€TRAINING

Developing Field Leaders in Industrial Security

Developing Field Leaders in Industrial Security

Introduction:

This training program is designed to cultivate effective leadership within the industrial security sector. It focuses on honing the skills and knowledge necessary for individuals to lead security teams and operations in industrial settings.

Program Objectives:

At the end of this program, participants will be able to:

- Implement comprehensive document security protocols.
- Design and manage information systems security plans.
- Enhance physical security measures for asset protection.
- Administer personnel security procedures effectively.
- Navigate international security challenges and compliance.
- Execute classification processes and handle classified information.
- Develop and deliver tailored security education programs.
- Conduct audits and vulnerability assessments for ongoing improvement.
- Specialize in elective areas such as intellectual property protection and counterintelligence.

Targeted Audience:

- Security Managers.
- Security Professionals.
- Managers.

Program Outlines:

Unit 1:

Document Security:

- Creation & Marking.

- Storage & Accountability.
- Transmission & Receipting.
- Reproduction & Destruction.
- End of Contract Actions.

Unit 2:

Information Systems Security:

- System Security Plans.
- Accreditation.
- Physical Protections.
- Administrative & Procedural Controls.
- Forensics.

Unit 3:

Physical Security:

- Theory: Graded & Layered Protection.
- Locks & Security Containers.
- Vaults & Vault-type Rooms.
- Alarms.
- CCTV.

Unit 4:

Personnel Security:

1. Forms.
2. Adjudication.
3. EPSQ/JPAS.
4. Clearances & Badges.
5. Insider Threat Detection.

Unit 5:

International Security:

- Export Control Regulations.
- Foreign Visits & Assignments.
- Foreign Ownership, Control, or Influence.
- Controlling Access by Foreign Persons.
- Cross-Border Data Protection Measures.

Unit 6:

Classification:

- Identifying Critical Information.
- Classification System & Guides.
- Declassification Procedures.
- Controlled Unclassified Information CUI.
- Handling Classified Information in Electronic Systems.

Unit 7:

Security Education:

- Requirements and Content.
- Ideas & Techniques.
- Training Methodologies.
- Security Awareness Programs.
- Continuous Learning Initiatives.

Unit 8:

Audits & Self-Assessments:

- Audits Planning & Execution.

- Compliance Monitoring.
- Vulnerability Assessments.
- Corrective Action Planning.
- Continuous Improvement Processes.

Unit 9:

Electives:

- Intellectual Property Protection.
- COMSEC/TEMPEST Principles.
- Counterintelligence Measures.
- Operations Security OPSEC Planning.
- Special Access Programs SAP Compliance.

Unit 10:

Advanced Security Techniques:

- Threat Intelligence Analysis.
- Security Automation and Orchestration.
- Risk Assessment and Management.
- Cybersecurity Incident Response.
- Security Governance and Compliance.