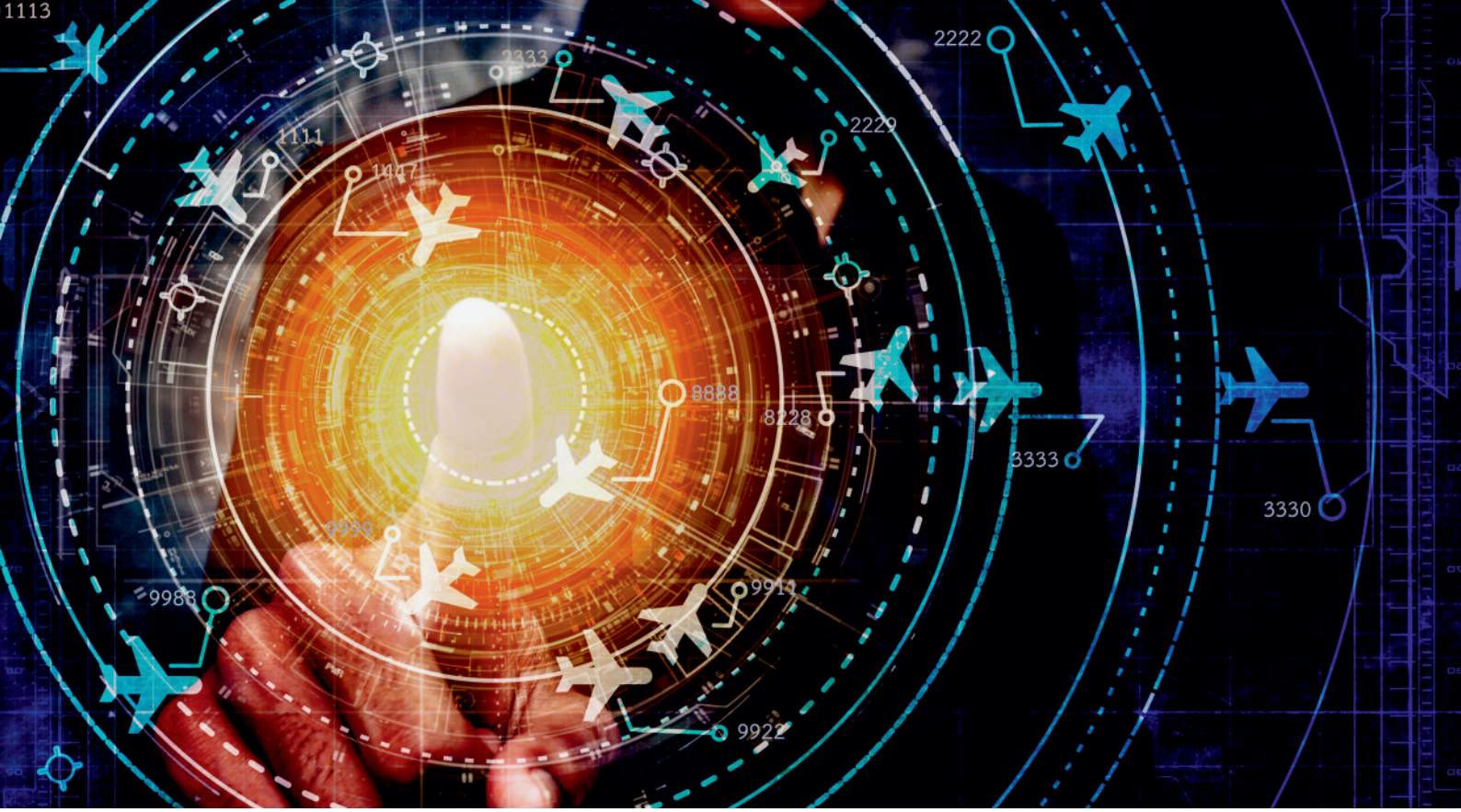

Aviation Cyber Security First Responder (ACSFR)

The Aviation Cyber Security First Responder (ACSFR) is a unique program aimed at all aviation industry employees. The program brings essential awareness in cybersecurity required for every individual servicing the aviation industry.

