Graduate Certificate in Aviation Cybersecurity (Asia-focus)

The Practice of Cybersecurity

This course is one of four cybersecurity courses required for the Aviation Cybersecurity Graduate Certificate. This 3-day, 24-hour course is designed with a particular emphasis on the Asia-Pacific Region.

Upon completion of this course, students should understand the overall concept and practice of information security as a comprehensive approach to securing an organization's digital assets. Students should also understand how information security fits into, and impacts, the entire organization, society and individuals. This course focuses on management and procedures rather than strictly technology.

Learning Objectives

Upon course completion, trainees will be able to:

- Describe access control mechanisms that work together to protect information and computing assets.
- Define network structures, transmission methods, and security measures used to provide confidentiality, integrity, and availability (CIA) of information.
- Propose governance and risk management policies, standards, procedures, and guidelines.
- Discuss the integration of information security methods and policies to organizational and legal structures.
- Apply controls to include security within systems and software applications development.
- Describe different cryptographic methods for the protection of information and communications.
- Articulate the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, and applications.
- Explain the various controls that can be employed to protect hardware and media.
- Devise incident response, disaster recovery, and business continuity plans.
- Identify relevant laws and regulations that impact the use of information, as well as investigative and evidence gathering methods that can be used to determine if a crime has been committed.

Course Contents

- Framework for Information Security
- Information Security - Roles and Responsibilities
- Data, Network, and Physical Security
- IT Systems Operations and Management
- Regulatory and Standards Compliance
- Information Security Risk Management
- Incident Management and Digital Forensics

Professional Education and Training
Embry-Riddle Aeronautical University – Asia
E-mail: wwaspet@erau.edu | Web: asia.erau.edu

- Disaster Recovery and Business Continuity
- Cybersecurity Breach Case Studies

Who Should Attend

- Students about to enter, or recently entered the aerospace workforce
- Aerospace professionals in an operations or management role (airport, airline, air navigation, MRO, legal, etc.)
- Government officials in the aerospace industry
- Other professionals interested in the Aviation Cybersecurity landscape in Asia-Pacific

Training Method

- Face-to-Face instructions in classroom or using Virtual Reality, or online synchronous
- Supported by practical case studies
- OJT may be provided if coordinated with airport authority.

General Information

Duration: 3 days or 24 hours

Venue: Local or Virtual Classroom

Participants: Maximum 25

Prerequisites:

- Familiarity with IT word-processing and presentation software
- Basic knowledge of aviation industry