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

Syllabus for M.Sc. in Cyber Security (MSCS)

Duration: 02 Years **Total credit: 72**

1st Semester (MSCS)			
Theory			
Course Code	**Course Title**	**(T-L-P)**	**Credit**
CSP-10	Operating System Basics	T	02
CSP-11	Data Communication & Networking	T	04
CSP-12	Information Security	T	04
Total Theory Credits			**10**
Project / Laboratory			
CSPL-10	Operating System Basics Lab	L	02
CSPL-11	Data Communication & Networking Lab	L	02
CSPL-12	Information Security Lab	L	02
Total Project / Laboratory Credits			**06**
TOTAL SEMESTER CREDITS			**16**

2nd Semester (MSCS)			
Theory			
Course Code	**Course Title**	**(T-L-P)**	**Credit**
CSP-13	Application Cyber Security	T	04
CSP-14	Network Cyber Security	T	04
CSP-15	Web Technology	T	02
Total Theory Credits			**10**
Project / Laboratory			
CSPL-13	Application Cyber Security Lab	L	02
CSPL-14	Network Cyber Security Lab	L	02
CSPL-15	Web Technology Lab	L	02
Total Project / Laboratory Credits			**06**
TOTAL SEMESTER CREDITS			**16**
TOTAL CUMULATIVE CREDITS			**32**

3rd Semester (MSCS)			
Theory			
Course Code	**Course Title**	**(T-L-P)**	**Credit**
CSP-16	White Hat Hacking	T	04
CSP-17	Security Analysis and Reporting	T	04
CSPE-01	Application development using PHP	T	02
	Total Theory Credits		**10**
Project / Laboratory			
CSPL-16	White Hat Hacking Lab	L	02
CSPL-17	Security Analysis and Reporting Lab	L	02
CSPEL-01	Application development using PHP Lab	L	02
CSPP-04	Project Work	P	04
	Total Project / Laboratory Credits		**10**
	TOTAL SEMESTER CREDITS		**20**
	TOTAL CUMULATIVE CREDITS		**52**

4th Semester (MSCS)			
Theory			
Course Code	**Course Title**	**(T-L-P)**	**Credit**
CSP-18	E-Governance & Case Studies	T	04
CSP-19	Cyber law and Regulation of Cyberspace	T	04
CSPE-02	Programming in Java	T	04
CSPE-03	Programming in Python	T	02
	Total Theory Credits		**14**
Project / Laboratory			
CSPL-18	E-Governance & Case Studies Lab	L	02
CSPEL-02	Programming in Java Lab	L	02
CSPEL-03	Programming in Python Lab	L	02
	Total Project / Laboratory Credits		**06**
	TOTAL SEMESTER CREDITS		**20**
	TOTAL PROGRAMME CREDITS		**72**

1st Semester: Theory Syllabus

CSP-10 : OPERATING SYSTEM BASICS (2 Credit)	
Block-1	**Windows Operating System**
Unit-1	Introduction, Operating System Concept and its Types, Function of OS, Evolution of Operating Systems, Introduction to Windows, Version of Windows, Operating System Administrator, My Computer, Recycle Bin, Desktop, Drives, create a directory/folder, rename/change to a directory/folder, creating a file in a directory/folder, Make the file read only, Make the file/directory hidden, Editing a file in a directory/folder, Delete a file in a directory/folder.
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 Operating System**
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-11 : DATA COMMUNICATION & NETWORKING (4 Credit)	
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-12 : INFORMATION SECURITY (4 Credit)	
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 Confidentiality, 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

1st Semester: Practical Syllabus

CSPL-10: OPERATING SYSTEM BASICS LAB (2 Credit)			
Windows OS			**Linux OS**
1	Windows 7 installation	**16**	Red Hat Linux Installation
2	File and folder management in Windows	**17**	Linux Installation using Ubuntu
3	Create a file in windows	**18**	Linux Installation using Open Suse
4	Create a folder in Windows	**19**	Working with Linux Graphical User Interface
5	Copy a file to a folder	**20**	Working with terminal mode
6	Move a file to a folder	**21**	Basic Linux commands used in terminal Mode
7	Rename a file/ folder	**22**	Creating a file using Nano
8	Delete a file / folder	**23**	Working with the su command
9	Make a file read only	**24**	Working with sudo
10	Hide the file and unhide the file in Win 7	**25**	User and group management
11	Working with the command prompt	**26**	Working with Permissions
12	Steps to create user accounts	**27**	Installing Software with Rpm
13	Changing Your Password	**28**	Working with Yum
14	Changing Your Picture	**29**	Yast
15	Creating a Password-Reset Disk	**30**	Webmin
		31	Data compression in Linux

CSPL-11 : DATA COMMUNICATION & NETWORKING LAB (2 Credit)	
Expt-1	To study about different physical equipment's used for networking
Expt-2	To study different internetworking devices in a computer network
Expt-3	To study the working of Basic Networking Commands
Expt-4	To assign IP address to the PC connected to the internet
Expt-5	To connect the computers in Local Area Network
Expt-6	Creating a Network topology using CISCO packet tracer software

