B.TECH. CSE with Specialization in Cyber Security and Hacking

Departmental Elective-I	Information Security Fundamental(BCS 048)
Departmental Elective-II	Concepts of Ethical Hacking (BCS 058)
Departmental Elective-III	Physical Security(BCS 068)
Departmental Elective-IV	Data Security (BCS 077)
Open Elective	Network Management(BOE 077)
Departmental Elective-V	I T Network Security (BCS 087)
Departmental Elective-VI	I T Business Continuity and Disaster Recovery Planning (BCS 091)

Department Elective-1

BCS-048 Information Security Fundamental

L T P **Credit-4**

3 1 0

Unit 1 **08 hours**

Security concepts: data threats, distinguish between data and information, cyber crime, difference between hacking and cracking and ethical hacking, recognize threats to data from force majeure like: fire, floods, war, earthquake, recognize threats to data from: employees, service providers and external individuals

Unit 2 **08 hours**

Value of information: understand the reasons for protecting personal information like: avoiding identity, theft, fraud, reason for protecting commercially sensitive information like preventing theft or miss use of client details financial information ,encryption ,password, confidentiality ,integrity availability identify data protection, retention and control requirement in your country

Unit 3 **08 hours**

Personal security: understand the terms social engineering and it implication like information gathering ,fraud computer system access identify method of social engineering like phone call, phishing, shoulder surfing identify theft and it applications personal , financial businesses legal identify method of identity theft like , information diving ,skimming pretexting

Unit 4 **08 hours**

File security: enabling/disabling macro security settings, seta password for files link: documents, compressed files, spreadsheets, understand the advantage and limitation of encryption

Unit 5 **08 hours**

Malware: Definition and function types of protection, Networks: networks types, function and limitation of a firewall

References:

1. William Stallings, “Cryptography and Network Security Principles and Practice”, 5th Edition, Pearson, 2013
2. Behrouz A Forouzan and Debdeep Mukhopadhyay, “Cryptography and Network Security”, 2nd Edition, Mc Graw Hill, 2007
3. Atul Kahate, “Cryptography and Network Security”, 2nd Edition, Mc graw Hill, 2007

Department Elective-II

BCS-058 Concepts of Ethical Hacking

L T P **Credit-4**

3 1 0

Unit –I **08 hours**

Ethical Hacking: Introduction, Networking & Basics, Foot Printing, Google Hacking, Scanning, Windows Hacking, Linux Hacking, Trojans & Backdoors, Virus & Worms, Proxy & Packet Filtering, Denial of Service, Sniffer, Social Engineering,

Unit –II **08 hours**

Introduction to Computer Systems and Networks , information systems and networks (including wireless networks) and their role in industry business and society, System and Network Vulnerability and Threats to Security , various types of attack and the various types of attackers in the context of the vulnerabilities associated with computer and information systems and networks.

Unit –III **08 hours**

Physical Security, Steganography, Cryptography, Wireless Hacking, Firewall & Honey pots, IDS & IPS, Vulnerability, Penetration Testing, Session Hijacking, Hacking Web Servers, SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow, Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobile s Phone Hacking

Unit –IV **08 hours**

An introduction to basic ethical hacking tools and usage of these tools in a professional environment in a form of project

Unit –V **08 hours**

An introduction to the particular legal, professional and ethical issues likely to face the domain of ethical hacking, Ethical responsibilities, professional integrity and making appropriate use of the tools and techniques associated with ethical hacking.

Reference Books:

1. Hands-On Ethical Hacking and Network Defense–By Michael T. Simpson, Kent Backman, James Corley
2. Official Certified Ethical Hacker Review Guide –By Steven De Fino, Barry Kaufman, Nick Valenteen.
3. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy(Syngress Basics Series)[Paperback]
4. Hands-On Ethical Hacking and Network Defense[Print Replica] [Kindle Edition

Departmental Elective-III

BCS -068 Physical Security

L	T	P	Credit-4
3	1	0	

UNIT I **08 hours**

Introduction: Physical Protections and attacks, locks and safes, Authentication technologies, Direct attacks against computer, special purpose machines physical intrusion detection. Need of physical security, physical security, physical security of information system resources, Physical entry controls

UNIT-II **08 hours**

Operating System Security: Operating system concepts, process security, memory and file system security, Application program

UNIT-III **08 hours**

Network Security-I: Network Security concepts, the data link layer, network layer, transport layer, denial of service Attacks.

