Certificate Programme in Cyber Security

Objective of the Course: The programme has been framed to achieve the following objectives

- To develop a basic understanding of the building blocks of cyber security.
- To develop an understanding and knowledge of the basic theory related to cyber security with good foundation on theory and practical.
- To be a foundation Certification Programme this will act as a feeder course for higher studies or professional career in cyber security.
- To acquire necessary and state-of-the-art skills to take up industry challenges in cybersecurity
- The ability to synthesize the acquired knowledge, understanding and experience for a better and improved comprehension of the cyber related problems

Learning Outcomes:

- Understanding the fundamentals of cybersecurity
- Knowledge of cybersecurity threats and vulnerabilities
- Proficiency in cybersecurity tools and technologies
- Ethical and legal considerations

Duration of the Course:
Certificate course: 6 months

Eligibility: Any student enrolled in the degree program of the college and having knowledge about the basics of Computers.

Sr. No.	Topics	Credits
1	CCCS-1-01T Data Communication and Networks CCCS-1-01P Data Communication and Networks Lab	Credits: 5(3 Th. 2 Lab)
2	CCCS-1-02T Fundamentals of Information Security CCCS-1-02P Fundamentals of Information Security Lab	Credits: 5(3 Th. 2 Lab)
3	CCCS-1-03T Cyber Attacks and Counter Measures CCCS-1-03P Cyber Attacks and Counter Measures Lab	Credits: 5(3 Th. 2 Lab)
4	CCCS-1-04T Cyber Security Techniques CCCS-1-04P Cyber Security Techniques Lab	Credits: 5 (3 Th. 2 Lab)
5	CCCS-1-05T Operating System CCCS-1-05P Operating System Lab	Credits: 5 (3 Th. 2 Lab)

CCCS-1-01T: Data Communication andNetworks

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 4
Pass Percentage: 40%

Objective

Objective of this paper is to explain the basic Data Communication and Computer Networks.

Section A

Unit I: Basic concepts: Components of data communication, modes of communication, standards and organizations, Network Classification, Network Topologies; Transmission media, network protocol; layered network architecture.

Unit II: Models: Overview of OSI reference model; TCP/IP protocol suite. Physical Layer: Cabling, Network Interface Card, Transmission Media Devices- Repeater, Hub, Bridge, Switch, Router, Gateway; Transmission impairments.

Unit III: Data Link Layer: Framing techniques; Error Control; Flow Control Protocols; Shared media protocols - CSMA/CD and CSMA/CA.

Unit IV: Network Layer: Virtual Circuits and Datagram approach, IP addressing methods – Subnetting; Routing Algorithms (adaptive and non-adaptive)

Section B

Unit V: Transport Layer: Elements of transport protocols – Addressing, Connection establishment and release, Flow control and buffering, Transport services, Transport Layer protocol of TCP and UDP.

Unit VI: Session and Presentation Layer: Session Layer – Design issues, remote procedure call. Presentation Layer – Design issues, Data compression techniques, Cryptography.

Unit VII: Application Layer: Application layer protocols and services – Domain name system, HTTP, E-mail, WWW, telnet, FTP, SMTP.

Unit VIII: Network Security: Common Terms, Firewalls, Virtual Private Networks.

Suggestive Readings

1. B.A. Forouzan: Data Communication and Networking, 4th Edition, Tata McGraw Hill, 2017.
2. A. S. Tanenbaum, Computer Networks, 5th Edition, Pearson, 2011
3. D.E. Comer, Internetworking with TCP/IP, Vol. I, Prentice Hall of India, 2015
4. W. Stalling, Data & Computer Communication, 8th edition, Prentice Hall of India, 2013
5. D. Bertsekas, R. Gallager, Data Networks, 2nd edition, Prentice Hall of India. 1992

CCCS-1-01P: Data Communication and Networks Lab

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 2

Pass Percentage: 40%

Practical will be Based on CCCS-1-01T: Data Communication and Networks.

CCCS-1-02T Fundamental of Information Security

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits:4
Pass Percentage: 40%

Objective

Objective of this paper is to explain the basic Fundamental of Information Security.

Section-A

Unit I: Internet: Address Scheme, IPV4, IPV6, IP Subnet and address assignment, Routing, Modifications to IP addresses, Classification of ISP, DNS, WWW,

Unit II: e-Gov: Aim, Stages, Models: Broadcast, Comparative Analysis's critical Flow, E-advocacy, Interactive service, e-Governance: Evaluation and Maturity e-readiness, e-comm: Business Models, Infrastructure, Payment Methods.

