audits of systems and networks to identify vulnerabilities and weaknesses. They then recommend and implement security improvements based on their findings.
* Developing security policies and procedures: Cybersecurity engineers create and enforce security policies and procedures to ensure compliance with industry regulations and best practices. They also educate users and stakeholders on security best practices.
* Conducting research and staying updated: Given the constantly evolving nature of cyber threats, cybersecurity engineers stay abreast of the latest trends, technologies, and tactics used by cyber attackers. They conduct research and participate in training programs to enhance their knowledge and skills.

فقط................................................................................................... دولار أميركي.

1. يدفع ثمن الشهر الواحد بدل أعمال إشراف مهندس شبكات وعلى أن تشمل:

* Designing network infrastructure: Planning and designing the layout of computer networks, including hardware components, software applications, and connectivity protocols.
* Installing and configuring network equipment: Setting up routers, switches, firewalls, and other network devices to ensure efficient data transmission and security.
* Troubleshooting network issues: Identifying and resolving connectivity problems, performance issues, and security breaches to ensure uninterrupted network operation.
* Monitoring network performance: Regularly monitoring network traffic, bandwidth usage, and security protocols to identify potential issues and optimize network performance.
* Upgrading network infrastructure: Assessing and implementing upgrades to network hardware and software to support evolving business needs and technological advancements.
* Implementing security measures: Configuring firewalls, intrusion detection systems, and other security measures to protect the network from unauthorized access and cyber threats.
* Providing technical support: Assisting users with network-related issues, offering guidance on network usage best practices, and conducting training sessions for staff members.
* Documenting network configurations: Maintaining detailed documentation of network configurations, procedures, and troubleshooting steps to facilitate future maintenance and upgrades.

فقط................................................................................................... دولار أميركي.

1. يدفع ثمن الشهر الواحد بدل أعمال فني أمن سبراني وشبكات على أن تشمل:

* Assessing and analyzing network infrastructure and security systems.
* Designing and implementing security measures to protect against cyber threats.
* Conducting vulnerability assessments and penetration testing.
* Providing recommendations for improving network security posture.
* Troubleshooting and resolving network security incidents.
* Developing and implementing security policies and procedures.
* Training staff on security best practices and protocols.
* Keeping up-to-date with the latest security threats and technologies.
* Collaborating with IT teams and management to ensure compliance with industry standards and regulations.
* Offering guidance on risk management and mitigation strategies.
* Installing and configuring security software and tools.
* Performing security audits.
* Providing technical support to employees, handling error, detects and repairs it.
* Save data and backed up regularly
* Coordinating with programming companies and preparing the necessary resources for the programs.
* Adopting policies and procedures that enable every employee to access the computer system and information in accordance with security standards.

فقط................................................................................................... دولار أميركي.