Curriculum Structure										
Session 2025-2026 onwards										
Name of the Program: P.G. Diploma in Cyber Security and Cyber Law										
Year: First							Semester: I (Pawas)			
	Course Code	Course Title	Contact Hrs per Week			Credits	Weightage (%)			
			L	T	P		CW$	MTE	ETE	
Pawas Semester I	**Discipline Specific Core (DSC):**									
	25MCL9101T	Fundamental of Computing and Networking	4	0	0	4	10	20	70	
	25MCL9102T	Applied Cryptography	4	0	0	4	10	20	70	
	25MCL9103T	Information Security and Privacy	4	0	0	4	10	20	70	
	25MCL9101P	Python Laboratory	0	0	4	2	-	-	100	
	25MCL9101V	Project	0	0	4	2	+			
	Discipline Specific Elective (DSE): (Select any one)									
	25MCL9104T	Banking Technology and Financial Frauds	4	0	0	4	10	20	70	
	25MCL9105T	Cyber Threat intelligence	4	0	0	4	10	20	70	
	25MCL9106T	Cyber Crime scene management and Investigation	4	0	0	4	10	20	70	
	Value Added Course (VAC):									
	---	---	--	--	--	2	--	--	--	
	Seminar/Internship/Apprenticeship/Project/Community Outreach (S/I/A/P/C):									
	---	---	--	--	--	--	--	--	--	
		Total				22				

Summary: I Semester (Pawas)		Credits
S.N.	**Particulars**	
1.	Discipline Specific Core (DSC):	16
2.	Discipline Specific Elective (DSE):	04
3.	Value Added Course (VAC):	02
4.	Seminar/Internship/Apprenticeship/Project/Community Outreach (S/I/A/P/C):	00
	Total	22
$CW (Class work): It would include attendance, class test/quiz test/assignments, ppt, play, learn by fun activities etc.		

Note: VAC to be selected from the list of VAC courses for PG, given on University website.

Dy. Registrar
Pandit Deendayal Upadhyaya
Shekhawati University,
Sikar(Rajasthan)

Curriculum Structure										
Session 2025-2026 onwards										
Name of the Program: P.G. Diploma in Cyber Security and Cyber Law										
Year: First							Semester: II (Vasant)			
	Course Code	Course Title	Contact Hrs per Week			Credits	Weightage (%)			
			L	T	P		CW$	MTE	ETE	
Vasant Semester II	**Discipline Specific Core (DSC):**									
	25MCL9201T	Web Application and Penetration Testing	4	0	0	4	10	20	70	
	25MCL9202T	Cyber Security and Auditing Framework	4	0	0	4	10	20	70	
	25MCL9203T	Cyber Law, Policy, and Guidelines	4	0	0	4	10	20	70	
	25MCL9201P	ISO 27000 Auditing Laboratory	0	0	4	2	-	-	100	
	25MCL9201V	Project	0	0	4	2	-	-	100	
	Discipline Specific Elective (DSE):									
	25MCL9204T	Digital Forensic	4	0	0	4	10	20	70	
	25MCL9205T	Cloud Computing and Security	4	0	0	4	10	20	70	
	25MCL9206T	Network Security Using AI	4	0	0	4	10	20	70	
	Value Added Course (VAC):									
	---	---	--	--	--	2	--	--	--	
	Seminar/Internship/Apprenticeship/Project/Community Outreach (S/I/A/P/C):									
	---	---	--	--	--	--	--	--	--	
		Total				**22**				

Summary: II Semester (Vasant)		Credits
S.N.	**Particulars**	
1.	Discipline Specific Core (DSC):	**16**
2.	Discipline Specific Elective (DSE):	**04**
3.	Value Added Course (VAC):	**02**
4.	Seminar/Internship/Apprenticeship/Project/Community Outreach (S/I/A/P/C):	**00**
	Total	**22**
$CW (Class work): It would include attendance, class test/quiz test/assignments, ppt, play, learn by fun activities etc.		

Note: VAC to be selected from the list of VAC courses for PG, given on University website.

Dy. Registrar
Pandit Deendayal Upadhyaya
Shekhawati University,
Sikar(Rajasthan)

Course Title:	Fundamental of Computing and Networking	Course Code: 25MCL9101T
Total Lecture hour 60		**Hours**
Unit I	**Foundations of Computing and Digital Logic** History and Classification of Computers; Computer Hardware Components CPU, memory hierarchy (RAM, ROM, Cache); I/O devices and storage (HDD, SSD, optical drives); Number Systems and Conversions - Binary, decimal, hexadecimal; Logic Gates and Boolean Algebra - AND, OR, NOT, NAND, NOR, XOR, Truth tables and basic logic circuits	15
Unit II	**Operating Systems and System-Level Computing** Introduction to Operating Systems (OS) - Functions of OS: process, memory, and file management, Types of OS: batch, multitasking, real-time, mobile OS; File Systems and Data Structures- FAT, NTFS, ext4 basics, File permissions and access control; User and Process Management- Users, groups, privileges, Process scheduling, inter-process communication; Virtualization Basics - Concept of virtual machines and hypervisors, Isolation and sandboxing, Practical usage of Virtual environments for malware analysis and secure testing	15
Unit III	**Computer Networks – Architecture and Communication** Networking Basics- Network types: LAN, WAN, MAN, PAN; Topologies: star, bus, ring, mesh; OSI and TCP/IP Models - Layered communication approach; Common protocols: IP, TCP, UDP, HTTP, HTTPS, FTP, SMTP; Network Hardware - Switches, routers, hubs, access points; Wired vs wireless communication; IP Addressing and Subnetting - IPv4 and IPv6 basics; Static vs dynamic addressing (DHCP), **Network Security Fundamentals** - Firewalls: types (packet filtering, stateful, proxy), Intrusion Detection and Prevention Systems (IDS/IPS): signature and anomaly-based detection; Virtual Private Networks (VPNs), Logging, Monitoring, and Incident Response	15
Unit IV	**Advanced Networking and Computing Applications in Security Contexts** Network Services and Configuration - DNS, NAT, DHCP, VPN; Introduction to Wireless Networks - Wi-Fi standards (802.11 a/b/g/n/ac/ax); Security protocols (WPA2/WPA3); Cloud Computing Fundamentals - Service models: IaaS, PaaS, SaaS; Cloud deployment: public, private, hybrid; Basics of Shell Scripting and Command Line Interfaces - File and user management via CLI; Network tools: ping, traceroute, ipconfig/ifconfig, netstat; Logging and Monitoring Fundamentals - System and network logs; Introduction to syslog and log analysis; Understanding logs for threat detection	15