UNIT-IV **08 hours**

Network Security-II: Application layer and DNS, firewalls, tunneling, intrusion detection wireless networking.

UNIT-V **08 hours**

Security models: Access control models administration and auditing, Kerberos, secure storage. Biometrics controls for security: biometrics based security issues and challenges, classification of biometrics applications, architectural and design issues in biometrics systems

References Books:

1. Network Security Essentials: Application and standards, 4th Edition, William Stalling, Prentice Hall, 2011
2. Nina Godbole.2011" Information systems security" security management, metrics, frameworks and best practices: Wiley
3. William Stallings, "Cryptography and Network Security Principles and Practice", 5th Edition, Pearson, 2013
4. Behrouz A Forouzan and Debdeep Mukhopadhyay, "Cryptography and Network Security", 2nd Edition, Mc Graw Hill, 2007
5. Atul Kahate, "Cryptography and Network Security", 2nd Edition, Mc graw Hill, 2007

Departmental Elective-IV

BCS-077: I T Data Security

L	T	P	Credit-4
3	1	0	

UNIT-I **08 hours**

Introduction: Fundamental Concepts of data security, Access control models, cryptographic concepts, and implementation and usability issues.

UNIT-II **08 hours**

Cryptography: Symmetric cryptography, Public Key Cryptography, Cryptographic Hash Functions, Digital Signatures, details on AES and RSA.

UNIT-III **08 hours**

Malware: Attacks, Computer viruses, Malware attacks privacy invasive software, counter measures.

UNIT-IV **08 hours**

Distributed application security: Data base security, E mail security, Payment systems and Auctions digital rights management, Social networking security

References Books:

1. Network Security Essentials: Application and standards, 4th Edition, William Stalling, Prentice Hall, 2011
2. Nina Godbole.2011" Information systems security" security management, metrics, frameworks and best practices: Wiley

Open Elective

BOE- 077: Network Management

L T P **Credit-4**

3 1 0

UNIT-I **08 hours**

Introduction-Network management architecture and organization-Network Management standards- Network Management Models -SNMP protocol - SNMP model- SNMP V1-SNMP V1 communication and functional model

UNIT-II **08 hours**

SNMP V2: system architecture- Structure of management information- Management Information Base- protocol-compatibility with SNMP V1.SNMP V3: key features-architecture-applications- Management Information Base-Security-User based security model-Access control Remote Monitoring: RMON SMI and MIB-RMON1-RMON2-ATM remote monitoring

UNIT-III **08 hours**

Network management tools, system and Engineering:-System Utilities for management-Network statistics measurement system- MIB Engineering -NMS design TMN: Operating Systems-Conceptual model-standards-architecture- Management service architecture- Implementation Network Management Applications: Network Configuration Management- Fault Management - Performance Management - Security Management-Accounting Management – Report Management-Policy based management-Service level management

UNIT-IV **08 hours**

Broadband Network management: ATM network management - MPLS OAM engagement – Optical and man feeder networks-Broadband access network-Cable access network management –DOCSIS network - DSL access network - ADSL managment-ADSL2,ADSL2+ and VDSL2-Passive Optical Network management. Ethernet management-802.11 Networks management CORBA based NM technology-XML based NM technology -Comparison of NM technologies-NM related standards.

References:

1. Mani Subrahmanian,"Network Management Principles and Practice", 2nd edition, Pearson Education, 2010
2. Stephen B. Morris, "Network Management, MIBs and MPLS", Prentice Hall, 2003.
3. Jianguo Ding , "Advances in Network Management" ,CRC Press, 2010.

