Certificate in Cyber Security (CCS)

Course Overview

Subject Code	Title of the paper	Credits
Semester 01		
CCCS-01	Cyber Crime & IT Act	4
CCCS -02	Fundamentals to Information Security	4
CCCS -03	Network Security	4
CCCS -04	Web Application Security	4

Cyber Crime & IT Act

Paper Code: CCCS-01 Credit: 04

Unit I

Definition and types of cybercrimes, electronic evidence and handling, electronic media, collection, searching and storage of electronic media, introduction to internet crimes, hacking and cracking, credit card and ATM frauds, web technology, cryptography, emerging digital crimes

UNIT-II

IT Act 2000; E-commerce; E-records, electronic signatures; Certifying Authorities and Cyber Appellate Tribunal. Retention and preservation of information; Protected systems and critical information infrastructure.

UNIT-III

Cyber offences and types; Cyber terrorism, Cybercrime investigation; Legal provision for financial transactions and documents, Digital evidence and its types. Admissibility in court of Law, Case studies

UNIT-IV

Cyber Security-Legal mandate, Compliance and Risk assessment, Cyber crisis management plan, General Data Protection Regulation (GDPR); OCED Guidelines; Personal Data Protection Bill 2019, Nodal Agencies for IT Security

Fundamentals to Information Security

Paper Code: CCCS-02 Credit: 04

Unit-I

Data & Information Definition, quality and need of information, categories of Information in business organization level of information, storage and retrieval of data, comparison of manual and electronic storage of data, the number system (binary, digital, octal and hexadecimal and their inter conversions), character encoding

Unit-II

Evolution of Encryption Techniques, Historical Perspective of Information Security, Various Encryption and Decryption Techniques, Stream and Block Cypher introduction, Introduction of Asymmetric and Symmetric Encryption Techniques

Unit-III

Definition of Threats and Vulnerability to Computerized Environment, Cyber Crimes categories, Threats due to Cyber Crimes, Risk Assessment, Techniques for Risk Evaluation.

Unit-IV

Worms and Botnets, DDoS: Spoofing, Reflection, Amplification, Routing, Spam, Phishing, Scams, DNS Security; Defenses: IDS and Firewalls, VPNs and Anonymous Communication, Internet Censorship, Human Factors and Usable Security

Network Security

Paper Code: CCCS-03 Credit: 04

Unit I

Define computer network, identifying basic networking elements and describing roles of Clients, Server, Peers, and Transmission Media & Protocols Network Services: File, print, Message, Database Application Identifying Differences bet. Centralized & distributed network architecture Identifying appropriate transmission media to meet a business need. Wireless Media, Network Connectivity devices, Modern repeaters, Hubs Bridges, Multiplexes and routers

Unit II

Identifying 7 Layers of OSI Physical Layer: Connection types used in Computer Network; Common Physical technologies used in computer Network: BUS, Ring, Star, Cellular, Analog & Digital Signals, bandwidth Data link Layer: Purpose of data link Layer, Switching Methods, Routing, Network layer connection services, Bridging Transport Layer: Purpose of transport layer, Address name resolution, Flow control, Error control Session Layer: Purpose of Session Layer, Session Administration, Dialog control methods Presentation Layer: Purpose of Presentation Layer, Application Layer: Purpose of Application Layer

Unit III

Identifying Network Classes, obtain register IP address, Domains, how Host name, host table and DNS work. Windows Internet naming services (WINS), Subnets, Subnet's mask Assigning and managing IP subnets.

Unit IV

Electronic Mail security – PGP, S/MIME – IP security – Web Security, SSL, TLS – Server Hardening, authentication and access control issues, CIA Triad, non-repudiation, Authorization, conventional encryptions techniques, public key cryptography, message confidentiality, message authentication, Intruders – Malicious software – viruses, botnets, worms – Firewalls. Types of Firewalls Adv. Topics including Blockchains, Cloud Security and IoT security.

Web Application Security

Paper Code: CCCS-04 Credit: 04

Unit I

Web Fundamentals – HTML, HTTP 1.0 and 1.1, Client-side scripting: JavaScript, Server-side scripting: PHP; Web server architecture - Windows & Linux, IIS and LAMP servers, and DMZ

Unit II

Overview of web authentication technologies, Recent attack trends, Web infrastructure security/Web application firewalls, Managing configurations for web apps, Authentication vulnerabilities and defence, Multifactor authentication

Unit III

Input-related vulnerabilities in web applications, SQL injection, Cross-site request forgery, Cross-site scripting vulnerability and defences, Unicode handling strategy, File upload handling, Business logic and concurrency

Unit IV

Introduction to Networks security, End point security, Mobile and web applications security, Risk Assessment, Common Mistakes in Development, Security Best Practices for Web Application & API Security, Secure SDLC, Threat Modelling, Source Code Review, VAPT, DevSecOps, What is DevSecOps, DevSecOps vs Secure SDLC