ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

SYLLABUS OF
POST GRADUATE DIPLOMA IN CYBER SECURITY (PGDCS)

For Academic Session 2017-18

Duration: 18 Months **Total Credit: 48**

Semester - I		
Course Code	**Course Title**	**Credit**
CSP – 010	Operating System Basics	6
CSP – 011	Data Communication & Networking	6
CSP – 012	Information Security	6
Semester - II		
CSP – 013	Application Cyber Security	6
CSP – 014	Network Cyber Security	6
CSP – 015	Minor Project	2
Semester - III		
CSP – 016	White Hat Hacking	6
CSP – 017	Security Analysis and Reporting	6
CSP – 018	Major Project	4

1st Semester	
CSP-010 : OPERATING SYSTEM BASICS	
Block-1	**Windows**
Unit-1	Introduction, Types Of Operating System, My Computer, Recycle Bin, Desktop, Drives; Creating, Renaming a directory/folder, Make a file read only, hidden, Editing a file; Delete a file.
Unit-2	Listing the files in the directory, Create a file, Copy a file from one directory to the other, Deleting all files from a directory/folder, Deleting a director/folder, Formatting a hard disk and loading operating system, Domain, workgroup, Active Directory, User Management, Network Setting, Services, IIS Configuration
Block -2	**Linux**
Unit -1	Introduction, History of Linux, Distributions of Linux, Devices and drivers, File system hierarchy, The components: Kernel, Distribution, XFree86, Sawfish, Gnome, The command line commands, File, management commands, Working with nano, Working with help (man).
Unit -2	SSH and X-forwarding, Managing compressed archives with zip and tar, Working with GNU screen, How to add users and groups, working with su, working with sudo, Changing user password, Printing, Installing software with Yum, Yast, Rpm, Installing webmin.
CSP-011 : DATA COMMUNICATION & NETWORKING	
Block-1	**Introduction to Data communication and Networking**
Unit-1	Fundamentals of data communication and networking
Unit-2	Network Reference Models: OSI and TCP/IP Models
Unit-3	Transmission media and network devices
Block -2	**Physical and data link layer functionalities**
Unit -1	Analog and Digital Signals
Unit -2	Encoding
Unit -3	Multiplexing and Switching: FDM,TDM,WDM,SDM, Message Switching and Circuit Switching and Packet Switching
Unit -4	Data Link Control Protocols: Token Passing, CSMA/CD,CSMA,CSMA/CA
Block -3	**Internet Protocols and Services**
Unit-1	Network Layer : Internetworking, and IP addressing, ARP, RARP,ICMP,IGMP
Unit-2	Transport Layer protocols: TCP& UDP
Unit-3	Application Layer protocols: HTTP, HTTPs, SMTP, POP, DNS, TELNET, FTP
Unit-4	Internet and its Services: Intranet, Extranet, www, Email
CSP-012 : INFORMATION SECURITY	
Block-1	**Information Security Concepts and Cryptography**
Unit-1	Information Security Concepts: Information security issues, goals, architecture, attacks, Security Services and Mechanisms.
Unit-2	Introduction to Cryptography: Network security model, Cryptographic systems, Cryptanalysis, Steganography.Types of Cryptography: Symmetric key and Asymmetric Key Cryptography, Encryption and Decryption Techniques.

Unit-3	Cryptographic Algorithms: Cryptographic hash, Message Digest, Data Encryption Standard, Advanced Encryption Standard, RSA(Introductory concepts only)
Block-2	**Security Threats and Vulnerabilities**
Unit-1	Overview of Security threats and Vulnerability: Types of attacks on onfidentiality, Integrity and Availability. Vulnerability and Threats.
Unit-2	Malware: Viruses, Worms, Trojan horses
Unit-3	Security Counter Measures; Intrusion Detection, Antivirus Software
Block-3	**Ethical Issues in Information Security & Privacy**
Unit-1	Information Security, Privacy and Ethics
Unit-2	Cyber Crime and Cyber Terrorism
Unit-3	Hacking: Ethical issues, Ethical Hacking