CSPL-12 : INFORMATION SECURITY LAB (2 Credit)	
Expt-1	To study the Private Key and Public Key cryptographic systems.
Expt-2	To study the classical encryption techniques: substitution and transposition
Expt-3	To analyze the encryption and decryption of RSA – Public Key Cryptography Algorithm
Expt-4	To study working of Intrusion detection System (IDS) tool
Expt-5	To study the prevention mechanisms to avoid Virus and other Malware in one's PC
Expt-6	To study the prevention mechanisms to protect one's PC from Hackers

2nd Semester: Theory Syllabus

CSP-13 : APPLICATION CYBER SECURITY (4 Credit)	
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-14 : NETWORK CYBER SECURITY (4 Credit)	
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-15: WEB TECHNOLOGY (2 Cr.)	
Block-01	**Web Applications-I**
UNIT -01	**Getting Started with HTML** Introduction of HTML, Writing my first HTML Page, Basic tags used in HTML, Elements In HTML, Attributes In HTML, Formatting In HTML, Meta Tags and their use, Commenting a HTML Code, Images and incorporating images, working with Tables, Working with Lists, Working with hyperlinks, Frames and frame management, Working with Iframes, Working with Block elements.
UNIT -02	**Advanced HTML** Background images, Coloured text and coloured background, working with fonts, Form designing and Form Management, Using Multimedia inside HTML, Marquee Tag, Headers, Working with Layouts, Role of Tags in Html, Attributes in Html, Event Handling, MIME Media Types.
Block-02	**Web Applications-II**
UNIT -03	**Getting Started With CSS** Introduction of CSS, CSS Syntax, CSS Selectors, Ways To Insert CSS, Background image handling, Background colour management using CSS, Text management using CSS, Font management using CSS, Managing Hyperlinks using CSS, Managing Lists using CSS, Designing Tables using CSS, Working with the BOX Model, Designing Borders using CSS, Designing Outline using CSS, Setting Page Margin using CSS.
UNIT -04	**Getting Started With JS** JavaScript Basics, JavaScript Syntax, Enabling JavaScript in Browsers, Placing JavaScript, Variables, Operators, Conditional Statement(if, if else), Switch case, Loops(while, do while and for loop), Functions, Events and event handling, Cookies, Page Redirection, Dialog Box(Alert, Confirm, prompt), void keyword, Printing webpage using JavaScript.
Block-03	**Web Technology**
UNIT -01	**Website Development** Websites Overview, Websites Types, Website Designing, Websites Development, Website Publishing, Website URL Registration, Website Hosting, Website Security.
UNIT -02	**HTML-5 & XHTML** **HTML-5:** Overview, Syntax, Attributes, Events, SVG, MathML, Web Storage, Web SQL, Server-Sent Events, Web Socket, Canvas, Audio & Video, Geolocation, Micro-data, Drag & drop, Web Workers, Indexed DB, Web Messaging, Web CORS, Web RTC. **XHTML:** What is XHTML, Why use XHTML, HTML v/s XHTML, XHTML Syntax, XHTML Events, XHTML Doc types, XHTML Attributes, Difference between HTML4 and HTML5, Difference between HTML and XHTML.
UNIT -03	**XML** Introduction to XML - eXtensible Markup Language ,XML for data centric files ,Displaying XML on the web, Displaying XML with CSS ,XSLT - eXtensible Style Sheet Language ,Displaying XML with XSLT.
UNIT -04	**Macromedia Flash** What is flash?, Starting of Flash., The workspace, Using the Tools panel, Selection Tool, Coloring Tool, Text Tool., Create a new Flash Document, Animate using Frame, Symbols and Animation, Crate a Motion Tween, Shape Tween, Motion Guide Tween, Working with layers.

2nd Semester: Practical Syllabus

CSPL-13 : APPLICATION CYBER SECURITY LAB (2 Credit)	
Expt-1	Study of steps to protect your personal computer system by creating User Accounts with Passwords and types of User Accounts for safety and security.
Expt-2	Study the steps to protect a Microsoft Word Document of different version with different operating system.
Expt-3	Study the steps to remove Passwords from Microsoft Word
Expt-4	Study various methods of protecting and securing databases.
Expt-5	Study "How to make strong passwords" and "passwords cracking techniques".
Expt-6	Study the steps to hack a strong password.

CSPL-14 : NETWORK CYBER SECURITY LAB (2 Credit)	
Expt-1	Study of different wireless network components and features of any one of the Mobile Security Apps.
Expt-2	Study of the features of firewall in providing network security and to set Firewall Security in windows.
Expt-3	Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome)
Expt-4	Study of different types of vulnerabilities for hacking a websites / Web Applications.
Expt-5	Analysis the Security Vulnerabilities of E-commerce services.
Expt-6	Analysis the security vulnerabilities of E-Mail Application.

