Fundamentals of Information Security (MIT(CS)-101)

BLOCK I

UNIT I: INTERNET

HISTORY OF INTERNET, HOW INTERNET WORKS?, Hosts and Domain Names, Path Name and File Name, ADDRESSING SCHEME IN THE INTERNET, IP versions, IPv4 Addresses, Subnetting, Private Addresses, IPv4 address exhaustion, IPv6 Addresses, Private addresses, IP Subnetworks, IP address assignment, Methods, Uses of dynamic address assignment, Address autoconfiguration, Uses of static addressing, Conflict, Routing, Unicast addressing, Broadcast addressing, Multicast addressing, Anycast addressing, Public addresses, Modifications to IP addressing, IP blocking and firewalls, IP address translation, INTERNET SERVICE PROVIDER, Classification of ISP, Access providers ISP, Mailbox providers, Hosting ISPs, Transit ISP, Virtual ISPs, Free ISPs, Wireless ISP, DOMAIN NAME SYSTEM(DNS), How does it work?, Top-Level Domain(TLD), Second-Level Domain, WORLD WIDE WEB(WWW), Is Intenet and www similler?, The www, The Internet, APPLICATION OF INTERNET.

UNIT II: MODELS OF E-GOVERNANCE

E-GOVERNANCE, Benefits of e-governance, Evlolution of e-governance in India, AIM OF E-GOVERNANCE, STAGES OF E-GOVERNANCE, MODELS OF E-GOVERNANCE, Broadcasting Model, Comparative Analysis Model, Critical Flow Model, E-Advocacy Model, Interactive Service Model, LEGAL AND POLICY FRAMEWORK FOR FACILITATING ICT IN E-GOVERNANCE, SIGNIFICANCE OF E-GOVERNANCE, CHALLENGES IN THE IMPLEMENTATION OF E-GOVERENCE , EVOLUTION IN E-GOVERNANCE AND MATURITY MODELS, Difference between E-Government and E-Governance, Levels of E-Governance, e-Governance maturity model, DIGITAL INDIA PROGRAM, Services, TOWARDS GOOD GOVERNANCE THROUGH E-GOVERNANCE

UNIT III: E-READINESS

STAGES IN E-GOVERNANCE, E-READINESS, Is the Technology Infrastructure Ready?, Is the Legal Infrastructure Ready?, Is the Institutional Infrastructure Ready?, Is the Human Infrastructure Ready?, Is the Technology framework Ready?, Is the Leadership and Strategic Thinking Ready?, BENEFITS OF E-GOVERNANCE.

UNIT IV: E-COMMERCE

INTRODUCTION, E-COMMERCE, Advantages of E-Commerce, Challenges in E-Commerce, E-COMMERCE BUSINESS MODELS, INFRASTRUCTURE, National Information Infrastructure, Message Distribution Infrastructure, Electronic Publishing Infrastructure,

Business Services Infrastructure, Electronic Commerce Application, PAYMENT SYSTEMS, Electronic Funds Transfer, Digital Cash, e-cash, Credit card, Google Wallet.

BLOCK II

UNIT I: INTRODUCTION TO CYBER CRIME

INTRODUCTION, Classification of Cyber Crimes, Reasons for Commission of Cyber Crimes, MALWARE AND ITS TYPES, Adware, Spyware, Browser hijacking software, Virus, Worms, Trojan Horse, Scareware.

UNIT II: KINDS OF CYBER CRIME

KINDS OF CYBER CRIME, Cyber Stalking, Child Pornography, Forgery and Counterfeiting, Software Piracy and Crime related to IPRs, Cyber Terrorism, Phishing, Computer Vandalism, Computer Hacking, Creating and distributing viruses over internet, Spamming, Cross Site Scripting, Online Auction Fraud, Cyber Squatting, Logic Bombs, Internet Time Thefts, Web Jacking, Denial of Service Attack, Salami Attack, Data Diddling, Email Spoofing.

UNIT III: ORGANIZED CYBER CRIME

ORGANIZED CRIME, Types of organized crime groups, Classification of Cyber Crimes, Cyber Crime and Cyber Terrorism, Information Warfare and surveillance, IT ACT 2002, Objects and Reasons, Applicability of the Act, Exceptions to the Act, Basic Characteristics of the Act, Objectives of the Act, Definitions, Why was IT Act 2000 amended in 2008?, Data privacy, What are the responsibilities of a company handling personal data?, What is the punishment for cyber crimes?, Who can conduct RAIDS AND INVESTIGATION for Cybercrimes?

UNIT IV: CYBER CRIMES - CASE STUDIES

INTRODUCTION, CYBER CRIME - CASE STUDIES, Cyber Stalking, Cyberstalking Facts, Examples of Cyberstalking, Guidelines for victim of Cyberstacking, Prevention Tips from Cyberstalking, Below are some tips useful for the prevension of cyber stalking: Case Study on Cyber stalking, Ransomware, How does Cryptolocker work?, Prevention Tips from RANSOMWARE, Case studies on Ransomware, Silkroad, Case Studies on Silkroad, Phishing, Phishing Types, Anti-Phishing Groups, Legal Clause in Indian Penal Code, Case Studies in Phishing, 419(Advance-Fee Fraud) Scam, What is 419 (Advance-fee Fraud) Scam?, Types of advance fee fraud and other Nigeria-related fraud emails, What should you do if you‘re a victim of 419 (Advance-fee Fraud) Scam, Protection Tips, Case Studies on 419 Scam, Unexpected prize and lottery, Dating and Romance Scam.