Suggestive Readings:

1	Computer Fundamentals – P.K. Sinha & Priti Sinha Publisher: BPB Publications, 6th Edition, 2020
2	Introduction to Computing and Programming in Python – Mark Guzdial & Barbara Ericson Publisher: Pearson Education, 4th Edition, 2016
3	Fundamentals of Computers – V. Rajaraman Publisher: PHI Learning Pvt. Ltd., 6th Edition, 2014
4	Data Communications and Networking – Behrouz A. Forouzan Publisher: McGraw Hill Education, 5th Edition, 2012
5	Computer Networking: A Top-Down Approach – James F. Kurose & Keith W. Ross Publisher: Pearson Education, 7th Edition, 2016

Course Title:	Applied Cryptography	Course Code: 25MCL9102T
Total Lecture hour 60		**Hours**
Unit I	**Introduction to Cryptography and Cybersecurity Context** Evolution and History of Cryptography; Classical ciphers: Caesar cipher, monoalphabetic, transposition; Importance of cryptography in the digital age; Key Cryptographic Goals - Confidentiality, Integrity, Authentication, Non-repudiation; Introduction to Cybersecurity Concepts - Threats, vulnerabilities, and the CIA triad; Role of cryptography in securing systems and networks; Types of Cryptographic Systems - Symmetric vs Asymmetric encryption; Hashing and Message Authentication Codes (MACs)	15

Dy. Registrar
Pandit Deendayal Upadhyaya
Shekhawati University,
Sikar(Rajasthan)

Unit II	**Symmetric Key Cryptography and Applications** Concepts of Symmetric Encryption; Key generation, key distribution challenges; Block vs stream ciphers; Classical and Modern Symmetric Ciphers - DES, 3DES, AES; Modes of operation: ECB, CBC, CFB, OFB, CTR; Stream Ciphers (RC4 – deprecated); Cryptanalysis Basics - Brute-force, known-plaintext, chosen-plaintext attacks; Applications in Cybersecurity - Disk encryption (e.g., BitLocker, VeraCrypt), Secure file storage and secure messaging	**15**
Unit III	**Asymmetric Cryptography, Hashing, and Digital Signatures** Public Key Cryptography - RSA, Diffie-Hellman Key Exchange; Elliptic Curve Cryptography (intro only), Digital Certificates and PKI; Certificate Authorities, X.509, SSL/TLS; Hash Functions - MD5, SHA-1, SHA-256, Properties: pre-image resistance, collision resistance; Digital Signatures - Signing and verifying data, Role in software and email authentication; Applications in Cybersecurity - HTTPS and secure websites, Password hashing and verification, Software/code signing	**15**
Unit IV	**Applied Cryptography in Systems, Networks, and Emerging Technologies** Secure Communication Protocols - SSL/TLS, SSH, VPN encryption; Email encryption (PGP, S/MIME); Cryptography in Network Security - IPSec, Wi-Fi encryption standards (WEP, WPA2, WPA3); Cryptographic Key Management - Key lifecycle, key storage, HSMs, key exchange protocols; Blockchain and Cryptography (Intro) - Cryptographic hash in blockchain; Digital signatures and consensus algorithms; Cryptographic Tools and Libraries -OpenSSL, GnuPG, HashCalc, VeraCrypt (hands-on)	**15**

Suggestive Readings:

1	Applied Cryptography: Protocols, Algorithms, and Source Code in C – Bruce Schneier, Wiley, 2nd Edition, 1996
2	Cryptography and Network Security: Principles and Practice – William Stallings, Pearson Education, 8th Edition, 2023
3	Introduction to Modern Cryptography – Jonathan Katz, Yehuda Lindell, CRC Press, 3rd Edition, 2020
4	Serious Cryptography: A Practical Introduction to Modern Encryption – Jean-Philippe Aumasson, No Starch Press, 1st Edition, 2017