Departmental Elective-V

BCS- 087: I T Network Security

L T P **Credit-4**

3 1 0

UNIT-I **08 hours**

Introduction: Motivating examples, Basic concepts: confidentiality, integrity, availability, security policies, Security mechanisms, assurance, Basic Cryptography: Historical background Transposition/Substitution, Caesar Cipher Introduction to Symmetric crypto primitives, Asymmetric crypto Primitives and Hash functions

UNIT-II **08 hours**

Secret Key Cryptography: Applications, Data Encryption Standard (DES), Encrypting large messages (ECB, CBC, OFB, CFB, CTR), Multiple Encryption DES (EDE)

Message digests: Applications, Strong and weak collision resistance, The Birthday Paradox, MD5, SHA-1

UNIT-III **08 hours**

Public Key Cryptography: Applications, Theory: Euclidean algorithm, Euler Theorem, Fermat Theorem, Totent functions, multiplicative and additive inverse, RSA, Selection of public and private keys

Authentication: Security Handshake pitfalls, online vs. offline password guessing, Reflection attacks, Per-session keys and authentication tickets, Key distribution centers and certificate authorities

UNIT-IV **08 hours**

Trusted Intermediaries: Public Key infrastructures, Certification authorities and key distribution centers, Kerberos

Real-time Communication Security: Introduction to TCP/IP protocol stack, Implementation layers for security protocols and implications I P sec: AH and ESP, I P sec: IKE, SSL/TLS

UNIT-V **08 hours**

Electronic Mail Security: Distribution lists, Establishing keys, Privacy, source authentication, message integrity, non-repudiation, Proof of submission, proof of delivery, message flow confidentiality, anonymity, Pretty Good Privacy (PGP)

Firewalls and Web Security: Packet filters, Application level gateways, Encrypted tunnels, Cookies, Web security problems

References:

1. Network Security Essentials: Application and standards, 4th Edition, William

Stalling, Prentice Hall, 2011

2. William Stallings, “Cryptography and Network Security Principles and Practice”, 5th Edition, Pearson, 2013
3. Behrouz A Forouzan and Debdeep Mukhopadhyay, “Cryptography and Network Security”, 2nd Edition, Mc Graw Hill, 2007
4. Atul Kahate, “Cryptography and Network Security”, 2nd Edition, Mc graw Hill, 2007

Departmental Elective-VI

BCS-091: I T Business Continuity and Disaster Recovery Planning

L T P **Credit-4**

3 1 0

UNIT-I **08 hours**

Introduction: Genesis of DRP, importance of BCP, business impact analysis, approaches to DRP, defining business goals to prepare for BCP and DRP, DRP test types, identification of key personnel, business interruptions preparedness checklist, business resilience

UNIT-II **08 hours**

Auditing for security: Basic term related to audits, security audits, need for security audits in organizations, organizational roles and responsibilities for security audit, types of security audits, approaches to audits , phases in security audits, budgeting for security audits

UNIT-III **08 hours**

Privacy best practices in organizations: Privacy organizational implications, privacy audits- driving factors, privacy practices , privacy auditing standards and privacy audits phases, privacy impact assessment of information systems applications, organizational reactions to privacy audits

UNIT-IV **08 hours**

Asset management: understanding the organizational context for asset management, security aspects in IT asset management's, asset management in organizations issues and challenges, asset management life cycle, benefits of asset management, role and responsibilities, managing software assets

UNIT-V **08 hours**

Ethical issues and intellectual property concerns: information system, characteristics of inside attacks on organizational information systems, natural of ethical issues in the networked enterprise, implications for the healthcare industry ethical and legal concerns, data auctioning, data hijacking and data laundering, ethical issues owing to information warfare, understanding ethical hacking, social engineering issues

References books:

1. Hiles, A. (ed.) 2011. The Definitive Handbook of Business Continuity Management (3rd ed.). West Sussex, UK: Wiley.
2. Nina Godbole.2011" Information systems security" security management, metrics, frameworks and best practices: Wiley