Unit III: Cybercrimes: Classification, Malware: Adware, Spyware, Browser Hijacking, Virus, Worm, Trojanhorse, Scareware , Kinds of Cyber Crime, Organised Crime, IT Act 2002

Unit IV: Cyber Crime Case Studies: Cyber Stalking, Ransomware, Silkroad, Phishing, Scam,

Section-B

Unit V: Information Security, models for discussing security issues, Parkerian Heaxd, Attacks, Threats, vulnerability and Risk, Control, Defense in Depth

Unit VI: Information Security Management, Imperatives and Incentives, Information Assets, Planning an Information Security Management System (ISMS), ISMS Documentation, Risk Assessment and Assets Identification, The PDCA cycle

Unit VII: Electronic Commerce: Business Model and Revenue Model, Concerns and Security Solution, Identification, Authentication, Authorization, Secure Electronic Transaction, Security Precautions, Industry Standards

Unit VIII: Antivirus Software, Issues and Concerns, Firewall, Computer Forensics, Steganography, Computer Security and Ethics, Ethical Issues, Information Privacy and Ethics, Privacy issues in Modern Data Management,

CCCS-1-02P: Fundamental of Information Security Lab

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 2

Pass Percentage: 40%

Practical will be Based on CCCS-1-02T: Fundamental of Information Security.

CCCS-1-03T Cyber Attacks and Counter Measures

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits:4
Pass Percentage: 40%

Objective
Objective of this paper is to explain the basic Cyber Attacks and Counter Measures.

Section-A

Unit I: Cyber Attacks: Introduction, Types. Assets: Identification, Accountability. Vulnerability and Threats, Risk Management, Qualitative Risk Assessment, Information Security Framework: Introduction, Policies, Standards, Baselines, Guidelines and Procedures.

Unit II: Security: Basics, User Access Controls, Authentication, Access Control: Framework, Techniques and Technologies, Training and Awareness and Its types, Technical Security Controls: Preventive, Detective, Corrective. Protection form malicious attacks

Unit III: Networks and Communication: Data Communication, Characteristics and components, Data flow. Computer Network, Categories, Protocol, External Services, Cloud Computing: Introduction, Models, Benefits, Challenges, Private, Public Clouds,

Unit IV: Software Engineering Life Cycle: Stages, Models: Waterfall, Iterative, Spiral, V-Model, Big Bang, Agile, RAD, Prototype,

Section-B

Unit V: Authentication: Authentication Vs Authorization, Methods and Protocols: Kerberos, SSL, Protocol, Password Authentication, Challenge-Handshake Authentication (CHAP), MS-CHAP, Extensible Authentication, Remote Authentication.

Unit VI: Service Set Identification (SSID), Encryption Methods: Wire Equivalent Privacy, WPA, WPA2, MAC Filtering, Wireless Routers, Creating Wireless Network, WLAN

Unit VII: Investigation Techniques and Cyber Forensics, Types of Investigation, Evidence and Analysis, Steps for Forensics Investigation, Forensics Tools, Investigation, Common Types of Email Abuse, Tracking Location of Email Sender, Scam or Hiex Emails and Websites, Fake Social Media Profile,

Unit VIII: Cryptography: Objectives, Type, OS Encryption, Public key Cryptography,

CCCS-1-03P: Cyber Attacks and Counter Measures Lab

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 2

Pass Percentage: 40%

Practical will be Based on CCCS-1-03T: Cyber Attacks and Counter Measures.

CCCS-1-04T Cyber Security Techniques

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits:4
Pass Percentage: 40%

Objective

Objective of this paper is to explain the basic Cyber Security Techniques.

Section-A

Unit I: IT Security Policies, Types of Information Security Policies, IT SECURITY PROCEDURES, ORGANIZATIONAL SECURITY: Physical Security, Financial Security, Online Security, Security Token, Electronic Mail Security, Pretty Good Privacy, Multipurpose Internet Mail Extensions, Message Authentication Code, Firewall, Malicious Software, Denial of Service Attack, Phishing,

Unit II: ATTACKS: Insider Attack and its Prevention, Outsider Attack and its Prevention, CYBER CRIME: Overview, Categories, Challenges, Complexities and effects, Intrusion Detection System (IDS): Introduction, Components, CHARACTERSTICS, Types of IDS: Network IDS, Host Based IDS, Misuse-Detection IDS, Anomaly- Detection IDS, STEPS TO INSTALL AN IDS IN AN ORGANIZATION, INCIDENT HANDLING,

Unit III: Assets: Introduction, SECURING AN ASSET, HARDWARE BASED SECURITY: Types, Functionality, Implementation, FIREWALL: Types, Hardware Based, Software Based, WIRELESS SECURITY, NFORMATION ASSURANCE: Introduction, Dimensions of McCumber Cube, CYBER SECURITY ASSURANCE FRAMEWORK – INDIA: Strategic Approach, Actions, Strategic Objectives,

Unit IV: CYBER SECURITY MATURITY AND SELF ASSESMENT: Cyber Security Capability Maturity Model (CMM), Selection of Cyber Capacity Building Factors, Guidelines for the use of Cyber CMM, Virus and its Types, Worm and its tyoes, Trojan Horse, Bot and Botnets, RANSOMWARE, ROOTKITS, EXPLOIT KITS, CYBER WEAPONS, POS MALWARE , MALWARE PERPETRATORS, MALWARE ATTACKING TECHNIQUES, MOBILE MALWARE TRANSITION: App Based Threats, OS based Threats, Android Security Threats, Android Security Threats,