Course Title:	**Information Security and Privacy**	**Course Code: 25MCL9103T**
Total Lecture hour 60		**Hours**
Unit I	**Foundations of Information Security** Introduction to Information Security - why security matters in the digital world; Definitions: Threats, vulnerabilities, attacks; The CIA Triad - Confidentiality, Integrity, Availability; Security Objectives and Risk Management; Threat modelling - Security policies and controls (administrative, technical, physical); Types of Attacks - Malware, phishing, denial of service; Privacy Threats and Risks - Insider threats and data leaks, Tracking, profiling, and surveillance risks.	**15**
Unit II	**Privacy Principles and Data Protection** Introduction to Privacy - Privacy in the digital era: challenges and importance; Privacy vs. security: key distinctions and overlap; Personally Identifiable Information (PII) -Types of PII and sensitive personal data, Classification of data sensitivity: public, internal, confidential, restricted, Data Protection Techniques - Data masking: techniques and scenarios (e.g., payment card data masking), Data anonymization, Pseudonymization, Privacy Frameworks and Standards - Fair Information Practices (FIPs): notice, choice, access, integrity, security, enforcement; OECD Privacy Principles and their global influence; Overview of privacy regulations (GDPR, CCPA) and their impact on data handling	**15**
Unit III	**System and Network Security Fundamentals** Security Architectures and Defence in Depth; Secure system design principles: least privilege, fail-safe defaults; Hardening operating systems and applications: patch management, configuration best practices; Authentication Mechanisms - Password-based	**15**

	authentication Multi-factor Authentication (MFA): types (something you know, have, are), Biometric authentication: advantages and limitations; Access Control Models -Role-Based Access Control (RBAC), Mandatory Access Control (MAC), Discretionary Access Control (DAC), Attribute-Based Access Control (ABAC)	
Unit IV	**Password Policies, Compliance, and Security Frameworks** Password Policies and Best Practices; Password complexity, expiration, reuse restrictions; Password storage (hashing, salting); multi-factor authentication (MFA); Definitions and Concepts - Guidelines, Compliance, Requirements; Governance, Risk Management, and Compliance (GRC);Introduction to ISO/IEC 27001; Role of Policies and Standards in Security Compliance.	**15**

Suggestive Readings:

1	Information Security: Principles and Practice – Mark Stamp, Wiley, 3rd Edition, 2021
2	Principles of Information Security – Michael E. Whitman, Herbert J. Mattord, Cengage Learning, 6th Edition, 2017
3	Information Privacy Engineering and Privacy by Design – William Stallings, Pearson, 1st Edition, 2021
4	Introduction to Information Security – Umesh Hodeghatta, Umesha Nayak, Wiley India, 1st Edition, 2014
5	Network Security Essentials: Applications and Standards – William Stallings, Pearson, 6th Edition, 2023

Course Title:	**Python Lab**	**Course Code: 25MCL9101P**

Lab 1: Python Basics and Variables

==========

Objective: Learn Python syntax, data types, and variable handling.
Tasks:
1. Write a Python program to input user name, age, and email, then display it.
2. Practice using strings, integers, floats, and type conversion.
3. Use comments to document your code.
Python Concepts Used: input/output, variables, data types, type casting

Lab 2: Conditional Statements and Loops

==========

Objective: Practice using conditionals and loops to control program flow.
Tasks:
1. Write a program to check if a number is even or odd.
2. Create a number guessing game using a while loop.
3. Use a for loop to print a multiplication table for a given number.
Python Concepts Used: if-else, for loop, while loop

Lab 3: Functions and Modular Code

==========

Objective: Use functions to organize code and promote reusability.
Tasks:
1. Write functions for basic operations: add, subtract, multiply, divide.
2. Create a calculator program using these functions.
3. Demonstrate use of default and keyword arguments.
Python Concepts Used: functions, return values, arguments

Lab 4: Lists, Tuples, and Dictionaries

==========

Objective: Practice with Python collections to manage grouped data.
Tasks:
1. Store and display a list of student names.

2. Create a phonebook using a dictionary and allow lookup by name.
3. Demonstrate tuples for storing read-only coordinates.
Python Concepts Used: list, tuple, dictionary, iteration

Lab 5: File Handling and Basic CSV Operations
==========
Objective: Learn how to read and write files in Python.
Tasks:
1. Create a program to save user data to a text file.
2. Read and print content from a file.
3. Append new data to an existing CSV file.
Python Concepts Used: open(), read(), write(), CSV module

Lab 6: Data Anonymization and Masking (Unit 2)
==========
Objective: Implement basic data anonymization and masking techniques.
Tasks:
1. Load a CSV file containing PII.
2. Mask sensitive fields (e.g., partial phone/email).
3. Anonymize fields using hashing and save the result.
Python Concepts Used: pandas, hashlib, file I/O

Lab 7: Password Strength Checker and Hashing (Unit 3 & 4)
==========
Objective: Develop a tool for checking password strength and storing it securely.
Tasks:
1. Prompt for a password and evaluate its strength.
2. Hash the password using SHA-256 or bcrypt with salt.
3. Save the hashed password securely.
Python Concepts Used: re, hashlib, bcrypt (optional), file handling

Lab 8: Network Traffic Capture and Analysis (Unit 3)
==========
Objective: Capture and analyze basic network packets.
Tasks:
1. Capture packets using pyshark or scapy.
2. Filter for HTTP or DNS traffic.
3. Analyze and summarize packet source/destination.
Python Concepts Used: pyshark/scapy, filtering, parsing

Lab 9: Role-Based Access Control (RBAC) Simulation
==========
Objective: Implement a simple RBAC model in Python.
Tasks:
1. Define roles and permissions using dictionaries.
2. Create a function decorator to check access rights.
3. Test user access scenarios with different roles.
Python Concepts Used: classes, decorators, dictionaries

Lab 10: Log Analysis for Incident Detection
==========
Objective: Identify suspicious behavior through log file analysis.
Tasks:
1. Parse sample server logs.
2. Identify repeated failed login attempts.

	3. Generate a report of suspicious IPs. Python Concepts Used: regex, file I/O, collections **Project** Project can be taken by the students in various formats as per the discussion with the course coordinator. Some of the proposed and accepted formats are mentioned below: 1. Research experiments on cutting edge technology with some results. 2. Survey paper publication in repute journal. 3. Colloquium on a topic with in depth knowledge.

