

CSCO 512: CYBER LAWS

Course Objectives:

1. To make the student aware about the legal aspects of our actions in cyberspace.
2. To make the student aware about the punishments for cyber offences.

Course Outcomes:

1. Student gets the required frame of mind to work in a IT powered workplace and all walks of life.
2. Student gets the knowledge of the need to protect the data privacy of the clients.

UNIT I

(12 Hours)

The Information Technology Act (IT Act), 2000 : Preliminary, Digital Signature And Electronic Signature, Electronic Governance, Attribution, Acknowledgement And Despatch Of Electronic Records, Secure Electronic Records And Secure Electronic Signature, Regulation Of Certifying Authorities, Electronic Signature Certificates, Duties Of Subscribers, Penalties, Compensation And Adjudication, The Appellate Tribunal, Offences, Intermediaries Not To Be Liable In Certain Cases, Examiner Of Electronic Evidence, Miscellaneous, Amendments As Introduced By The IT Amendment Act, 2008, Amendments to Indian Penal Code, Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934 due IT Act 2000.

UNIT II

(12 Hours)

Personal Data Protection Bill (PDPB), 2019: Preliminary, Obligations Of Data Fiduciary, Grounds For Processing Of Personal Data Without Consent, Personal Data And Sensitive Personal Data Of Children, Rights Of Data Principal, Transparency And Accountability Measures, Restriction On Transfer Of Personal Data Outside India, Exemptions, Data Protection Authority Of India, Penalties And Compensation, Appellate Tribunal, Finance, Accounts And Audit, Offences, Miscellaneous

UNIT III

(12 Hours)

General Data Protection Regulation (GDPR), 2018 of European Union : General provisions, Principles, Rights of the data subject, Controller and processor, Transfers of personal data to third countries or international organisations, Independent supervisory authorities, Cooperation and consistency, Remedies, liability and penalties, Provisions relating to specific processing situations, Delegated acts and implementing acts, Final provisions.

Textbooks :

1. “The Information Technology Act”, 2000
2. “The Personal Data Protection Bill”, 2019 38
3. “General Data Protection Regulation(GDPR)”- Official Journal of the European Union, 2016, <https://gdpr-info.eu/>
4. “The Information Technology ACT”, 2008
5. “A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians”- Expert Committee Report under the Chairmanship of Justice B.N. Srikrishna, 2018
6. “Computer Forensics and Cyber Crime An Introduction”- Marjie T. Britz, Pearson, Third Edition, 2013

CSCO 513 : Ethical Hacking and Digital Forensics

Course Objectives:

1. To make the student aware of the need to ethically hack one's own systems and network to know the loopholes.
2. To make the student aware of the forensics which need to be performed to produce digital trails of crimes in the modern world

Course Outcomes:

1. Student gets the skills and the knowledge of the tools required for performing ethical hacking and the digital forensics
2. Student gets the legal architecture of the nation which needs to be observed while performing ethical hacking and digital forensics

UNIT I

(12 Hours)

HACKING WINDOWS : Network Hacking, Web Hacking, Common Network Hacking Techniques, Password hacking, Cracking Passwords, Input Validation Attacks, SQL Injection Attacks, Buffer overflow attacks, Privacy Attacks,

TCP / IP AND FIREWALLS : TCP/IP Checksum, TCP / IP and Firewalls, IP Spoofing, Services Vulnerable to IP Spoofing, Port Scanning, DNS Spoofing, DNS ID Spoofing, DOS Attack, Application Level Attacks, Distributed Denial-of-Service Attacks (DDoS), DDoS Tools, UDP Flooding, Firewalls, Packet Filtering Firewall, Filtering on IP Header Criteria, Application Proxy Firewalls, Firewall's security policy, Batch File Programming

UNIT II

(12 Hours)

COMPUTER FRAUD: Insider Threat Concepts, Insider Threat Study, Methodology for the Optimization of Resources in the Detection of Computer Fraud, Managing the Insider Threat, The Insider Threat Strategic Planning Process, Cyber-Security Risk Governance Processes for Web-Based Application Protection (Understanding the External Risks and Internal Information Security Risks), The Risk Management Process, The Tailored Risk Integrated Process (TRIP), Security Controls in Application Systems Controls (ISO 27001, The Strategic Planning Process for Reducing the Insider Threat, The Threat Assessment Matrix, Application and Code Review, Strategic, Legal/Regulatory, and Operational Risk Ratings, The Information Security Scorecard, Develop Security Patterns for Applications/ Systems Software Engineering (Process and Product Improvements), Implemented Software Engineering InfoSec Process and Product Improvements

UNIT III

(12 Hours)

ARCHITECTURE STRATEGIES: Architecture strategies for computer fraud prevention, Architectural Strategies to Prevent and Detect ICF, Intrusion Detection Systems, NIDS Network Intrusion Detection Systems, Host-Based Intrusion Detection Systems (HIDS), The Penetration Testing Process, Web Services-Reducing Transaction risks, Extensible Markup Language (XML), XML and Security, Simple Object Access Protocol (SOAP), Problems with Web Services Security, **FRAUD SELECTION & DETECTION:** Key Fraud Indicator selection process, Macro Computer Fraud Taxonomy, Key fraud signature selection process, Accounting Forensics, Computer Forensics, Journaling and its requirements, The National Industrial Security Program Operating Manual (NISPOM), Journaling Risk/Controls Matrix, Standardised Logging Criteria for Forensic Photo Frames, Neural networks – Misuse detection and Novelty detection.

Textbooks :

Textbooks :

1. Kenneth C. Brancik, Insider Computer Fraud, Auerbach Publications Taylor & Francis, Group 2008.
2. Ankit Fadia, Ethical Hacking, Second Edition Macmillan India Ltd, 2006.
3. <https://healholistic.files.wordpress.com/2013/08/batch-file-programming-ankitfadia.pdf>.
4. <https://www.princeton.edu/~rblee/ELE572F02presentations/DDoS.pp> Permission to reproduce extracts from BS ISO/IEC/2700: 2005 is granted by BSI. British Standards can be obtained in PDF format from the BSI Online Shop: <http://www.BSI-Global.com/en/shop>
5. GTAG (Global Technology Audit Guide), Application Based Controls. The Institute of Internal Auditors, 2005.
6. The FFIEC Information Security Booklet, 2006.
7. Komanosky, Sasha. Enterprise Security Patterns, June 2004. The original source for the security pattern was the 3/03I SSA Password/Journal Enterprise Security Patterns
8. Caudill, Maureen and Butler, Charles, Naturally Intelligent Systems, MIT Press, Cambridge, MA, 1992.
9. Hawkins, Jeff, On Intelligence, Times Books, Henry Holt, New York, 2004.
10. Saffron Technologies, Technical White Paper, Morrisville, NC, 2004 (www.saffrontech.com).
11. Nigrini, Mark, Fraud Detection—I've Got Your Number. Journal of Accountancy, May, 79–83, 1999.