SYLLABUS FOR THE BATCH FROM YEAR 2025 TO 2026

FOR

Certificate/Diploma in Cybersecurity

(Credit Based Evaluation and Grading System)

Semester: I-II

EXAMINATIONS: 2025-2026

The Certificate/Diploma Programme Offered:

- **Certificate/Diploma in Cybersecurity (1 Year duration)**

Program Outcomes:

- The online cybersecurity course provides fundamental knowledge in the computers, Computer networks, cloud computing and cybersecurity technology
- This course provides hands-on experience with cutting-edge tools to help the student enter and advance in the field of cybersecurity.
- Students will learn penetration testing, network assessment and protection, intrusion detection, and encryption and decryption methods.
- They will also master the basics of incident management and forensic analysis.

Name of the Department: Computer Science

In collaboration with

Directorate of Open & Distance Learning and Online Studies

GURU NANAK DEV UNIVERSITY AMRITSAR

Certificate/Diploma in CYBERSECURITY (SEMESTER SYSTEM) Offered by Department of Computer Science in collaboration with Directorate of Open & Distance Learning and Online Studies, Guru Nanak Dev University, Amritsar

Eligibility:

- +2 in any stream with at least 45% marks in aggregate (40% for SC/ST candidates).
- Any student doing Bachelor Degree, Master Degree, M.Phil., Ph.D. from GNDU.

SEMESTER-I

Paper Code	Subject	Marks			Credits
		Internal Assessment	End Term	Total	
ODCS101T	Introduction to Computers & Cybersecurity	30	70	100	4
ODCS102T	Computer Networks & Cloud Computing	30	70	100	4
ODCS103T	Cybersecurity Regulations and Compliance Frameworks	30	70	100	4
ODCS104P	Practical Lab – 1	30	70	100	4
Total Marks & Credits		**120**	**280**	**400**	**16**

SEMESTER-II

Paper Code	Subject	Marks			Credits
		Internal Assessment	End Term	Total	
ODCS201T	Networks and Cloud Security Essentials	30	70	100	4
ODCS202T	Incident Management and Digital Forensics	30	70	100	4
ODCS203T	Ethical Hacking	30	70	100	4
ODCS204P	Practical Lab – 2	30	70	100	4
Total Marks & Credits		**120**	**280**	**400**	**16**

Certificate/Diploma in CYBERSECURITY (SEMESTER SYSTEM) Offered by Department of Computer Science in collaboration with Directorate of Open & Distance Learning and Online Studies, Guru Nanak Dev University, Amritsar

Subject Name: Introduction to Computers & Cybersecurity
Course Code: ODCS101T
Semester-I

Section-A

Introduction to computer hardware and software;input/output devices; Operating system (OS): overview of OS role and functions (user interface, file management; process and memory management); OS components (kernel, shell, system calls, user interface); file management: concept of a file; Types of files (text, binary, executable, etc.); File attributes (name, type, size, permissions); File operations (create, read, write, delete, append); File System Architecture (file control block, directories).

Section B

Introduction to the internet and web browsing:IP address, MAC address; Client-Server/P2P Architecture, why security matters?Confidentiality, Integrity, availability of information; desktop and mobile apps; Authentication & authorization; Data trails of an Internet user; cookies;

Section C

What is cybersecurity?Importance of cybersecurity in daily life;Threats**:** Malicious software, Cyber threats, hackers, trackers, types of hackers, hacker motives; Types of Attacks: virus, worms, Trojan horse, spam, spoofing, phishing, spear-phishing, whaling, social engineering, ransomware, spyware, adware, malvertising, supply-chain attacks, zero-day viruses - software/hardware vulnerabilities, exploits; denial of service attacks; bots, botnets; Data breaches; risks of using public Wi-Fi; Cyber bullying;

Section D

Safeguaring Using http/https; Anti-virus software, analysis of the tools available in the market; strong passwords/passphrases, password managers, changing passwords regularly; Cryptography: Encryption, Decryption, public/private cryptography, Digital signatures; Virtual private networks; Setting up private and secure Wi-Fi; Data backup and recovery – full/incremental/differential backup, backup v/s archive; software updates/patches; URL filtering; privacy vs security vs anonymity, privacy settings in apps/browsers and popular social networking sites such as Facebook, Instagram, Snapchat; using web browser incognito mode, the tor browser;

Recommended Books:

- Peter Norton, introduction to Computers, McGraw Hill Education
- Anita Goel, Computer Fundamentals, Pearson India
- Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Operating System Concepts, John Wiley & Sons, Inc.
- Douglas E Comer, The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works, CRC Press
- Introduction to cyber security: stay safe online, The Open University
- Oreku, G.S., Mtenzi, F.J. (2017). Cybercrime: Concerns, Challenges and Opportunities. In: Alsmadi, I., Karabatis, G., Aleroud, A. (eds) Information Fusion for Cyber-Security Analytics. Studies in Computational Intelligence, vol 691. Springer, Cham.