2nd Semester	
CSP-013 : APPLICATION CYBER SECURITY	
Block-1	**System Security**
Unit-1	Desktop Security
Unit-2	Programming Bugs and Malicious code
Unit-3	Database Security
Unit-4	Operating System Security: Designing Secure Operating Systems, OS Security Vulnerabilities.
Block -2	**Security Management**
Unit -1	Disaster recovery
Unit -2	Digital Signature
Unit - 3	Ethical Hacking, Penetration Testing
Unit -4	Computer Forensics
Block -3	**Cyber Laws and Standards**
Unit-1	ISO 27001, Cyber Law (Information Technology Act, 2000)
Unit-2	International Standards maintained for Cyber Security
Unit-3	Security Audit ,Investigation by Investing Agency
Unit-4	Cyber Security Solutions
CSP-014 : NETWORK CYBER SECURITY	
Block-1	**Network Security**
Unit-1	Network Security Model, Network Security Threats
Unit-2	Firewalls: Overview, Types, Features, User Management
Unit-3	Intrusion Detection System , Intrusion Prevention System
Unit-4	Public Key Infrastructure, Digital Signature Schemes
Block-2	**Internet and Web Application Security**
Unit-1	Email security: PGP and SMIME
Unit-2	Web Security: Web authentication, Injection Flaws, SQL Injection
Unit-3	Web Browser Security
Unit-4	E-Commerce Security
Block-3	**Wireless Network Security**

Unit-1	Wireless Network Components
Unit-2	Security issues in wireless Networks
Unit-3	Securing a wireless network
Unit-4	Mobile security
CSP-015 : Minor Project	
Report (75 Marks)	Presentation & Viva (25 Marks)

3rd Semester	
CSP-016 : WHITE HAT HACKING	
Block-1	**Introduction to hacking**
Unit-1	**Introduction:** Hacking, Types of Hacking/Hackers, Cybercrime, Types of cybercrime, Hacker Mind set, Threats, Concept of ethical hacking, , Phases involved in hacking, Role of Ethical Hacking, Common Hacking Methodologies, Profiles of Hackers, Benefits of Ethical Hacking, Limitations of Ethical Hacking.
Unit-2	**Foot Printing & Reconnaissance:** Introduction to foot printing, Use of foot printing, Types of foot printing, Understanding the information gathering process, Information on a company website, methodology of the hackers, Tools used for the reconnaissance phase.
Unit-3	**System Hacking:** System hacking, Types of System hacking, hacking tools, Computer Hole, Hacking Process, Various methods of password cracking, Remote Password Guessing, Role of eavesdropping, Keystroke Loggers, Types of Keystroke Loggers, Detection, Prevention and Removal.
Unit-4	**Sniffers:** Introduction, Sniffer, Types of Sniffer, Protocols Susceptible to Sniffing, Active and Passive Sniffing, ARP Spoofing, ARP Spoofing, ARP Poisoning, DNS Spoofing Techniques, MAC Flooding, Sniffing Countermeasures.
Block-2	**Hacking Techniques**
Unit-1	**Trojans, Backdoors, Viruses, and Worms:** Trojans and Backdoors, Overt and Covert Channels, Types of Trojans, Reverse-Connecting Trojans, Netcat Trojan ,Indications of a Trojan Attack, Wrapping, Trojan Construction Kit and Trojan Makers , Countermeasure Techniques in Preventing Trojans, Trojan-Evading Techniques, System File Verification Sub objective to Trojan Countermeasures Viruses and Worms, Difference between a Virus and a Worm, Types of Viruses, Understand Antivirus Evasion Techniques, Understand Virus Detection Methods..
Unit-2	**Session Hijacking:** Understanding Session Hijacking, Phases involved in Session, Hijacking, Types of Session Hijacking, and Session Hijacking Tools.
Unit-3	**Social Engineering** Social Engineering, Common Types Of Attacks, Insider

