Airport Network Security Training Course

Professional Development Training Course Outline

Category	Aviation and Airport Management	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Airports are increasingly dependent on interconnected digital systems that support air traffic operations, passenger processing, baggage handling, surveillance, communication, and critical infrastructure. As cyber threats continue to evolve, Airport Network Security has become a strategic priority for aviation authorities, airport operators, airlines, and regulatory agencies. Airport Network Security Training Course equips participants with advanced knowledge of cybersecurity frameworks, network defense strategies, cyber resilience, threat intelligence, risk management, zero-trust architecture, secure network design, and regulatory compliance. Participants will gain practical skills to protect airport operational technology (OT), information technology (IT), and mission-critical aviation systems from cyber threats while ensuring operational continuity.

The course combines international best practices, ICAO cybersecurity recommendations, aviation security standards, digital transformation strategies, cloud security, artificial intelligence-driven threat detection, endpoint protection, and incident response planning. Through practical exercises and global case studies, participants will learn how to identify vulnerabilities, implement layered security controls, strengthen airport cyber resilience, secure communication networks, and develop effective cybersecurity governance aligned with modern airport operations.

Programme Curriculum

Airport Network Security Training Course

Introduction

Airports are increasingly dependent on interconnected digital systems that support air traffic operations, passenger processing, baggage handling, surveillance, communication, and critical infrastructure. As cyber threats continue to evolve, Airport Network Security has become a strategic priority for aviation authorities,

airport operators, airlines, and regulatory agencies. Airport Network Security Training Course equips participants with advanced knowledge of cybersecurity frameworks, network defense strategies, cyber resilience, threat intelligence, risk management, zero-trust architecture, secure network design, and regulatory compliance. Participants will gain practical skills to protect airport operational technology (OT), information technology (IT), and mission-critical aviation systems from cyber threats while ensuring operational continuity.

The course combines international best practices, ICAO cybersecurity recommendations, aviation security standards, digital transformation strategies, cloud security, artificial intelligence-driven threat detection, endpoint protection, and incident response planning. Through practical exercises and global case studies, participants will learn how to identify vulnerabilities, implement layered security controls, strengthen airport cyber resilience, secure communication networks, and develop effective cybersecurity governance aligned with modern airport operations.

Course Objectives

By the end of this course, participants will be able to:

1. Understand airport network security architecture and cybersecurity principles.
2. Identify emerging cyber threats targeting aviation infrastructure.
3. Implement Zero Trust security frameworks for airport networks.
4. Strengthen airport cyber resilience using modern defense strategies.
5. Conduct cybersecurity risk assessments and vulnerability analysis.
6. Secure Operational Technology (OT) and Information Technology (IT) environments.
7. Apply network segmentation and secure access management techniques.
8. Develop effective airport cyber incident response and recovery plans.
9. Utilize AI-powered threat detection and Security Operations Centers (SOC).
10. Ensure compliance with ICAO cybersecurity guidance and international standards.
11. Protect airport cloud services, IoT devices, and connected infrastructure.
12. Improve cybersecurity governance and digital risk management.
13. Build a proactive cybersecurity culture across airport operations.

Organizational Benefits

- Strengthened protection of critical airport infrastructure.
- Improved cyber resilience against evolving threats.
- Reduced operational disruptions from cyber incidents.
- Enhanced compliance with international aviation cybersecurity standards.
- Better protection of passenger and operational data.
- Improved incident detection and response capabilities.
- Increased business continuity and disaster recovery readiness.
- Stronger collaboration between IT, OT, and security teams.
- Reduced cybersecurity risks and financial losses.
- Enhanced organizational reputation and stakeholder confidence.

Target Audiences

- Airport IT Managers

- Network Engineers
- Airport Cybersecurity Officers
- Aviation Security Managers
- ICT Administrators
- Airport Operations Managers
- Regulatory Authority Personnel
- Airline Technology Specialists

Course Duration: 5 days

Course Modules

Module 1: Airport Network Security Fundamentals

- Airport network architecture
- Aviation cybersecurity principles
- Airport communication systems
- Network infrastructure components
- Cybersecurity governance
- Global Case Study: Heathrow Airport cybersecurity modernization

Module 2: Cyber Threats and Vulnerability Management

- Aviation cyber threat landscape
- Vulnerability identification
- Risk assessment techniques
- Penetration testing basics
- Threat intelligence integration
- Global Case Study: EasyJet cyberattack lessons

Module 3: Secure Network Design and Zero Trust

- Zero Trust architecture
- Network segmentation
- Identity and access management
- Multi-factor authentication
- Secure remote access
- Global Case Study: U.S. TSA cybersecurity initiatives

Module 4: Protecting Airport IT and OT Systems

- Operational Technology security
- SCADA protection

- Endpoint security
- Secure industrial networks
- Asset inventory management
- Global Case Study: Colonial Pipeline cybersecurity lessons for critical infrastructure

Module 5: Security Monitoring and Incident Response

- Security Operations Center functions
- SIEM implementation
- Incident detection
- Digital forensics basics
- Business continuity planning
- Global Case Study: Copenhagen Airport cyber resilience practices

Module 6: Cloud Security and Emerging Technologies

- Cloud security controls
- IoT security management
- Artificial Intelligence in cybersecurity
- Secure wireless networks
- Data encryption strategies
- Global Case Study: Singapore Changi Airport digital transformation security

Module 7: Compliance, Governance and Risk Management

- ICAO cybersecurity guidance
- ISO 27001 implementation
- NIST Cybersecurity Framework
- Regulatory compliance
- Enterprise cyber governance
- Global Case Study: European aviation cybersecurity regulatory practices

Module 8: Building Cyber Resilience

- Cybersecurity awareness programs
- Cyber resilience planning
- Crisis communication
- Continuous security improvement
- Future cybersecurity trends
- Global Case Study: Israel Ben Gurion Airport integrated cyber defense strategy

Training Methodology

- Interactive expert-led presentations.
- Facilitated group discussions.
- Hands-on cybersecurity simulations.
- Practical network security laboratories.
- Airport cyber risk assessment workshops.
- Global aviation case study analysis.
- Scenario-based incident response exercises.
- Group projects and collaborative learning.
- Knowledge assessments and feedback sessions.
- Action planning for workplace implementation.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.
f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com