

S.S. Jain Subodh P.G. College, Jaipur

(Autonomous)

Skill Enhancement Course (SEC)

Cyber Security and Ethics

Credits: 2
Maximum Marks: 50

Classes per Week: 2
EoSE: 35
CIA: 15

Unit I

Fundamentals of Cyber Security and Threat Landscape: Importance and challenges in Cyber Security, Cyberspace, and Cyber threats, Cyber warfare, CIA Triad, Cyber Terrorism, Cyber Security of Critical Infrastructure. Cyber Attacks and Intrusion Techniques: Types of Hackers - Hackers and Crackers, Cyber Attacks and Vulnerabilities, Malware threats, Sniffing, Gaining Access - Escalating Privileges, Executing Applications, Hiding Files, Covering Tracks. Worms, Trojans, Viruses, Backdoors

Unit II

Ethical Hacking and Information Security Practices: Ethical Hacking Concepts and Scopes, Threats and Attack Vectors, Enterprise Information Security Architecture, Vulnerability Assessment and Penetration Testing. Legal Framework and Countermeasures in Cyber Security: The Indian IT Act 2000 and amendments, Hackers-Attacker-Countermeasures, Web Application Security, Counter Cyber Security Initiatives in India, Cyber Security Incident Handling, Cyber Security Assurance

Unit III

Social Ethics: Ethics in the Business World; Corporate Social Responsibility; Fostering Corporate Social Responsibility and Good Professional Ethics; Improving Business Ethics; Ethics in Information Technology; Managing IT Worker, Encouraging Professionalism of IT Workers. Social Engineering and Insider Threats: Types of Social Engineering - Insider Attack - Preventing Insider Threats - Social Engineering Targets and Defence Strategies.

Unit IV

Cyber Ethics: The Importance of Cyber Law, Significance of Cyber-Ethics, Need for Cyber Regulations and Ethics. Ethics in Information society, Introduction to Artificial Intelligence Ethics: Ethical Issues in AI and core Principles, Introduction to Blockchain Ethics.

Suggested Books and References

1. Cyber Security and Cyber Laws Nilakshi Jain Wiley
2. Mike Shema, Anti-Hacker Tool Kit (Indian Edition), Publication McGraw Hill.
3. Nina Godbole and Sunit Belpure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Publication Wiley.
4. Marjie T. Britz, Computer Forensics and Cyber Crime: An Introduction, Pearson Education
5. Debirag E. Bouchoux, Intellectual Property, Cengage Learning.

Course Learning Outcomes:

- Remember the broad set of technical, social & political aspects of Cyber Security.
- Understand the importance of ethical hacking, its tool and ethical hacking process.
- Analyse security principles to system design.
- Understand the methods for authentication, access control, intrusion detection and prevention in Cyber Security
- Develop an understanding of ethical and socio-technical challenges faced by an ICT professional, including human factors, accessibility and usability.
- 6. Evaluate the role of standards, codes of conduct and legislative/regulatory obligations on the level of professionalism of the ICT industry.