MADHYA PRADESH BHOJ (OPEN) UNIVERSITY,
Raja Bhoj Marg Kolar Road, BHOPAL (M.P.)

PG DIPLOMA IN
CYBER SECURITY

Post Graduate Diploma in Cyber Security II Year

S. No.	Name of Subject	Assignment		Theory		Total Marks	
		Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks
1	Cyber Crime, Laws & Forensic Investigation	30	12	70	28	100	40
2	Mobile Concepts & Security	30	12	70	28	100	40
3	Cloud Computing	30	12	70	28	100	40
4	Project I: Industrial Training					100	40
	II Project -II					200	80
5	Lab: Mobile Concepts & Security					100	40
6	Lab: Cloud Computing					100	40

2

Cyber Crime, Laws & Forensic Investigation

Unit 1. Cyber Crime & Issues:

Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses, Ethical issues in IT, Ethical Conducts, technology trends that raise ethical issues.

Unit 2. Security Policies:

Need for an Information Security Policy, Information Security Standards-ISO, WWW policy, Email Security policy, corporate policy, sample security policy, Policy Review Process

Unit 3. Cyber Laws and Regulatory Framework of Information and Technology Act 2000:

Cyber Laws: Need for Cyber Laws, Copyright Act, Patent Law, IPR, Intellectual Property Law: Copy Right Law, Software License, Semiconductor Law and Patent Law, Software License.

Regulatory Framework: Digital Signature, E Signature, Electronic Records, ElectronicEvidence and Electronic Governance. Controller, Certifying Authority and Cyber Appellate Tribunal. (Rulesannounced under the Act)

Unit 4. Offenses & Penalties:

Offences under the Information and Technology Act 2000 & it's amendments, Penalty and adjudication. Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed). Limitations of Cyber Law.

Unit 5. Cyber Forensics Investigation

Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking, Cracking with GPU Systems, Hashcat. Work on open Source, Commercial tools and Cyber range.
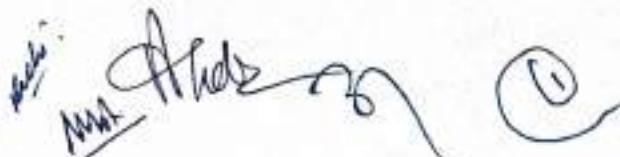
Mobile Concepts & Security

Unit I: Introduction to Mobile Concepts & Security

Mobile Security Model, Enterprise Mobile Environment, Mobile Crypto Algorithm.

Unit II: Mobile System Technology

Mobile Devices - features and security concerns, Platforms, Applications - development, testing anddelivery.

Unit III: Mobile Networks

Cellular Network - baseband processor and SIM card, GSM encryption and authentication and otherattacks, VoLTE and its working, WIFI Networks - public hotspots and enterprise WLANs, SSL/TLS, Web Technologies - server-side and client-side web applications

Unit IV: Mobility Management

Enterprise Mobility Program, Transactions Security, File Synchronization and Sharing, Vulnerability Assessments, BYOD Device Backup, Data Disposal/Sanitization, NAC for BYOD, Container Technologies, Exchange ActiveSync (EAS), Mobile Authentication, Mobile Management Tools.

Unit V: Scenario Testing

Cellular Attacks, Attacking Web Interface, Wireless Attacks, SSL attacks, Android, iOS

List of Practical's

➢ To understand various types of Cellular Attacks
➢ To identify WEP/WPA attacks.
➢ To understand mobile crypto algorithms.
➢ To use mobile management tools.
➢ To implement the mobile backup & data recovery using open-source tools.
➢ To use mobile vulnerability assessment tools.
➢ To do mobile testing using open source tools like Monkey Talk, Appium, Katalan Studio.
➢ To use the container technologies.

Cloud Computing

Unit I:

Infrastructure as a Service& Platform as a Service Learning Objective, Cloud Service Models, Infrastructure as a Service, Platform as a Service, Case Studies.

Unit II:

Software as a Service and Database as a Service Learning Objectives, Software as a Service (SaaS), Database as a Service (DBaaS).

Unit III:

Security as a Service Learning Objectives, Introduction to Security as a Service, Cloud Security Risk analysis, SECaaS Categories, Benefits Of Security As A Service, Evaluation of Cloud Security Issues, Cloud Security Standards.

Unit IV:

Specialized Cloud Services Learning Objectives, Recovery as a Service (RaaS), Identity as a Service (IDaaS), Storage as a Service, Communication as a Service (CaaS).

Unit V:

Cloud Security: Top concern for cloud users, Risks, Privacy Impact Assessment, Cloud Data Encryption, Security of Database Services, OS security, VM Security, Security Risks Posed by Shared Images and Management OS, XOAR, A Trusted Hypervisor, Mobile Devices and Cloud Security Cloud Security and Trust Management: Cloud Security Defense Strategies, Distributed Intrusion/Anomaly