Outcome:

- Learn to protect sensitive information
- Prevent being a target of social engineering
- Defend against Phishing and Whaling attacks
- Secure your passwords and accounts
- Protect the organization from Ransomware attacks
- Prevent cyber-attacks on passengers and other critical airport systems
- Prevent misconducts with professional ethics at the workplace

Duration:

10 Hours / 2 Hours per Day / Five Days

GMR AVIATION ACADEMY
A Gateway to Global Aviation Learning
ISO 9001:2015 CERTIFIED

ISAC

CYBERSECURITY PROGRAMS

Course Details

Module 1 – Introduction
- What is a cyber law?
- Importance of cyber law and its usage
- What is a cyber-attack?
- What is a CII?
- What are the different types of attack and how to prevent them

Module 2 – The Cyber Kill Chain
- What is the Cyber Kill Chain?
- How it happens
- Impact of a cyber attack – Notable case studies in the Aviation Industry

Module 3 – Role of First Responder
- Who is a first responder?
- Why every role matters?
- How first responders can prevent potential cyber-attacks?

Module 4 – Dealing with Social Engineering Attacks
- What is a social engineering attack?
- Various techniques of social engineering
- Best practices to avoid social engineering attacks

Module 5 – Phishing and Whaling Attacks
- What are Phishing attacks?
- All about fake emails
- Spear-phishing
- Clone phishing
- Whaling – phishing for executives.
- Smishing and Vishing Attacks.
- Spotting and preventing phishing attacks

Module 6 – Malware and Ransomware Attacks
- What is malware?
- Trojan Horses
- Risk of free programs, games, and unverified software
- Ransomware attacks.
- How to prevent malware or ransomware attacks
- What do to if your system is compromised

Module 7 – Protecting customers
- Cyber-attacks on Point-of-sale (POS) devices – frauds and challenges.
- Credit card cloning
- Attack on WiFi Networks
- Rogue access points
- Man-in-the-middle attack.
- Best practices to protect consumers

Module 8 – Protecting Information and Disclosure
- Checking the security of your passwords
- Has your account been compromised before?
- Securing the data on your computer and personal devices.
- Baseline security for your systems
- Best practices for responding to emails asking for information
- Best practices for responding to questions by telephone and in-person
- Protecting sensitive files and information
- Dealing with colleagues, vendors, external parties, customers, suppliers, service providers etc.

Module 9 – Professional Ethics at Workplace
- What are professional ethics?
- Various frauds and misconducts in Aviation Industry
- Employee collusion with external parties.
- Risks to Airport Security from misconducts
- How to deal with unethical practices
- How to respond to potential misconducts
- Case Studies

Module 10 – Review and Assessment
- Review of best practices
- Acting as a First Responder
- Supporting and Helping others
- Additional Resources
- Quiz

GMR AVIATION ACADEMY
A Gateway to Global Aviation Learning
ISO 9001:2015 CERTIFIED

ISAC

CYBERSECURITY PROGRAMS

New Delhi, Academy, Terminal 2, opp. Departure Gate No. 1,
Indira Gandhi International Airport, New Delhi, India – 110037
Contact:+ 91 88103 76483

Hyderabad, Academy, Ground Floor, SSC, GMR Aero Towers,
Rajiv Gandhi International Airport, Shamshabad, Hyderabad, India – 500108
Contact:+ 91 70131 89812 / 99896 54915

/gmraviationacademy
/company/gmraviationacademy
/gmraviationacademy

www.gmraviationacademy.org
gmraa.contact@gmrgroup.in

Click Here to Register

To enroll & pay
NEFT/ RTGS details –

Bank Name: IDFC First Bank Limited
Branch Address: Barakhamba Road, New Delhi
Beneficiary Name: GMR Airports Limited
Current Account No. : 10057844842
IFSC Code: IDFB0020101

Or Click Here