# Wi-Fi Security (CWSP) Training

## Course Contents

**Module 1 – Security Fundamentals**

- Security Basics
- CWNA Security Review
- Industry Organizations
- Terminology
- Wireless Vulnerabilities

**Module 2 – Wireless Security Challenges**

- Network Discovery
- Pseudo-Security
- Legacy Security Mechanisms
- Network Attacks
- Recommended Practices

**Module 3 – Security Policy**

- Defining Security Policies
- Policy Enforcement
- Policy Management
- Policy Types

**Module 4 – Understanding Authentication**

- Passphrase Authentication
- AAA
- RBAC
- RADIUS
- 802.1X
- EAP

**Module 5 – Authentication and Key Management**

- Robust Security Networks (RSN)
- RSN Information Element
- RSN Authentication and Key Management (AKM)

**Module 6 – Encryption**

- Encryption Fundamentals
- Encryption Algorithms
- WEP
- TKIP
- CCMP

**Module 7 – Security Design Scenarios**

- Virtual Private Networks (VPN)
- Remote Networking
- Guest Access Networks

**Module 8 – Secure Roaming**

- Roaming Basics and Terminology
- Pre-authentication
- PMK Caching
- Opportunistic Key Caching (OKC)
- 802.11r FT
- Proprietary Roaming
- Voice-Enterprise

**Module 9 – Network Monitoring**

- Wireless Intrusion Prevention Systems (WIPS)
- WIPS Deployment Models
- WIPS Policy
- Threat Mitigation
- Location Services
- WNMS

- Protocol Analysis
- Spectrum Analysis