	Attacks, Identity Theft, Phishing Attacks, Online Scams, URL Obfuscation, Social-Engineering Countermeasures.
Unit-4	**Denial of Service:** Denial of Service, Types of DoS Attacks, DDoS Attacks, BOTs/BOTNETs, "Smurf" Attack, "SYN", Flooding, DoS/DDoS Countermeasures.
Block-3	**Hacking Web applications and Wireless Networks**
Unit-1	**Hacking Web Applications & SQL Injection:** Hacking Web Servers, Types of Web Server Vulnerabilities, Attacks against Web Servers, IIS Unicode Exploits, Patch Management Techniques, Web Server Hardening Methods Web Application Vulnerabilities, Objectives of Web Application Hacking, Anatomy of an Attack, Web Application Threats, Google Hacking, Web Application Countermeasures Web-Based Password Cracking Techniques, Authentication Types, Password Cracker, Password Attacks: Classification ,Password-Cracking Countermeasures.
Unit-2	**SQL Injection and Buffer Overflows:** SQL Injection, Steps to Conduct SQL Injection, SQL Server Vulnerabilities, SQL Injection, Countermeasures Buffer Overflows, Types of Buffer Overflows and Methods of Detection, Stack-Based Buffer Overflows, Buffer Overflow Mutation Techniques
Unit-3	**Hacking Wireless Networks:** Introduction to 802.11, Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS, attacks, WLAN Scanners, WLAN Sniffers, Hacking Tools, Securing, Wireless Networks.
Unit-4	**IDS, Firewalls & Honey pots**

CSP-017 : SECURITY ANALYSIS AND REPORTING	
Block-1	**Multidisciplinary Risk Management.**
Unit-1	**Packet Analysis & Risk Management:** Introduction, Learning Objectives, Packet analysis and Packet Sniffers, Evaluating a packet sniffer, How packet sniffers work, The Multidisciplinary Approach, How to protect your sensitive resources? Frame the Threats and Sources, National Governments, Terrorists, Industrial Spies and Organized Crime Groups, Hacktivists, Hackers, Nature of the Computer Security Community, GAO Threat Table, Hierarchy of Needs, Multidisciplinary Risk Management, Solution strategies, Module 1 – Fundamentals of risk management, Module 2 – Applied standards and cyber risk management, Module 3 – Field skills on cyber risk management, Seven Principles of Network Security Analysis Strategy, Network Traffic Monitoring and Analysis, Importance of Network Monitoring and Analysis, Monitoring and Analysis Techniques, Router Based Monitoring Techniques, Non-Router Based Techniques
Unit-2	**Wireless Network Analysis:** Wireless Networks, Wi-Fi Networks, Wireless Standards, Wi-Fi Authentication Modes, Wireless Encryption, Break an Encryption, Wireless Threats, Wireless Hacking Methodology, Wireless Traffic Analysis, Launch Wireless Attacks, Crack Wireless Attacks. Best practices on

	using wireless networks. Tips on internet surfing via public wireless services.
Unit-3	**Intrusion Detection & Prevention System:** Intrusion Detection System, Types, Passive system v/s reactive system, Signature Based Detection v/s Anomaly Based Detection, Signature Based Detection of Worms and Polymorphic Worms, Control Flow Graph based approach for detecting Polymorphic Worms [2], Tools in intrusion detection, Needs and challenges, IDS in various domains, Intrusion Prevention Systems (IPS), Types of IPS, Host based Intrusion Prevention (HIP), Network based Intrusion Prevention (NIP).
Unit-4	**Cyber Crime. IT assets and wireless security:** Cybercrime, Overview, Categories, Challenges, Complexities, Effects, Solutions, How to report an incident?, IT assets and wireless security, Securing an asset, Steps of securing an asset, Hardware based security, Types of HSMs, HSM Functionality, How to implement HSM, Firewall, Types of Firewalls, Software Based Firewalls, Hardware Based Firewalls, How to prevent your network from anonymous attack., Wireless security, Use of Wi-Fi, Types of Wireless Security, WPA.
Block-2	**Internet Security Analysis**
Unit-1	**Malware Analysis:** Introduction, What is Malware Analysis?The Goals of Malware Analysis. Malware Analysis Techniques. Basic Static Analysis, Basic Dynamic Analysis, Advanced Static Analysis, Advanced Dynamic Analysis, Types of Malware, General Rules for Malware Analysis, Malware Functionality, Downloaders and Launchers, Backdoors, Reverse Shell, RATs, Botnets, RATs and Botnets Compared, Credential Stealers, INA Interception, Hash Dumping, Keystroke Logging, Persistence Mechanisms, Trojanized System, Binaries, DLL Load-Order Hijacking, Privilege EscalationUsing SeDebugPrivilege, Covering Its Tracks-User-Mode Rootkits, IAT Hooking, Inline Hooking, Tools for malware analysis, ApateDNS, Autoruns, BinDiff, BinNavi, Deep Freeze.
Unit-2	**Email Security Analysis:** Threat and Vulnerability analysis of the email system. Threats: Spam, Social Engineering (phishing, targeted attacks), Massive eavesdropping, Other targeted criminal acts, Vulnerabilities: Integrity of email communications, Confidentiality of email communications, Phishing, Types of Phishing, Clone Phishing, Spear Phishing, Phone Phishing, Phishing Techniques and Countermeasures: Email Spoofing, Web Spoofing, Pharming, Malware, Phishing through PDF Documents. Privacy and security countermeasures: Cryptography Overview, Encryption Algorithms, Key Exchange Algorithms, Signature Algorithms, Certificates.
Unit-3	**Vulnerability Assessment and Penetration Testing (VPAT):** Introduction, Benefits, Methodology, Vulnerability Assessment, Reasons for Vulnerability Existence, Steps for Vulnerability Analysis, Web Application Vulnerabilities, Types: SQL-Injection, Blind Injection Detection, Cross-Site Scripting, Broken Authentication & Session Management, Insecure Direct Object References, Failure to Restrict URL, Remote Code Execution. Vulnerability Assessment Using Acunetix, Working of Vulnerability Assessment Tool. Penetration Testing Overview: What is Penetration Testing? Step 1: Defining the Scope, Step 2: Performing the Penetration Test, Step 3: Reporting and Delivering Results, Why is Penetration Testing Required? When to Perform Penetration Testing? How is Penetration Testing Beneficial? Penetration Testing Method: Steps of Penetration Testing Method, Planning & Preparation, Reconnaissance,