Course Title:	**Project**	**Course Code: 25MCL9101V**
	Project can be taken by the students in various formats as per the discussion with the course coordinator. Some of the proposed and accepted formats are mentioned below: 1. Research experiments on cutting edge technology with some results. 2. Survey paper publication in repute journal. 3. Colloquium on a topic with in depth knowledge.	

Course Title:	**Banking Technology and Financial Frauds**	**Course Code: 25MCL9104T**
Total Lecture hour 60		**Hours**
Unit I	**Introduction to Banking Technology** Evolution of Banking: Traditional to Digital; Types of Banks and Financial Institutions; Core Banking Systems (CBS) -Architecture and functionalities, Real-time processing, and system integration; ATM Networks, RTGS, NEFT, IMPS; Mobile and Internet Banking Platforms; Electronic Fund Transfer (EFT) Systems; Emerging Trends: Open Banking, Neo Banks, API Banking	**15**
Unit II	**Digital Payment Systems and FinTech** Introduction to Digital Payments Ecosystem; Payment Gateways and Payment Aggregators; UPI, BHIM, Wallets, POS Devices; Card Payment Networks (Visa, MasterCard, RuPay); PCIDSS Standard and data localization concept in correspond to DPDP Act; FinTech Innovations in Banking; Cryptocurrencies and Blockchain in Finance; Digital Lending Platforms and Crowdfunding	**15**
Unit III	**Financial Frauds and Cyber Threats in Banking** Classification of Financial Frauds: Credit card frauds, Phishing, vishing, smishing, KYC frauds, Loan frauds, identity theft, synthetic identities, malware-based OTP less frauds; Insider Threats and Social Engineering; ATM Skimming and Point-of-Sale Fraud; SIM Swapping and Mobile App Exploits; Fraud in Online Banking and E-commerce; Deepfake and AI-driven frauds	**15**
Unit IV	**Risk Management, Prevention, and Regulatory Framework** Fraud Detection Mechanisms: Rule-based vs AI/ML-based monitoring, Anomaly detection systems; Risk Assessment and Fraud Prevention Strategies; Regulatory Compliance: RBI Guidelines, KYC/AML Norms, FATF Recommendations; Cybersecurity Frameworks for Banking (ISO 27001, NIST CSF); Data Privacy and Customer Protection; Role of CERT-In and Indian Cybercrime Coordination Centre (I4C); current guidelines by RBI in Risk Management and case studies related to the NBFC and Banking industry.	**15**
Suggestive Readings:		
1	Banking Technology – Dr. R. Padmanabhan, Himalaya Publishing House, Revised Edition, 2020	

2	Banking Technology: Financial Services and Modern Banking Trends – R.K. Uppal & Rimpi Jatana, New Century Publications, 1st Edition, 2006
3	Digital Banking – Debadutta K Panda, Wiley, 1st Edition, 2021
4	Cyber Frauds in Banking Sector – Dr. Shakti Jagirdar, Notion Press, 1st Edition, 2022
5	Cybercrime and Fraud Management – Balsing Rajput, SAGE Publications India, 1st Edition, 2023

Course Title:	Cyber Threat Intelligence	Course Code: 25MCL9105T
Total Lecture hour 60		**Hours**
Unit I	**Fundamentals of Cyber Threat Intelligence** Introduction to Cyber Threat Intelligence (CTI); Intelligence vs Information; Types of Intelligence: Tactical, Operational, Strategic, Technical; Threat Intelligence Lifecycle (Direction, Collection, Processing, Analysis, Dissemination, Feedback); Sources of Threat Intelligence: OSINT, HUMINT, SIGINT, Technical Feeds; Intelligence Sharing Platforms: ISACs, ISAO, STIX/TAXII, MISP; Intelligence Requirements and Priority Intelligence Requirements (PIRs)	15
Unit II	**Threat Actor Profiling and Campaign Analysis** Adversary Motivation and Objectives; Threat Actor Typologies (Nation-State, Cybercrime, Hacktivists, Insider Threats); Threat Modeling: STRIDE, DREAD, ATT&CK, Kill Chain; MITRE ATT&CK Framework: Tactics, Techniques, Procedures (TTPs); Diamond Model of Intrusion Analysis; Use of Threat Feeds (AlienVault OTX, VirusTotal, Anomali, Recorded Future); Campaign Tracking and Infrastructure Pivoting	15
Unit III	**Intelligence Collection, Analysis, and Tools** Open-Source Intelligence (OSINT) Tools and Techniques; Social Media Intelligence (SOCMINT); Dark Web Monitoring and Intelligence Gathering; Indicators of Compromise (IOCs): IPs, Hashes, Domains, Artifacts; Analysis Tools: Maltego, SpiderFoot, TheHarvester, Shodan, Censys; Threat Intelligence Platforms (TIPs): MISP, Anomali, IBM X-Force; Enrichment and Correlation of Intelligence	15
Unit IV	**Operationalization, Ethics, and Intelligence in Practice** Operationalizing CTI in SOC, IR, and Threat Hunting; Threat Intelligence in SIEM, SOAR, and EDR Environments; Fusion with Vulnerability and Risk Management Programs; Legal and Ethical Issues in Threat Intelligence Collection; Compliance and Privacy Considerations (GDPR, NIST 800-53, ISO 27001 and DPDP Act); Case Studies of Successful Intelligence-Driven Defence; Building blocks for CTI Reports and Briefs for Executives and Analysts	15

Suggestive Readings:

1	Cyber Threat Intelligence – Henry Dalziel, Syngress (Elsevier), 1st Edition, 2014
2	Intelligence-Driven Incident Response: Outwitting the Adversary – Scott J. Roberts, Rebekah Brown, O'Reilly Media, 1st Edition, 2017
3	The Threat Intelligence Handbook: A Practical Guide for Security Teams – Recorded Future, Independently Published, 2nd Edition, 2019
4	Practical Threat Intelligence and Data-Driven Threat Hunting – Valentina Costa-Gazcon, Packt Publishing, 1st Edition, 2021
5	The Practice of Network Security Monitoring: Understanding Incident Detection and Response – Richard Bejtlich, No Starch Press, 1st Edition, 2013

Course Title:	Cyber Crime scene management and Investigation	Course Code: 25MCL9106T
Total Lecture hour 60		Hours
Unit I	**Introduction to Cybercrime and Indian Legal Framework** Definition and Classification of Cybercrime; Cyberstalking, hacking, identity theft, financial fraud, ransomware, cyberbullying; Key Sections of Indian Laws: IT Act 2000 (and amendments), BNS, BNSS, BSA 2023; Data Privacy under Indian context with specific reference to DPDP Act; Role of Cybercrime Police Cells, CERT-In, I4C and other collaborative bodies; Jurisdiction and Admissibility in Indian Courts; Cybercrime Trends in India and Case Studies	15
Unit II	**Cybercrime Scene Management (Digital and Physical)** Definition and Principles of Crime Scene Management; Types of Digital Crime Scenes (laptop, mobile, server, cloud, IoT); Scene Preservation and Initial Response Protocols; Identifying and Isolating Volatile vs Non-Volatile Evidence; Scene Safety, Securing Network Devices; Precautions to Prevent Evidence Tampering; Discussion of various SOPs developed by BPR&D and other law enforcement agencies across the world.	15
Unit III	**Evidence Collection, Documentation, and Chain of Custody** Types of Digital Evidence: Emails, Logs, Media, Browsing History, Metadata; Disk Imaging and Bitstream Copy Techniques; Use of Write Blockers and Forensic Tools (FTK Imager, Autopsy, EnCase, etc.); Chain of Custody Protocol in India; Evidence Logging, Labelling, and Preservation Formats; Importance of Forensic Notes and Court-Admissible Documentation; RAM data acquisition and USB history.	15
Unit IV	**Cybercrime Investigation, Reporting & Legal Procedures Cybercrime FIR Filing Process under BNSS 2023** Role of Law Enforcement, NCIIPC, and State CERTs; Cyber Forensics Lab Setup (Indian Context); Mobile Forensics, Email Tracing, IP Tracking, Packet Analysis; Report Writing and Expert Testimony; Cross-border Investigation Issues and MLAT Requests; Emerging Challenges: Deepfakes, Encryption, Dark Web; Forthcoming usage of AR, VR technologies in forensic investigation and crime scene management learning.	15

Suggestive Readings:

1	Digital Evidence and Computer Crime – Eoghan Casey, Academic Press, 3rd Edition, 2011
2	Cyber Crime Investigation – Anthony Reyes, Richard Brittson, Kevin O'Shea, and James Steele, Syngress (Elsevier), 1st Edition, 2007
3	Scene of the Cybercrime – Debra Littlejohn Shinder and Michael Cross, Syngress (Elsevier), 2nd Edition, 2008
4	Handbook of Digital Forensics and Investigation – Eoghan Casey, Academic Press, 1st Edition, 2009
5	Cyber Crime and Digital Evidence: Materials and Cases – Thomas K. Clancy, Carolina Academic Press, 1st Edition, 2011
6	Guide to Computer Forensics and Investigations – Bill Nelson, Amelia Phillips, Christopher Steuart, Cengage Learning, 6th Edition, 2019
7	The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics – John Sammons, Syngress, 3rd Edition, 2015

Semester - II

Course Title:	Web Application and Penetration Testing	Course Code: 25MCL9201T
Total Lecture hour 60		**Hours**
Unit I	**Introduction to Web Applications and Ethical Hacking** Web Application Architecture (Client-Server, Frontend-Backend, APIs); HTTP 1.0 and HTTP 1.1 RFCs; HTTP Protocol Basics (Requests, Methods, Status Codes, Cookies, Sessions); Introduction to Penetration Testing; Phases of Penetration Testing: Reconnaissance, Scanning, Exploitation, Reporting; Rules of Engagement, Scope, Permissions, and NDAs; Legal & Ethical Considerations (Bug Bounty, Safe Harbor, Indian IT Act 2000)	**15**
Unit II	**Reconnaissance, Mapping, and Vulnerability Scanning** Active vs Passive Reconnaissance; Enumeration of Subdomains, Directories, and Resources (Google Dorking, Burp Suite, Dirb, Gobuster); Banner Grabbing and Fingerprinting (WhatWeb, Wappalyzer); Vulnerability Scanning Tools: OWASP ZAP, Nikto, Nuclei; Introduction to CVEs, CVSS, and Vulnerability Databases (GHDB); Automation of Recon using OSINT tools (Shodan, SpiderFoot); Nessus	**15**
Unit III	**Exploiting Web Vulnerabilities** OWASP Top 10 (A01–A10): In-depth Understanding and Exploitation Techniques; SQL Injection, XSS (Reflected, Stored, DOM-Based); input validation, Canonicalization attack, Buffer overflow; Broken Authentication, Insecure Deserialization; SSRF, CSRF, Command Injection, Path Traversal, File Upload; Broken Access Control, Security Misconfiguration, IDOR; Manual Testing Techniques vs Automation; Exploitation Labs (DVWA, Juice Shop, WebGoat, PortSwigger Labs)	**15**
Unit IV	**Reporting, Remediation, and Advanced Concepts** Report Writing: Executive Summary, Risk Ratings, PoCs, Remediation; Use of CVSS v3.1 for Severity Scoring; Secure Coding Practices (Input Validation, Output Encoding, Authentication Hardening); Penetration Testing in CI/CD Environments (DevSecOps); Advanced Topics: WebSocket Security, JWT Attacks, GraphQL and API Security, RCE via Insecure File Upload; Introduction to Red Teaming and Bug Bounty Methodologie	**15**
Suggestive Readings:		
1	The Web Application Hacker's Handbook – Dafydd Stuttard, Marcus Pinto, Wiley, 2nd Edition, 2011	
2	Hacking: The Art of Exploitation – Jon Erickson, No Starch Press, 2nd Edition, 2008	
3	OWASP Testing Guide – OWASP Foundation, v4.2, 2023 (Free Open Source Resource)	
4	Advanced Penetration Testing: Hacking the World's Most Secure Networks – Wil Allsopp, Wiley, 2nd Edition, 2017	
5	Kali Linux Web Penetration Testing Cookbook – Gilberto Najera-Gutierrez, Packt Publishing, 2nd Edition, 2018	
6	Hands-On Penetration Testing on Windows – Phil Bramwell, Packt Publishing, 1st Edition, 2020	