Subject Name: Computer Networks & Cloud Computing
Course Code: ODCS102T
Semester-I

Section-A

Define a Computer Network; Types of Networks: LAN, WAN, MAN, and PAN; Internet, Intranet, and Extranet; Communication Media; Basic networking devices (Routers, Switches, Hubs, Bridges, and Modems); Network Topologies (Bus, Star, Ring, Mesh, Tree); Wireless and Mobile Networks;

Section-B

Packet Switching vs Circuit Switching; OSI Model and TCP/IP Model (Layers and Functions); IP Addressing: Subnetting and Supernetting; IPv4 and IPv6; Protocols: HTTP, FTP, SMTP, POP3, IMAP;TCP/IP Protocol Suite; How data travels over the internet (TCP/IP, DNS, HTTP); Overview of Routing Protocols (RIP, OSPF, BGP)

Section-C

Definition of Cloud Computing; Characteristics of Cloud Computing: On-demand, Resource pooling, Scalability; Service Models: IaaS, PaaS, SaaS; Deployment Models: Public Cloud, Private Cloud, Hybrid Cloud; Key Cloud Providers: AWS, Google Cloud, Microsoft Azure

Section-D

Cloud Service Architecture and Components; Virtualization: Concepts, Types (Server, Network, Storage), Benefits; Hypervisors and Virtual Machines (VMs); Cloud Storage (Object Storage, Block Storage, File Storage); Containers and Orchestration.

Recommended Books:

- James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach
- William Stallings, Data and Computer Communications,
- Thomas Erl, Cloud Computing: Concepts, Technology & Architecture by
- ArshdeepBahga and Vijay Madisetti, Cloud Computing: A Hands-On Approach,
- Chellammal Surianarayanan, Pethuru Raj Chelliah, Essentials of Cloud Computing- A Holistic, Cloud-Native Perspective, Springer

Certificate/Diploma in CYBERSECURITY (SEMESTER SYSTEM) Offered by Department of Computer Science in collaboration with Directorate of Open & Distance Learning and Online Studies, Guru Nanak Dev University, Amritsar

Subject Name: Cybersecurity Regulations and Compliance Frameworks

Course Code: ODCS103T
Semester-I

Section-A

Role of Regulatory Bodies in Cybersecurity, Key Compliance Concepts (Data Protection, Privacy, etc.), Risk Management and Vulnerability Assessment; Data Classification and Security Control;
Cybersecurity Standards and Frameworks - ISO/IEC 27001- Key Components; Certification and Audit Processes; NIST Cybersecurity Framework: Implementation and Risk Management; General Data Protection Regulation (**GDPR**); Legal Implications of GDPR on Organizations; Health Insurance Portability and Accountability Act (**HIPAA**) - Compliance and Penalties for Non-Compliance; Payment Card Industry Data Security Standard (**PCI DSS**)- Compliance Requirements for Payment Systems; Implementing and Auditing PCI DSS Standards

Section-B

Cybersecurity Laws in India (e.g., IT Act 2000,): Indian IT Act 2000 and Amendments; CERT-In and its Role in National Cybersecurity; Compliance Requirements for Indian Organizations
Cybersecurity Regulations in the US (e.g., CCPA, FISMA) - California Consumer Privacy Act (CCPA); Federal Information Security Modernization Act (FISMA); Understanding the implications for organizations operating in the US
European Union (EU) Cybersecurity Regulations: EU Cybersecurity Act and ENISA; Network and Information Systems (NIS) Directive; National Data Protection Laws in the EU
Regional Cybersecurity Regulations in Asia and Africa: Cybersecurity Laws in Southeast Asia (Singapore, Malaysia); Africa’s Approach to Cybersecurity (e.g., South Africa’s Protection of Personal Information Act)

Section-C

Cybersecurity Compliance Practices and Enforcement –Risk Assessment Frameworks and Tools; Continuous Monitoring for Compliance; Penalties and Consequences of Non-Compliance
Auditing and Reporting in Cybersecurity Compliance - Internal and External Audits for Compliance; Cybersecurity Reporting and Documentation; Best Practices for Maintaining Compliance

Section-D

Future of Cybersecurity Regulations and Emerging Trends: AI, IoT, and Cloud Computing: Impact on Compliance; Upcoming Regulations and Future Trends; Preparing for the Next Generation of Cybersecurity Threats
Case studies from real-world cybersecurity compliance challenges
Comparative analysis of national cybersecurity regulations; Analysing application of a cybersecurity framework in an organization, including potential compliance issues and solutions.