BLOCK III

UNIT I: INFORMATION SECURITY

INTRODUCTION, WHAT IS INFORMATION SECURITY? Various Definitions, Information assurance, When Are We Secure?, MODELS FOR DISCUSSING SECURITY ISSUES, The Confidentiality, Integrity and Availability Triad, Confidentiality, Integrity, Availability, Relating the CIA triad to security, THE PARKERIAN HEXAD, Confidentiality, Integrity and Availability, Possession or Control, Authenticity, Utility, ATTACKS, Types of Attacks, Interception, Interruption, Modification, Fabrication, THREATS, VULNERABILITIES AND RISK, Threats, Vulnerabilities, Risk, Impact, CONTROLS, Physical, Logical, Administrative, DEFENSE IN DEPTH, Layers. INFORMATION SECURITY IN THE REAL WORLD.

UNIT II: INFORMATION SECURITY MANAGEMENT SYSTEMS

INTRODUCTION, WHY IS INFORMATION SECURITY IMPORTANT?, INFORMATION, INFORMATION SECURITY AND INFORMATION SECURITY MANAGEMENT, What is information?, What is information security?, What is information security management?, INFORMATION SECURITY IMPERATIVES AND INCENTIVES, Imperatives, Incentives, INFORMATION ASSETS, Information in an e-business age, Scarcity and Shareability, Confidentiality, integrity and availability, PLANNING AN INFORMATION SECURITY MANAGEMENT SYSTEM, The Standard's approach to planning an ISMS, ISMS documentation, Asset identification, Risk assessment, Risk treatment, Other approaches to information security management, SETTING UP AN ISMS, ISMS DOCUMENTATION, Context, scope and information security policy, The Statement of Applicability, RISK ASSESMENT AND ASSET IDENTIFICATION, A systematic approach to risk assessment, Threats, outcomes and impacts, Threats and vulnerabilities, Likelihood, impact and risk, Asset identification, THE PDCA CYCLE.

UNIT III: CYBER SECURITY TECHNIQUES FOR SECURE E-COMMERCE

ELECTRONIC COMMERCE, HISTORY, BUSINESS MODEL, REVENUE MODEL, CONCERNS, Security, Privacy and confidentiality, Authenticity, Data integrity, Non-repudiation, Access control, Availability, SECURITY SOLUTIONS, Access and data integrity, Encryption, Digital certificates, Digital signatures, E-COMMERCE INDENTIFICATION AND IDENTIFICATION TYPES, IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION, Identification, Authentication, Authorization, TYPES OF ECOMMERCE AUTHENTICATION, TYPES OOF BIOMETRIC AUTHENTICATION, OTHER FORMS OF AUTHENTICATION, SECURE ELECTRONIC TRANSACTION, History and development, Key features, Participants, How it Works, Dual signature, Digital signature, Explanation, How they work, Notions of security, Applications of digital signatures, Authentication, Integrity, Non-repudiation, ADDITIONAL SECURITY PRECAUTIONS, Putting the private key on a smart card, Using smart card readers with a separate keyboard, Other smart card designs, Using digital signatures only with trusted applications, Using a network attached hardware security module, DIGITAL SIGNATURES VERSUS INK ON PAPER SIGNATURES, Some digital signature algorithms, THE CURRENT STATE OF USE- LEGAL AND PRACTICAL, INDUSTRY

STANDARDS, Using separate key pairs for signing and encryption. ANTIVIRUS SOFTWARE, Identification methods for viruses, Signature-based detection, Heuristics, Rootkit detection, Real-time protection, ISSUES OF CONCERN, Unexpected renewal costs, Rogue security applications, Problems caused by false positives, System and interoperability related issues, Effectiveness, New viruses, Alternative solutions, Hardware and network firewall, Cloud antivirus, Online scanning, Specialist tools, FIREWALL, COMPUTER FORENSICS, Use as evidence, Forensic process, Techniques, Cross-drive analysis, Live analysis, Deleted files, Volatile data, Analysis tools, Stochastic forensics, STEGANOGRAPHY.

UNIT IV: ETHICAL ASPECT OF INFORMATION SECURITY

INTRODUCTION, COMPUTER SECURITY AND ETHICS, The Moral Importance of Computer Security, How does computer security pose ethical issues?, Computer Security and National Security, ETHICAL ISSUES IN COMPUTER SECURITY, Hacking and Computer Crime, Cyberterrorism and Information Warfare, Moral Responsibilities of Information Security Professionals, INFORMATION PRIVACY AND ETHICS, What is Privacy and Why is It Important?, Information Technology and Privacy, PRIVACY ISSUES IN MODERN DATA MANAGEMENT, Internet Privacy, Record Merging and Matching and Data Mining, Privacy in Public, Biometric Identification, Ubiquitous Computing and Ambient Intelligence, TACTICS TO ENSURE COMPUTER SECURITY AND MAINTAIN PRIVACY.