CYBER AND INFORMATION SECURITY COURSE

(Approved by Training dte. Signal No. S.XII. 10/2014-TRG.DA.13, dtd 24/11/14)

AIM

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

SCOPE OF THE COURSE: - The participants will be able to

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

METHODOLOGY:-

1. Lectures & Presentations.
2. Interactive learning and experience sharing.

ELIGIBILITY:-

Assistant Commandants to Commandants of CRPF.

CAPACITY:-

BLOCK TIME TABLE

Duration of the course
No. of periods in a day.
Total periods in the course
Duration of each period

SYLLABUS

S/NO	SUBJECT
01	Overview of networking concepts.
02	Information security concepts.
03	Security threats and vulnerabilities, cryptography/encryption.
04	Security Management Practices/ Security Laws and Standards.
05	Access control and intrusion detection, server management and firewalls, security for VPN and next generation technologies.
06	System Security, OS Security, Wireless Networks and Security.
07	Course overview, opening & valedictory ceremony.

DETAILED SYLLABUS

1. Overview of Networking Concepts

S/No	Subject
1	Basics of communication systems- Facsimile (Fax), E-mail, Voice mail, Internet, Multimedia, Teleconferencing, Mobile Phone Conversation, Video Conferencing, SMS, Advantages and limitations
2	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

3	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.
4	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.
5	Wireless networks - Radio Communications, Cellular Radio, Mobile Telephony (GSM & CDMA), Satellite, Networks (VSAT), Mobile Adhoc Networks (MANET).
6	The Internet - Addressing in Internet: DNS, Domain Name and their organization, understanding the Internet Protocol Address.

3. Information Security Concepts

S/No	Subject
1.	Information security overview: Information Security – Need, Principles of information security. Best approach to implement information security - System Vulnerability, Computer frauds, computer abuse.
2.	Types of attacks.
3.	Goals for security - Introduction, need for security, Principles of Security.
4.	E-Commerce security.
5.	Computer forensics- Cyber forensics, cyber crime examples, forensics investigative incident, response actions, computer forensics tools.
6.	Steganography- Introduction to Information hiding – Brief history and applications of information hiding, Principles, of Steganography – Frameworks for secret communication, Security of Steganography systems.

4. Security Threats and Vulnerabilities

S/No	Subject
1.	Overview of security threats- Introduction to security, information security, security threats and attacks.
2.	Weak/ strong passwords and password cracking - password management – viruses and related threats.
3.	Insecure network connections- prevent windows/OS for untrusted connections.
4.	Malicious code – types and effects on operating system for stealing of information, preventive measures.
5.	Cyber crimes and cyber terrorism – Case studies of investigations, online frauds and preventive measures.

4. Cryptography / Encryption

S/No	Subject
1.	Introduction of cryptography/ encryption - Cryptography, IPsec, SSL/ proxy, firewall, VPN.
2.	Digital signatures - Public Key Infrastructure (PKI), Digital Certificates, Certificate Authorities.

6. Security Management

S/No	Subjects
1.	Overview of security management: Security Management of IT Systems, Information Security Management Information classification, Password management.
2.	Security policy- Information Security Policies, Procedures, and Standards.
3.	Security procedure and guidelines- Guidelines for effective information, security management.
4.	Ethics and best practices- Ethics, legal issues and social responsibility.
5.	Security audit - Introduction to information security audit and principles of audit.
6.	Security laws, I.T. Act 2000 – Provision of Law and case study.

6. Access Control and Intrusion Detection

S/No	Subjects
1.	Overview of identification and authorization - Identification, Authentication, Authentication by passwords, Protecting passwords, Types of access control
2.	Overview of IDS: Concept, Scanning, filtering and blocking. Vulnerabilities. Sources of vulnerabilities, Viruses and content filtering.

7. Server Management, Firewalls & Ethical Hacking

S/No	Subjects
1.	Types of firewalls features, DMZ and firewalls features – use and importance of firewall.
2.	Types of Hacking & Ethical hacking, Hacking Windows operating system – Network hacking – Web hacking – Password hacking and techniques.

7. Security for VPN and Next Generation Technologies

S/No	Subjects
1.	VPN Security.- Introduction of virtual private network, Types and technologies used in VPN.

9. System Security

S/No	Subjects
1.	Desktop security - Intruders, Viruses and Related Threats, Examples using available software platforms/case tools.
2.	Email security: Prevents Email Data Leakage, Email Quarantine.
3.	Web Security: web authentication SSL, Content filtering.

10. OS Security

S/No	Subjects
1.	OS Security vulnerabilities, updates and patches.
2.	OS integrity checks.
3.	Anti-virus software.
4.	Configuring the OS for security.
5.	OS security Vulnerabilities updates and patches.

11. Wireless Networks and Security

S/No	Subjects
1.	Components of wireless networks – hotspots, access points use and security of hot spots.
2.	Security issues in wireless - Security Principles, Authentication, Access control and Authorization.

12. Miscellaneous

S/No	Subjects
1.	Course overview, opening & valediction ceremony.

Note:- 1) In addition to above, brain storming/open sessions/group discussions/workshops, screening of training films etc. will also be a part of the course in pursuance to Training Directorate, CRPF directives to include smart practices.

2) Academy can do some para-phrasing of the sub-topics mentioned in detailed syllabus as per need, requirement, immediate feedback and utility of trainees, without changing the block time table and block syllabus.

****