CSPL-15 : WEB TECHNOLOGY LAB (2 Credit)	
Expt-1	Develop static pages (using only HTML) of an online Book store. The pages should resemble: www.amazon.com.
Expt-2	Validate the registration, user login and user profile pages using JavaScript.
Expt-3	Use frames to Include Images and Videos.
Expt-4	Add a Cascading Style sheet for designing the web page.
Expt-5	Write a program in JavaScript to print the Fibonacci series.
Expt-6	Write a program in JavaScript to perform Arithmetic Operations.
Expt-7	Write a JavaScript function that checks whether a passed String is palindrome or not.
Expt-8	Write a program in html to Click the button to get your coordinates.
Expt-9	Create an XSLT document to meet the following requirements • Page should have a title Students. • Page should have a table of student details. • Columns should have following headers: Roll No, First Name, Last Name, Nickname, Marks
Expt-10	Write a table using html and CSS to create examination date sheet of OSOU.

3rd Semester: Theory Syllabus

CSP-16 : WHITE HAT HACKING (4 Credit)	
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-17 : SECURITY ANALYSIS AND REPORTING (4 Credit)	
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 Escalation Using 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? When to Perform Penetration Testing? How is Penetration Testing Beneficial? Penetration Testing Method: Steps of Penetration Testing Method, Planning & Preparation, Reconnaissance, Discovery, Analyzing 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.

CSPE-01: Application Development Using PHP (4 Credit)	
Block-1	**Introduction to PHP**
Unit-1	**Basics of PHP** Introduction**,** Algorithm, Flowchart, Program, Programming Languages and its generation, OOPs Concept.
Unit-2	**Introduction to PHP** **PHP Basic** (installing Process of PHP (XAMPP)), Structure of PHP program, Write the first PHP program, Syntax, Variables, Constants, Echo and Print Command, Data Type, Array Data Type, Types of Array in PHP, Multi dimension Array, Object data Type.
Block -2	**PHP**
Unit -3	**Condition Statement** (if Statement, if else statement, if else if else statement, Switch Statement), **Loop (**While, do While, for and for each Loop). Super global Variable.
Unit -4	**Form Management** **Form Design:** get and Post method, Working with Textbox, Text Area, Password, Check Box, Radio Buttons, Drop down Box, File, Submit Buttons, Reset, Button, data, date Time, Email, search, Tel, URL etc. Working with $Globals, $Server, $ENV, $SESSION, $COOKIE with Example. Form Validation, Form Navigation
Block -3	**Advance PHP**
Unit-1	**(Object Oriented Concept in PHP)** Introduction, Basics of OOP in PHP, Pillars of OOPS, Understanding Classes and Objects, PHP Class Properties and Methods, Static, Constants, Constructor and destructor, Magic Methods in PHP, Inheritance in PHP, Interface, Abstract class, Final, Polymorphism
Unit-2	**(File management and Exception Handling)** Introduction, what is File, File Formats supported by PHP, File Operations, File Permission. Error Handling in PHP, Exception Handling, try… catch and throw, Top Level Exception Handler, User Defined Exception Handler
Unit-3	**(Database Connectivity in PHP)** Introduction, Introduction to MySQL, What can MySQL do? Why MySQL use with PHP, Features of MySQL, Communication between PHP and MySql Server: Create a connect to the MySql server (mysql, mysqli (MySQL improved, pdo (PHP Data Object)), Create Database and Tables in MySql, Insert Data into MySql Server, Mysql SELECT Statement, Update MySql Records, Delete MySql Records, Example database access from Webpage.

3rd Semester: Practical Syllabus

CSPL-16 : WHITE HAT HACKING LAB (2 Credit)	
Expt-1	To learn about hacking tools and skills.
Expt-2	To study about Footprinting and Reconnaissance.
Expt-3	To study about Fingerprinting.
Expt-4	To study about system Hacking.
Expt-5	To study about Wireless Hacking.
Expt-6	To learn & study about Sniffing & their tools.

CSPL-17 : SECURITY ANALYSIS AND REPORTING LAB (2 Credit)	
Expt-1	Study various methods for Taping into the wire.
Expt-2	Study the steps for installing Wireshark, the packet-sniffing tool for performing Network analysis.
Expt-3	Study of working with captured packets.
Expt-4	Study of advanced Wireshark features.
Expt-5	Study of security packet analysis.
Expt-6	Study of Operating System Fingerprinting.

CSPEL-01: APPLICATION DEVELOPMENT USING PHP LAB (2 Credit)	
Expt-1	Show the steps to install XAMM Software for PHP Programming.
Expt-2	Write a PHP program to display a digital clock which displays the current time.
Expt-3	Write the PHP programs to do the following: a. Implement simple calculator operations. b. Find the transpose of a matrix. c. Multiplication of two matrices
Expt-4	Write a PHP program to Swapping two numbers
Expt-5	Write a PHP program to create a login table.
Expt-6	Write a PHP program for login page using database connectivity
Expt-7	Write a PHP program to find a word in a file.
Expt-8	Write a PHP program to upload an image to the data base.
Expt-9	Write a PHP program to design a registration for with proper validation
Expt-10	Write a program states whether a year is leap year or not from the specified range of years (1991 - 2016).using Exception Handling.

CSPP-05 : PROJECT WORK (2 Credit)