Section-B

Unit V: Web Architecture: Hyper Text Markup Language (HTML), Uniform Resource Identifier, Hyper Text Transfer Protocol (HTTP), ATTAACKS ON APPLICATIONS, DEMONSTRATION OF IMPACT OF XSS VULNERABILITY, APPLICATION SECURITY, SOCIAL ENGINEERING: Life Cycle, TYPES: Physical, Remote, Computer-based, Phone Based,

Unit VI: COMPUTER FORENSICS PROCEDURE: Data Collection, Examination, Analysis, Reporting, DATA COLLECTION AND ACQUISITION, WINDOWS LIVE RESPONSE/ FORENSICS, Capturing Memory, Capturing the volatile data, Transferring data to the investigators machine, Introduction to Disk Image.

Unit VII: CYBER SECURITY INITIATIVES: National Cyber Security Policy, Critical Information Infrastructure Protection, Cyber Crisis Management Plan, CERT-IN AND OTHER AGENCIES: Indian Computer Emergency Response Team (CERT-In), Ministry of Communications & IT, Institute for Defense Studies and Analysis (IDSA) , National Intelligence Grid (NATGRID), National Counter Terrorism Centre, Crime and Criminal Tracking Network & Systems (CCTNS), Data Security Council of India (DSCI)

Unit VIII: RISK MANAGEMENT, RISK ASSESSMENT METHODOLOGIES, GLOBAL CYBERSECURITY INDEX AND CYBERWELLNESS PROFILES, NATIONAL CYBER SECURITY POLICY- INDIA,

CCCS-1-04P: Cyber Security Techniques Lab

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 2
Pass Percentage: 40%

Practical will be Based on CCCS-1-04T: Cyber Security Techniques.

CCCS-1-05T Operating Systems

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 4
Pass Percentage: 40%

Objective

Understanding basics of operating system viz. system programs, system calls, user mode and kernel mode. Working with CPU scheduling algorithms for specific situation, and analyze the environment leading to deadlock and its rectification. Exploring memory management techniques viz. caching, paging, segmentation, virtual memory, and thrashing.

SECTION A

UNIT- I: Introduction and System Structures: Computer-System Organization, Computer-System Architecture, Operating-System Structure, Operating-System Operations, Process Management, Memory Management, Storage Management, Protection and Security, Computing Environments, Operating-System Services, User and Operating-System Interface, System Calls, Types of System Calls, System Programs.

UNIT II: Process Management: Process Concept, Process Scheduling, Operations on Processes, Multi-threaded programming: Multithreading Models, Process Scheduling: Basic Concepts, Scheduling Criteria, and Scheduling Algorithms.

Unit III: Deadlock: System Model, Deadlock Characterization, Methods for Handling Deadlocks, Deadlock Prevention, Deadlock Avoidance, Deadlock Detection, Recovery from Deadlock.

UNIT IV: Memory Management: Basic Hardware, Address Binding, Logical and Physical Address, Dynamic linking and loading, Swapping, Contiguous Memory Allocation, Segmentation, Paging, Demand Paging, Page Replacement algorithms

SECTION B

UNIT V: File Systems: File Concept, Access Methods, Directory and Disk Structure, File-System Structure, File-System Implementation, Directory Implementation, Allocation Methods, Free-Space Management.

UNIT VI: **Introduction to Linux:** Linux's shell, Kernel, Features of Linux, Using file system: Filenames, Introduction to different types of directories: Parent, Subdirectory, Home directory; rules to name a directory, Important directories in Linux File System,

UNIT VII: Linux Commands: cal, date, echo, bc, who, cd, mkdir, rmdir, ls, cat cp, rm, mv, more, gzip, tar, File ownership, file permissions, chmod, Directory permission, change file ownership,

UNIT VIII: Shell Scripting: Creating and Executing Shell Programs, Using variables: Assigning a value to a variable, Accessing the value of a variable, Positional Parameters and other Built-In Shell Variables; Special Characters, Conditional Statements : if Statement, case Statement; Iteration Statements : for Statement, while Statement, until Statement

Suggested Readings

1. A Silberschatz, P.B. Galvin, G. Gagne, Operating Systems Concepts, 8th Edition, John Wiley Publications, 2009

2. A.S. Tanenbaum, Modern Operating Systems, 3rd Edition, Pearson Education, 2014

3. G. Nutt, Operating Systems: A Modern Perspective, 2nd Edition Pearson Education, 2000

4. S. Das, Unix Concepts and Applications, 4th edition, McGraw Hill Education, 2017

CCCS-1-05P: Operating Systems Lab

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 2
Pass Percentage: 40%

Practical will be Based on CCCS-1-05T: Operating Systems.