Course Title:	Cyber Security and Auditing Framework	Course Code: 25MCL9202T
Total Lecture hour 60		**Hours**
Unit I	**Fundamentals of Cybersecurity & Information Assurance** Overview of Cybersecurity Principles: CIA Triad, Threats & Vulnerabilities; Categories of Security Controls: Preventive, Detective, Corrective; Introduction to Information Assurance & IT Governance; Risk Management Concepts: Threat Modeling, Risk Matrix, Likelihood & Impact; Business Continuity & Disaster Recovery Planning; Security Policies and Procedures	**15**
Unit II	**Auditing Principles and Processes**	**15**

	Introduction to IT and IS Auditing; Types of Audits: Compliance, Financial, Operational, Technical; First party, second party and Third party; Audit Planning and Scoping; Evidence Collection and Sampling Techniques; Controls Testing and Evaluation (Logical, Physical, Administrative); Audit Documentation and Report Writing; Audit Findings, Recommendations, and Follow-Up	
Unit III	**Cybersecurity Frameworks, Standards, and Best Practices** ISO/IEC 27001: ISMS Structure, PDCA; Controls (Annex A), Certification Process; NIST Framework: Core Functions (Identify, Protect, Detect, Respond, Recover); COBIT 5/2019: Governance and Management Objectives; PCI-DSS, HIPAA, and SOC 2 (Overview); OWASP Top 10 and Secure Software Development Lifecycle (SSDLC); Indian Regulatory Environment: IT Act 2000, CERT-In Guidelines, RBI Cybersecurity Framework	**15**
Unit IV	**Risk Assessment, Controls Implementation & Cyber Audit Execution** Risk Assessment Methodologies (ISO 27005, OCTAVE, FAIR); Asset Valuation and Impact Analysis; Control Selection and Risk Treatment Plan; Security Baselines and Benchmarking (CIS Benchmarks); Vulnerability Assessment and Penetration Testing in Audit Context; Internal Audit Lifecycle with Cybersecurity Focus; Case Studies: Cybersecurity Audits in BFSI, Healthcare, and Critical Infrastructure	**15**

Suggestive Readings:

1	Principles of Information Security – Michael E. Whitman, Herbert J. Mattord, Cengage Learning, 6th Edition, 2017
2	Information Security Management Principles – Andy Taylor, David Alexander et al., BCS Learning & Development Limited, 2nd Edition, 2013
3	Guide to Computer Security Log Management – Karen Kent, U.S. NIST Special Publication 800-92, 1st Edition, 2006 (Free Government Publication)
4	IT Auditing and Application Controls for Small and Mid-Sized Enterprises – Jason Wood, Wiley, 1st Edition, 2013
5	Cybersecurity Framework (NIST) – National Institute of Standards and Technology, 2020 Edition (Free Government Framework Document)
6	Auditing IT Infrastructures for Compliance – Martin Weiss, Michael G. Solomon, Jones & Bartlett Learning, 2nd Edition, 2015
7	ISO/IEC 27001:2013 – International Organization for Standardization, Latest Revision

Course Title:	**Cyber Law, Policy, and Guidelines**	**Course Code: 25MCL9203T**
Total Lecture hour 60		**Hours**
Unit I	**Foundations of Cyber Law and Legal Frameworks** Definition, Scope, and Evolution of Cyber Law; Jurisdiction and Legal Challenges in Cyberspace; Information Technology Act, 2000 (with 2008 & 2023 updates); Digital Signatures and Electronic Records; Admissibility of Electronic Evidence; International Cyber Law Treaties: Budapest Convention on Cybercrime; Tallinn Manual on Cyberwarfare	**15**
Unit II	**Cybercrimes – Legal Provisions and Enforcement** Classification of Cybercrimes: Hacking, phishing, cyberstalking, identity theft, financial fraud; Cyberterrorism, ransomware, and deepfake threats; Provisions under IT Act & IPC (Sections 66, 67, 72, etc.); Investigation and Adjudication Procedures - Role of law enforcement, Cyber Forensics and E-evidence collection; Landmark Cases: -Shreya Singhal v. Union of India, PNB fraud, Pegasus spyware	**15**
Unit III	**Digital Personal Data Protection (DPDP) Act and Privacy Law** Right to Privacy as a Fundamental Right (Justice Puttaswamy Judgment); Digital Personal Data Protection Act, 2023 – Overview and Purpose; Definitions: Personal data, consent, data	**15**