Recommended Books:

- Cybersecurity Law And Regulation, Uchenna Jerome Orji, aolf Legal Publishers (WLP)
- ISO/IEC 27001 and NIST Cybersecurity Framework documents
- GDPR, HIPAA, and PCI DSS guidelines (official documentation)
- Greiman, V.A. (2022). Cyber Law and Regulation. In: Lehto, M., Neittaanmäki, P. (eds) Cyber Security. Computational Methods in Applied Sciences, vol 56. Springer, Cham.
- Seng, N. Cybersecurity Regulation—Types, Principles, and Country Deep Dives in Asia. *Int. Cybersecur. Law Rev.* **5**, 387–411 (2024). https://doi.org/10.1365/s43439-024-00127-z

Practical Lab – I

Course Code: ODCS104P
Semester-I

Section-A

Installing a Linux distribution standalone (e.g., Ubuntu)/ in a virtual machine; Practicing basic terminal commands: Common terminal commands (e.g., cd, ls, mkdir, rm); Editing files with basic text editors (e.g., vi);File permissions and ownership (chmod); Setting up an antivirus software

Section-B

Setting up a basic network; installing a personal firewall; Configuring basic security settings on computers and mobile devices; Setting up an online social media profile securely; Exploring privacy settings and using privacy tools; Safe browsing practices and identifying online threats

Section-C

Exploring basic Linux security tools (e.g., netstat, ifconfig); Monitoring and analysing network traffic; Hands on the Wireshark packet sniffer

Section-D

Exploring cloud environments (creating a basic virtual machine in AWS or Azure); Secure Virtual Machines (VMs); Creating and using Containers (Docker, Kubernetes);

Certificate/Diploma in CYBERSECURITY (SEMESTER SYSTEM) Offered by Department of Computer Science in collaboration with Directorate of Open & Distance Learning and Online Studies, Guru Nanak Dev University, Amritsar

Subject Name: Incident Management and Digital Forensics

Course Code: ODCS201T
Semester-II

Section–A

Definition and types of incidents; Phases of incident management (detection, containment, eradication, recovery); Incident response policies and frameworks (NIST, SANS); fundamental incident response functions including detecting, responding, and recovering from security incidents. Understanding the provisions of a Computer Emergency Report Team portal in India (https://www.cert-in.org.in/) and at global level.

Section–B

The concept, need, and value of digital forensics. The digital forensics process: problem identification, collection, examination, analysis, and presentation; evidence preservation

Digital Evidence – sources; Collection, Search and Seizure of Computers: Data Acquisition of physical storage devices;Memory Acquisition; Recovering deleted evidences: time, registry, and Password recovery;Recover Internet Usage Data, Recover Swap Files/Temporary Files/Cache Files, Analyze digital evidence from non-PC devices, such as smartphones, tablets, GPS, game consoles, Smart TVs, and IoT devices. Email and Database Forensics;mobile and embedded forensics, Internet forensics; network forensics

Section–C

Data Recovery Procedures and Ethics, Preserve and safely handle original media, Chain of Custody, Using open-source forensics tools to perform digital investigation e.g. Autopsy and Sleuth Kit; digital forensics with kali linux;

Section–D

Digital Forensic readiness; ethical considerations; key rules, laws, policies, and procedures that impact digital forensics; international cooperation in order to collect digital evidence; challenges in digital forensics; limitations of forensics

References:

- Mike Sheward, Digital Forensic Diaries (Paperback), Independently published (June 17, 2017)
- André Årnes (Editor), Digital Forensics, Wiley, 2018
- Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics, Routeledge, 2nd Edition, 2018
- Britz Computer Forensics and Cyber Crime: An Introduction, 2e Paperback – 2011
- Shiva V.N. Parasram, Digital Forensics with Kali Linux: Perform data acquisition, digital investigation, and threat analysis using Kali Linux tools, 2017, Packt publishing

Certificate/Diploma in CYBERSECURITY (SEMESTER SYSTEM) Offered by Department of Computer Science in collaboration with Directorate of Open & Distance Learning and Online Studies, Guru Nanak Dev University, Amritsar

Subject Name: Networks and Cloud Security Essentials

Course Code: ODCS202T

Semester-II

Section-A

Security principles: Confidentiality, Integrity, Availability (CIA triad); Common network security threats: Malware, Phishing, DDoS, Man-in-the-Middle; Basic security measures: Firewalls, IDS/IPS, Antivirus, VPNs; Firewalls: Why? Types (Packet Filtering, application gateways); Intrusion Detection & Prevention Systems (IDS/IPS); Network Access Control (NAC) and Zero Trust Security Model; VPNs: Types, Benefits, and Implementation