	Discovery, Analysing Information and Risks, Active Intrusion Attempts, Final Analysis, Report Preparation. Penetration Testing Vs. Vulnerability Assessment, Penetration Testing, Vulnerability Assessment, Which Option is Ideal to Practice? Types of Penetration Testing: Types of Pen Testing, Black Box Penetration Testing. White Box Penetration Testing, Grey Box Penetration Testing, Areas of Penetration Testing. Penetration Testing Tools, Limitations of Penetration Testing, Conclusion.
Unit-4	**Social Engineering**: Social Engineering, Overview, Definition(s) of Social Engineering. The Social Engineering Life Cycle: Foot printing, Establishing Trust, Psychological Manipulation, The Exit. Social Engineering Attack Cycle: Research, Developing Rapport and Trust, Exploiting Trust Factor, Exploiting Trust Factor, Recruit & Cloak, Evolve/Regress. The Weapons of a Social Engineer: Shoulder Surfing, Dumpster Diving, Role playing, Trojan horses, Phishing, Surfing Organization Websites & Online forums, Reverse Social Engineering. Different Types of Social Engineering: Physical Social Engineering, Remote Social Engineering, Computer-based Social Engineering, Social Engineering by Email, Phishing, Nigerian 419 or advance-fee fraud scam, Pop-up windows / browser interceptions. Social Engineering by Phone, Mumble Attack, IVR or phone phishing. Detecting / Stopping Social Engineering Attacks. Defending Against Social Engineering.
Block-3	**Cyber Incident Handling and Reporting**
Unit-1	**Cyber security Incident Management:** The Cyber security Incident Chain, Stakeholders, Cyber security Incident Checklist. Five Phases of Cyber security Incident Management: Plan and Prepare, Detect and Report, Assess and Decide, Respond and Post-Incident Activity.
Unit-2	**Handling an Incident:** Preparation: Preparing to Handle Incidents, Preventing Incidents. Detection and Analysis: Attack Vectors, Signs of an Incident, Sources of Precursors and Indicators, Incident Analysis, Incident Documentation, Incident Prioritization& Incident Notification.
Unit-3	**Coordination and Information Sharing:** Coordination: Coordination Relationships, Sharing Agreements and Reporting Requirements. Information Sharing Techniques: Ad Hoc, Partially Automated, Security Considerations. Granular Information Sharing: Business Impact Information, Technical Information.
Unit-4	**Containment, Eradication, and Recovery:** Choosing a Containment Strategy, Evidence Gathering and Handling, Identifying the Attacking Hosts, Eradication and Recovery. Post-Incident Activity: Lessons Learned, Using Collected Incident Data, Evidence Retention.

CSP-018 : Major Project	
Report (75 Marks)	Presentation & Viva (25 Marks)