Dy. Registrar
Pandit Deendayal Upadhyaya
Shekhawati University,

	fiduciary, data principal, Lawful processing and meaningful consent, Rights of data principals (access, correction, grievance redressal), Obligations of data fiduciaries, Cross-border data transfer rules, Role of the Data Protection Board of India, Penalties and grievance handling mechanisms; Comparison with GDPR and other international models	
Unit IV	**Cybersecurity Policy, Institutional Guidelines & Compliance** National Cyber Security Policy (NCSP 2013) and Draft NCSP 2021; CERT-In Guidelines (April 2022 update); Guidelines for Intermediary Accountability and Due Diligence; Governance, Risk, and Compliance (GRC) Concepts; ISO/IEC 27001 and NIST Cybersecurity Framework; IT Governance and Secure Software Development Guidelines; Role of institutions: CERT-In, MeitY, I4C (Indian Cyber Crime Coordination Centre); Indian Computer Emergency Response Team; Data Protection Board (under DPDP Act)	**15**

Suggestive Readings:

1	Legal Aspects of Information Technology and Cyber Law – Saurabh Sharma, Vikas Publishing, 1st Edition, 2021
2	Cyber Law & Information Technology – Talwant Singh, Eastern Book Company, 1st Edition, 2022
3	Information Technology Law and Practice – Vakul Sharma, Universal Law Publishing, 6th Edition, 2021
4	The Information Technology Act, 2000 with Rules and Allied Laws – Taxmann Publications, Latest Edition, 2023
5	Cyber Law: The Indian Perspective – Justice Yatindra Singh, LexisNexis, 4th Edition, 2016
6	Data Protection Law: A Practical Guide to the GDPR – Rosemary Jay, Sweet & Maxwell, 5th Edition, 2020
7	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – OECD Publishing, Revised Edition, 2013
8	Handbook on Cyber Laws – Manoj Kumar Sinha, Universal Law Publishing, 1st Edition, 2015

Course Title:	**ISO 27000 Auditing Lab Manual**	**Course Code: 25MCL9201P**

Lab 1: Introduction to ISO/IEC 27001 and ISMS Concepts

Tasks:
1. Study the ISO/IEC 27001:2022 clauses and annex controls.
2. Identify key terms: asset, risk, control, threat, vulnerability.
3. Create a basic ISMS policy document template for a sample organization.

Lab 2: Context of the Organization and Risk Assessment

Tasks:
1. Define internal and external issues affecting information security.
2. Identify stakeholders and their requirements.
3. Perform a basic risk assessment using an asset-threat-vulnerability matrix.

Lab 3: ISMS Scope and Policy Development

Tasks:
1. Select a specific department or system for ISMS implementation.
2. Draft an ISMS scope statement.
3. Develop an ISMS information security policy aligned with ISO/IEC 27001.

Lab 4: Risk Treatment and Statement of Applicability (SoA)

Tasks:

Dy. Registrar
Pandit Deendayal Upadhyaya

	1. Select appropriate controls based on risk assessment. 2. Prepare a risk treatment plan with justification. 3. Draft a Statement of Applicability referencing Annex A controls. Lab 5: Internal Audit Planning and Execution ========== Tasks: 1. Draft an internal audit plan based on ISO 19011 guidelines. 2. Develop an audit checklist for selected clauses of ISO 27001. 3. Conduct a mock audit on a case study or sample process. Lab 6: Nonconformity Reporting and Corrective Actions ========== Tasks: 1. Record sample nonconformities identified in Lab 5. 2. Write a nonconformity report. 3. Propose and document corrective actions. Lab 7: ISMS Performance Evaluation and Metrics ========== Tasks: 1. Define KPIs for ISMS effectiveness (e.g., number of incidents, audit findings). 2. Analyze a case study or simulated data set. 3. Conduct a mock management review meeting. Lab 8: ISMS Documentation and Continuous Improvement ========== Tasks: 1. Prepare a list of mandatory and optional ISMS documents. 2. Conduct a gap analysis between existing and required documentation. 3. Propose improvements for ISMS documentation control and review processes.

Course Title:	**Digital Forensics**	**Course Code: 25MCL9204T**
Total Lecture hour 60		**Hours**
Unit I	**Introduction to Digital Forensics and Investigation Process** Overview and scope of digital forensics; Types of cybercrimes and digital evidence; Digital forensic investigation process: Identification, acquisition, preservation, analysis, documentation, and reporting; Role of digital forensics in incident response and law enforcement; Forensic readiness and planning.	**15**
Unit II	**Data Acquisition and Evidence Handling** Rules of evidence and legal standards (chain of custody); Evidence preservation and integrity (hashing, imaging); Bit-by-bit disk imaging and data recovery techniques; Write blockers and forensic hardware; Working with volatile data (memory, processes, network connections); File systems and data hiding techniques (steganography, encryption).	**15**
Unit III	**Analysis of Forensic Artifacts** Operating system artifacts: Windows Registry, log files, metadata, event logs; Linux Forensics: Log files: /var/log (auth.log, syslog, messages, secure, etc.); Bash history and command logs: ~/.bash_history, .zsh_history; User activity artifacts: last, w, who, lastlog, utmp, wtmp; Cron jobs and scheduled tasks: /etc/crontab, /etc/cron; File carving and data recovery; Email and browser forensics; Log file analysis and correlation; Timeline analysis and reconstruction; Anti-forensics and counter-forensics techniques and tools	**15**

