INTERNAL SECURITY ACADEMY

"Power through pursuit of knowledge" is the motto of Internal Security Academy (**An ISO Certified Training Academy**). The Academy endeavors to impart professional knowledge/skills, inculcate right attitudes and develop values in the trainee officers to enable them to serve the nation better.

The Academy was established at Mount Abu (Rajasthan) on 1st February 1975 on shifting of the Central Police Training College (later rechristened, Sardar Vallabh Bhai Patel National Police Academy) to Hyderabad. ISA took over all properties from NPA which were either hired or owned by CPWD. The main Academy campus is the campus of erstwhile the Abu Lawrence School. **"Never give in"** the motto of erstwhile Abu Lawrence school is also a motivating factor of the academy besides our own motto.

THE MISSION

The primary mission of the Internal Security Academy is to orient/re-orient officers of the CRPF/CPMF/State Police forces to carry out their assigned tasks and responsibilities with right attitude, uprightness, dedication and with a strong commitment of service to the people. The Academy aims at quality training with total quality management of the Institution. The Academy is a **"Centre of Excellence"** for training and research in various fields.

Centre of Excellence

By: - R&D Cell
INTERNAL SECURITY ACADEMY
MOUNT ABU (RAJ.)
E-mail- dcradisa@crpf.gov.in

CYBER & INFORMATION SECURITY
COURSE SL NO. 15

19th to 27th July, 2022

INTERNAL SECURITY ACADEMY
MOUNT ABU (RAJ.)
(ISO-9001:2015)
www.crpf.gov.in/Internal Security Academy

AIM

To apprise the officers about the cyber security threats and the importance of cyber security.

SCOPE

The participants would be able to:

- Appreciate the Cyber Security threats in context with the Internal Security.
- To learn ways and means to ensure cyber security in our day to day functioning.

ELIGIBILITY

Asstt. Commandant to Commandant of the CRPF.

CAPACITY- 25

BLOCK TIME TABLE

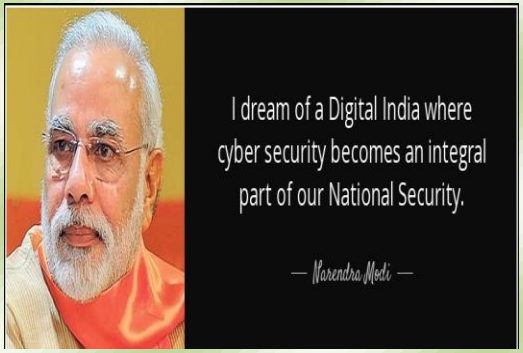
Duration of the Course.	08 Days
Total No. of working days.	08 Days
No. of periods in a day.	09 Periods
Total No. of periods.	72 Periods
Duration of period.	40 Minutes

METHODOLOGY

- Lectures & Presentations.
- Interactive learning and experience sharing.

CONTENT OF THE COURSE

- Basics of communication systems- Facsimile (Fax), E-mail, Voice mail, Internet, Multimedia, Teleconferencing, Mobile Phone Conversation, Video Conferencing, SMS, Advantages and limitations
- Transmission Media: Wired or Guided Media and Wireless or unguided Media. Radio and Microwave transmission. Media Cables - Twisted pair Cables, CAT Cables, Fiber Optic Cables, Co-axial cables, power lines, Attenuation, distortion, noise, throughput and comparison of media
- Topology and types of networks – LAN, WAN. Concept and topologies of network like Bus, Ring and Star. Common terminologies: LAN, WAN, Node, Host, Workstation, Bandwidth, Interoperability, Network Administrator, Network Security, Network, Components: Severs, Clients, Types of network: Peer to Peer, Clients Server.
- TCP/IP protocol stacks- Basic concept of Internet Protocols - Packet switching technology. Internet Protocols: TCP/IP, Router, Internet Addressing Scheme: Machine Addressing (IP address), E-mail Addresses.
- Wireless networks - Radio Communications, Cellular Radio, Mobile Telephony (GSM & CDMA), Satellite, Networks (VSAT), Mobile Adhoc Networks (MANET).



- The Internet - Addressing in Internet: DNS, Domain Name and their organization, understanding the Internet Protocol Address.
- Information security overview: Information Security – Need, Principles of information security. Best approach to implement information security - System vulnerability, computer frauds, computer abuse.
- Types of attacks.
- Goals for security - Introduction, need for security, Principles of Security.
- E-Commerce security.
- Computer forensics- Cyber forensics, cyber crime examples, forensics investigative incident, response actions, computer forensics tools.
- Steganography- Introduction to Information hiding – Brief history and applications of information hiding, Principles, of Steganography – Frameworks for secret communication, Security of Steganography systems.
- Overview of security threats- Introduction to security, information security, security threats and attacks.
- Weak/ strong passwords and password cracking - password management – viruses and related threats.
- Insecure network connections- prevent windows/OS for untrusted connections.
- Malicious code – types and effects on operating system for stealing of information, preventive measures.
- Cyber crimes and cyber terrorism – Case studies of investigations, online frauds and preventive measures.
- Introduction of cryptography/ encryption - Cryptography, IPsec, SSL/ proxy, firewall, VPN.
- Digital signatures - Public Key Infrastructure (PKI), Digital Certificates, Certificate Authorities.
- Overview of security management: Security Management of IT Systems, Information Security Management Information classification, Password management.
- Security policy- Information Security Policies, Procedures, and Standards.
- Security procedure and guidelines- Guidelines for effective information, security management.
- Ethics and best practices- Ethics, legal issues and social responsibility.
- Security audit - Introduction to information security audit and principles of audit.
- Security laws, I.T. Act 2000 – Provision of Law and case study.

ज्ञानेन साध्यते शक्ति