Section-B

Symmetric vs. Asymmetric Cryptography (AES, DES, RSA, ECC), Hash Functions (SHA, MD5) and Digital Signatures; Secure Socket Layer (SSL) and Transport Layer Security (TLS); Public Key Infrastructure (PKI) and Certificate Authorities (CAs); Secure Network Protocols: HTTPS, SSH, IPSec, RADIUS, Kerberos; Authentication & Authorization: Multi-Factor Authentication (MFA), Single Sign-On (SSO); Role-Based Access Control (RBAC) vs. Discretionary Access Control (DAC

Section-C

Cloud Security Challenges: Common cloud security threats (data breaches, misconfigurations, insider threats); Cloud service provider responsibilities vs. customer responsibilities; Shared responsibility model in the cloud; Cloud Security Best Practices: Data encryption, secure APIs, patch management; Compliance and Regulations: GDPR, HIPAA, ISO 27001

Section-D

Identity and Access Management (IAM) concepts; Cloud IAM solutions (AWS IAM, Azure Active Directory, Google IAM); Secure API authentication (OAuth, OpenID Connect); Cloud Key Management Systems (KMS) for encryption; Cloud Security Tools and Resources: Overview of cloud security tools (e.g., AWS Shield, Azure Security Center);

References:

- James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach, Pearson Education Limited; 8th edition (17 June 2021)
- William Stallings, Data and Computer Communications, Pearson Education; Tenth edition (20 September 2017);
- ArshdeepBahga and Vijay Madisetti, Cloud Computing: A Hands-On Approach, The Orient Blackswan (1 January 2014)

Certificate/Diploma in CYBERSECURITY (SEMESTER SYSTEM) Offered by Department of Computer Science in collaboration with Directorate of Open & Distance Learning and Online Studies, Guru Nanak Dev University, Amritsar

Subject Name: Ethical Hacking

Course Code: ODCS203T
Semester-II

Section–A

Basics of ethical hacking, Understanding the ethical hacker's role; The hacking lifecycle (reconnaissance, exploitation, post-exploitation); Introduction to legal and ethical considerations, hacker types (White, Black, Gray Hat), penetration testing methodology, reconnaissance techniques (OSINT, Google dorking), password cracking methods (brute force, dictionary attacks), social engineering techniques (Phishing, Vishing (voice phishing), Smishing (SMS phishing), Baiting, Impersonation), and real-world cyber threats.

Section–B

Kali Linux and Penetration Testing Tools: Installation and setup of Kali Linux, process management, and scripting (Bash), Network Penetration Testing, Detection, and Security–pre-connection, post connection, network scanning, vulnerability assessment, wireless security testing, and exploitation techniques using Metasploit.

Section–C

Web application testing (Burp Suite, SQLmap), Sever-side attacks, Metasploit remote code execution, Scanning Vulnerabilities Using Tools; Client-Side Attacks - Social Engineering, Twitter, emails; Attack and Detect Trojans with BeEF

Section–D

Real-World Applications, Case Studies, and Career Pathways; Case studies on real-world cyberattacks, introduction to bug bounty programs, red teaming vs. blue teaming, role of cybersecurity analysts, legal and ethical aspects of hacking, and career opportunities

References:

1. Kali Linux Revealed – Raphael Hertzog, Jim O'Gorman, MatiAharoni
2. The Basics of Hacking and Penetration Testing – Patrick Engebretson
3. Metasploit: The Penetration Tester's Guide – David Kennedy
4. CEH Certified Ethical Hacker Study Guide – Kimberly Graves

Certificate/Diploma in CYBERSECURITY (SEMESTER SYSTEM) Offered by Department of Computer Science in collaboration with Directorate of Open & Distance Learning and Online Studies, Guru Nanak Dev University, Amritsar

Subject Name: Practical Lab – 2

Course Code: ODCS204P
Semester-II

Section-A

Setting up and using basic network monitoring tools; Simulating a basic incident response scenario; Using an open-source SIEM tool (e.g., ELK Stack or Splunk)

Section-B

Configuring a secure cloud environment; Implementing basic encryption in the cloud; Using cloud security tools to monitor resources; Cloud-native security solutions (AWS Shield, Azure Security Center, Google Cloud Armor)

Section-C

Using Kali Linux **-** Installing and configuring Kali Linux; Basic Kali Linux commands for security testing; Practicing vulnerability scanning and network analysis

Section-D

Kali's tools Nmap, Metasploit, and Burp Suite; Performing basic penetration testing on a virtual machine; Reporting findings in a simulated penetration test; Network reconnaissance and analysis