Unit IV	**Specialized Forensics Domains and Legal Aspects** Network Forensics: packet capture, session reconstruction, intrusion detection; Mobile Device Forensics: Android and iOS data acquisition; Cloud Forensics: challenges, metadata tracking, legal jurisdiction; IoT Forensics: capturing data from smart devices; Legal frameworks and compliance: Admissibility of digital evidence in court; Laws: IT Act (India), GDPR, HIPAA (as applicable); Ethics and privacy in investigations with certain case studies.	**15**
Suggestive Readings:		
1	Guide to Computer Forensics and Investigations by Nelson, Phillips, and Steuart	
2	Digital Forensics by André Årnes	
3	Computer Forensics: Cybercriminals, Laws, and Evidence by John Vacca	
Tools:		
• Autopsy, FTK Imager, Sleuth Kit, Wireshark, Volatility, Plaso • Cellebrite (demo), MOBILedit, Oxygen Forensic Suite (trial)		

Course Title:	**Cloud Computing and Security**	**Course Code: 25MCL9205T**
Total Lecture hour 60		**Hours**
Unit I	**Fundamentals of Cloud Computing** Overview of cloud computing: History, benefits, and challenges; Cloud architecture: Frontend, backend, middleware, and network; Cloud service models: Infrastructure as a Service (IaaS); Platform as a Service (PaaS); Software as a Service (SaaS); Deployment models: Public, Private, Hybrid, and Community Cloud; Key Enabling Technologies: Virtualization, Containers, Orchestration (Kubernetes)	**15**
Unit II	**Cloud Infrastructure and Management** Cloud resource provisioning, scalability, and elasticity; Virtual machines, containers (Docker), serverless computing; Hypervisors: Type 1 vs Type 2; Cloud orchestration: Kubernetes, Terraform, Ansible basics; Storage types: Object, Block, and File Storage; Monitoring and cost management (e.g., AWS CloudWatch, Azure Monitor	**15**
Unit III	**Cloud Security Concepts and Architecture** Cloud security fundamentals: Confidentiality, Integrity, Availability (CIA); Shared Responsibility Model; Data protection in cloud: Data-in-transit, data-at-rest, and data-in-use encryption; Identity and Access Management (IAM); Cloud-specific threats and vulnerabilities (e.g., multi-tenancy risks, VM escape); Network security controls in cloud: Firewalls, Security Groups, Virtual Private Cloud (VPC)	**15**
Unit IV	**Governance, Compliance & Incident Response in Cloud** Cloud governance models and frameworks; Risk assessment and mitigation in cloud environments; Cloud compliance standards: ISO/IEC 27017, ISO/IEC 27018; PCI-DSS, HIPAA, GDPR, SOC 2; Security automation and DevSecOps in cloud; Cloud incident response and digital forensics; Case studies: AWS, Azure, GCP security breaches and compliance strategies	**15**
Suggestive Readings:		
1	Cloud Computing: Concepts, Technology & Architecture – Thomas Erl	
2	Architecting Cloud Computing Solutions – Kevin L. Jackson	
3	Cloud Security and Privacy – Tim Mather et al.	
Recommended Tools and Platforms		
Cloud Providers: AWS Educate, Microsoft Azure for Students, Google Cloud Free Tier **Tools**: Terraform, Docker, Kubernetes, AWS CLI, Wireshark, OpenVAS		

Dy. Registrar
Pandit Deendayal Upadhyaya
Shekhawati University,
Sikar(Rajasthan)

Course Title:	Network Security Using AI	Course Code: 25MCL9206T
Total Lecture hour 60		Hours
Unit I	**Cryptography and Secure Communication** Advanced Encryption Techniques (AES, RSA, ECC); Key Management and Public Key Infrastructure (PKI); Secure Communication Protocols: SSL/TLS, IPsec; Quantum Cryptography Basics; Zero Trust Architecture	15
Unit II	**Intrusion Detection, Prevention, and Incident Response** IDS/IPS Concepts and Tools (Snort, Suricata); Signature-Based vs Anomaly-Based Detection; Network Segmentation and Micro-segmentation; Threat Intelligence Platforms and Feeds; Incident Response Lifecycle & Digital Forensics	15
Unit III	**Ethical Hacking and Security Auditing** Reconnaissance and Vulnerability Scanning (Nmap, OpenVAS); Exploitation Techniques and Payloads (Metasploit); Web Security Testing (OWASP Top 10); Wireless and Mobile Security Testing; Penetration Testing Framework and Reporting	15
Unit IV	**Security Governance, Risk & Compliance (GRC)** Cyber Risk Management and Threat Modeling; Regulatory Compliance: ISO 27001, NIST CSF, PCI-DSS, GDPR; Security Operations Center (SOC) and SIEM Concepts; Log Management and Correlation; Business Continuity and Disaster Recovery Planning; Different tiers of Data Centers	15

Suggestive Readings:

1	Artificial Intelligence for Cybersecurity: Techniques and Applications – Mark Stamp, Springer, 1st Edition, 2022
2	Machine Learning for Cybersecurity – Xiaofeng Chen, Jian Shen, Springer, 1st Edition, 2020
3	Network Security and Artificial Intelligence – Richard Jiang, Springer, 1st Edition, 2020
4	Artificial Intelligence in Cybersecurity – Leslie F. Sikos, Springer, 1st Edition, 2020
5	Hands-On Artificial Intelligence for Cybersecurity – Alessandro Parisi, Packt Publishing, 1st Edition, 2019

Dy. Registrar
Pandit Deendayal Upadhyaya
Shekhawati University,
Sikar(Rajasthan)