Corporate Security
Protecting Personnel and Property

Introduction:

Corporate security is a comprehensive concept that includes a set of procedures and policies aimed at protecting people and property from internal and external risks. These risks include theft, vandalism, violence, cybercrime, cyber breaches, natural disasters and other events that could harm the company.

The Importance of Corporate Security:

- **Employee Protection:** Employee safety is a top priority for any company. Corporate security contributes to providing a safe and comfortable work environment for employees, which enhances productivity and reduces absenteeism.

- **Property Protection:** Property, such as equipment, merchandise, and data, represent valuable company assets. Corporate security helps protect these assets from theft, damage, and vandalism.

- **Maintaining Company Reputation:** Security incidents may damage a company's reputation, which may result in the loss of customers and partners. Corporate security helps maintain a company's image as a reliable and responsible company.

- **Compliance With Laws and Regulations**: Many laws and regulations require companies to take certain measures to protect their data and systems. Corporate security helps ensure that a company complies with these requirements.

Corporate Security Elements:

- **Security Assessment:** The first step in creating an effective corporate security program is to conduct a comprehensive security assessment to determine the risks facing the company.

- *Security Policy:* The company must establish a security policy that specifies the procedures and policies that must be followed to protect individuals and property.

- *Training:* Employees should be trained on security risks and how to protect themselves and property.

- *Technical Controls:* The company must install technical controls, such as video surveillance systems and fire alarm systems, to prevent security incidents.

- *Incident Management:* The company must develop a plan to manage accidents if they occur.

Objectives:

At the end of the training, the trainee will be able to:

1- Clearly explains corporate security rules.

2- Able to apply self-security skills.

3- Applies the principles of crisis and disaster management.

4- Familiar with the rules for evaluating security threats.

5- He possesses information security skills and is able to follow up on hacking protection programs.

Program Topics:

First Day:

Introduction to the security of companies, establishments and individuals:

- Defining the security of companies, establishments and individuals.

- The importance of the security of companies, establishments and individuals.

- Threats facing companies, establishments and individuals.

Security Assessment:

- Steps to conduct a comprehensive security assessment.

- Identify the risks facing the company.

- Evaluate the effectiveness of current security measures.

The Second Day:

Security Policies:

- Establish a comprehensive security policy.

- Elements of an effective security policy.

- Implement security policy throughout the company.

- Security training:

- The importance of training employees on security.

- Content of effective security training programs.

- Providing security training programs for employees.

The Third Day:

Technical Controls:

- Different types of technical controls.

- Choosing appropriate technical controls.

- Installation and operation of technical controls.

- Incident management:

- Develop an incident management plan.

- Steps to respond to a security incident.

- Recovering from a security incident.

The Fourth Day:

Information Security:

- Protect data from theft and unauthorized access.

- Use anti-virus and anti-malware software.

- Protecting computer systems from electronic attacks.

Network Security:

- Securing company networks from external attacks.

- Use firewalls and encryption software.

- Monitor network activity.

The Fifth Day:

Building Security:

- Protecting buildings from theft and vandalism.

- Use of video surveillance systems and fire alarm systems.

- Conduct regular security inspections.

Security of Individuals:

- Protecting employees from violence and harassment.

- Providing a safe and comfortable work environment.

- Providing assistance programs for employees.

Training And Evaluation Methodology:

- The program will be implemented using PowerPoint

- Training includes simulation methods, narrating situations, and analyzing them

- Show specialized videos and extract their weak points

- Use brainstorming, discussion, and work team skills to extract solutions

- Means of maximizing security perception and observation skills.

Location	**Fairmont Nile City**
Start Date	**07 July 2024**
End Date	**11 July 2024**
Fees Before Discount	**3500 $**
Special Discount	**25% (To nominate five participants)**
Fees After Discount	**2625 $**