Syllabus and Scheme of Examinations

Open Electives

Cyber Forensics & Security (Open Elective)

Paper Code: 16CSAO1

Course Outcomes:

By the end of the course the students will be able to:

CO1 Identify adware, malware, spam's on their e-mails

CO2 Understand of biometric security systems

CO3 Understand how to protect their windows, network, password or other assets on web from being compromised

CO4 Understand about search warrants, privacy act, procedure for responding to incidents, reporting procedures, legal considerations,

CO5 Understand the complete knowledge about information technology act 2000

External: 80 **Time: 3Hrs.**
Internal: 20

Note: Examiner will be required to set NINE questions in all. Question Number 1 will consist of total 8 parts (short-answer type questions) covering the entire syllabus and will carry 16 marks. In addition to the compulsory question there will be four units i.e. Unit-I to Unit-IV. Examiner will set two questions from each Unit of the syllabus and each question will carr y 16 marks. Student will be required to attempt FIVE questions in all. Question Number 1 will be compulsory. In addition to compulsory question, student will have to attempt four more questions selecting one question from each Unit.

UNIT-1

Introduction to Information Systems: Types of information Systems, Introduction to information security, Need for Information security, Threats to Information Systems, Information Security Investigations.

Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Security Threats to E-Commerce, Cyber-crimes.

UNIT-2

Cyber Forensics: Cyber Security, Cyber Security roles, Cyber Security Principles, Difference between information Security and Cyber Security, Types of Computer Forensics Technology, Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised Internet Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls Biometric Security Systems

UNIT-3

Ethical Hacking: Essential Terminology, Hacking windows – Network hacking – Web hacking – Password hacking, Malware, Scanning, Cracking. Digital Evidence in Criminal Investigations: The Analog and Digital World, Training and Education in digital evidence, Evidence Collection and Data Seizure: Why Collect Evidence, Collection Options Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Artifacts, Collection Steps, Controlling Contamination: The Chain of Custody, Reconstructing the Attack, The digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies.

UNIT-4

Cyber Crimes and Cyber Security Standards: Crime incident Handling Basics: Cyber activism, Tracking hackers, clues to cyber-crime, privacy act, search warrants, common terms, organizational roles, procedure for responding to incidents, reporting procedures, legal considerations, Information Technology Act 2000: Scope, jurisdiction, offense and contraventions, powers of police, adjudication, Intellectual property issues in cyberspace, ISO, Cop yright Act, Patent Law, Cyber Laws in India.

Reference Books:

1. V.K. Pachghare, “Cryptography and Information Security”, PHI Learning Private Limited, India.

2. William Stallings and Lawrie Brown, “Computer Security: Principles and Practice”, Prentice Hall.

3. Swiderski, Frank and Syndex, “Threat Modeling”, Microsoft Press.

4. John W. Rittinghouse, William M. Hancock, “Cyber Security Operations Handbook”, ElsevierPub.

5. Deborah G Johnson, “Computer Ethics”, 4th Edition, Pearson Education Publication.

6. Earnest A. Kallman, J.P Grillo, “Ethical Decision making and IT: An Introduction with Cases”, McGraw Hill Publication.

7. Dr. Surya Prakash Tripathi, RitendraGoyal, Praveen Kumar Shukla, “Introduction to Information Security and Cyber Law”, WilleyDreamtech Press.

8. Kenneth J. Knapp, “Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions”, IGI Global.

9. Cahnder, Harish, “Cyber Laws and Its Protection”, PHI Learning Private Limited,Delhi,India

10. Michael E. Whitman, Herbert J. Mattord, “Principles of Information Security”, Cengage Learning Pub.

11. Charles P. Pfleeger, Shari LawerancePfleeger, “Analysing Computer Security”, Pearson Education India.
12. Joseph M Kizza, “Computer Network Security”, Springer Verlag.