Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Scheme of Teaching & Examination

M.Tech. (Information Security)

UNDER COMPUTER SCIENCE & ENGINEERING BOARD

3rd Semester

S.N.	Board of Study	Subject Code	Subject	Periods per Week			Scheme of Examination Theory/Practical			Total Marks	Credit L+(T+P)/2
				L	T	P	ESE	CT	TA		
1	Computer Science & Engg.	571311 (22)	Wireless Security Systems	3	1	-	100	20	20	140	4
2	Refer Table – III		Elective – III	3	1	-	100	20	20	140	4
3	Computer Science & Engg.	571321 (22)	Preliminary work on Dissertation	-	-	28	100	-	100	200	14
4	Computer Science & Engg.	571322 (22)	Technical Seminar	-	-	3	-	-	20	20	2
Total				**6**	**2**	**31**	**300**	**40**	**160**	**500**	**24**

L-Lecture, **T**- Tutorial, **P**- Practical, **ESE**- End Semester Examination, **CT**- Class Test, **TA**- Teacher's Assessment

Table – III

Elective – III

S.N.	Board of Study	Subject Code	Subject
1	Computer Science & Engg.	571331 (22)	Security Audit and Risk Assessment
2	Computer Science & Engg.	571332(22)	Cloud Computing
3	Computer Science & Engg.	571333(22)	Information Security in Industries

Note (1) → Choice of elective once made for an examination cannot be changed in future examinations.
Note (2) → Examination Duration of all Theory papers will be of THREE hours.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 3rd
Subject: **Wireless Security Systems**
Total Theory Periods: **40**
Minimum number of Class tests to be conducted: 02

Branch: **Information Security**
Code: **571311 (22)**
Total Tutorial Periods: **12**
Total Marks in End Semester Exam: **100**

Unit-I WIRELESS FUNDAMENTALS
Wireless Hardware, Wireless Network Protocols, Wireless Programming, WEP Security, Basic concepts on Wireless Cellular Technologies, Wireless reality, Security essentials, Information classification standards, Wireless Threats, Cracking WEP, Hacking Techniques, Wireless Attacks, Airborne Viruses.

Unit-II STANDARDS AND POLICY SOLUTIONS
Network Solutions, Software Solutions, Physical Hardware Security, Wireless Security, Securing WLAN, Virtual Private Networks, Intrusion Detection System, Wireless Public Key infrastructure, Auditing tools, Pocket PC hacking, Wireless hack walkthrough.

Unit-III SECURITY PRINCIPLES AND AUTHENTICATIONS
Security Principles, Authentication, Access control and Authorization, Non-repudiation, Privacy and Confidentiality, Integrity and Auditing, Security Analysis Process, Privacy in Wireless World, Legislation and Policy, Identify targets and roles analysis, Attacks and Vulnerabilities, Analyze Mitigations and Protection.

Unit-IV CONFIGURATIONS
WLAN Configuration, IEEE 802.11, Physical layer, Media Access Frame format, Systematic Exploitation of 802.11b, WLAN, WEP Decryption script, Overview of WEP attack, Implementation, Analyses of WEP attacks.

Unit-V M-COMMERCE SECURITY
Mobile Commerce Security and Payment Methods, Reputation and Thrust, Intrusion detection, Vulnerabilities analysis of mobile commerce platform, Secure Authentication for mobile users, Mobile Commerce security, Payment methods, Mobile Coalition, Key Evolving, Digital Signatures scheme for wireless mobile networks.

Text Books :

1. Russel Dean Vines, "Wireless Security Essentials: Defending Mobile from Data Piracy", John Wiley & Sons, First Edition, 2002.
2. Cyrus, Peikari and Seth Fogie, "Maximum Wireless Security", SAMS Publishing, 2002.
3. Wen Chen Hu, Chang Wiu Lee, and Weidong Kou, "Advances in Security and Payment Methods for Mobile Commerce", Idea Group Inc, 2004**.**

Reference Books :

1. Tara M. Swaminathan, Charles R. Eldon, "Wireless Security and Privacy: Best Practices and Design Techniques", Addison Wesley, 2002.
2. Bruce Potter and Bob Fleck, "802.11 Securities", O'Reilly Publications, 2002.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 3rd
Subject: **Security Audit and Risk Assessment (Elective-III)**
Total Theory Periods: **40**
Minimum number of Class tests to be conducted: 02

Branch: **Information Security**
Code: **571331 (22)**
Total Tutorial Periods: **12**
Total Marks in End Semester Exam: **100**

Unit-I INTRODUCTION
Evolution of information security, Information Assets, Security standards, Organizational impacts, Security certifications, Elements of information security program, Need for security assessment, Security assessment process, Security assessment planning, Business drivers, Scope definition, Consultant's perspective, Client's perspective, Development of project plan, Initial information gathering – Initial preparation, Analysis of gathered information.

Unit-II RISK ASSESSMENT
Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation, Security Risk assessment, Project Management, Security Risk Assessment approaches and methods.

Unit-III STANDARDS AND LEGISLATIONS
Information Security Standards (ISS), Information Security Legislation (ISL), Formal security, Verification, Security verification with SSL.

Unit–IV SECURITY MONITORING AND AUDITING
Assurance and Trust, Need for Assurance, Role of Requirements in Assurance, Audit Assurance in Software Development Phases, Building Secure and Trusted Systems, Designing an Auditing System, Implementation Considerations, Auditing to Detect Violations of a security Policy, Auditing Mechanisms, Audit Browsing.

Unit-V RISK MANAGEMENT AND SECURITY PLANNING
Risk Management, Process Overview, Cost-Benefit Analysis, Risk Analysis, Laws and Customs, Human Issues, Organizational issues, Information system Risk analysis, System approach to risk management, Threat assessment, Assets and Safeguards, Modes of risk analysis, Effective risk analysis, Qualitative Risk analysis, Value analysis.

Text Books :

1. Sudhanshu Kairab, "A Practical Guide to Security Assessments", CRC Press, 2005.
2. Douglas J. Landoll, "A Security Risk Assessment Handbook", Auerbach publications, 2006.
3. Matt Bishop, "Introduction to Computer Security", Addison-Wesley Professional, 2005.
4. Thomas R. Peltier, "Information Security Risk Analysis", CRC Press, 2001.

Reference Books :

1. Matt Bishop, "Computer Security: Art and Science", Addison-Wesley Professional, 2003.
2. Joseph M. Kizza, "Computer Network Security", Springer, 2005.
3. C. A. Roper, "Risk management for Security professional", Elsevier, 1999.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 3rd | Branches: **Information Security and Computer Technology.**
Subject: **Cloud Computing (ELECTIVE – III)** | Code: **571332 (22)**
Total Theory Periods: **40** | Total Tutorial Periods: **12**
Minimum number of Class tests to be conducted: 02 | Total Marks in End Semester Exam: **100**

Unit - I
What is the Cloud? The Emergence of Cloud Computing, Cloud-Based Service Offerings, Benefits of using a Cloud Model, What Are the Key Characteristics of Cloud Computing?, The Evolution of Cloud Computing – Hardware & Internet Software Evolution.

Unit - II
Communication-as-a-Service (CAAS), Infrastructure-as-a-Service (IAAS), Monitoring-as-a-Service (MAAS), Platform-as-a-Service (PAAS), Software-as-a-Service (SAAS).

Unit - III
The Evolution from the MSP Model to Cloud Computing and Software-as-a-Service, The Cloud Data Center, Basic Approach to a Data Center-Based SOA, Where Open Source Software is Used?, Service-Oriented Architectures as a Step Toward Cloud Computing.

Unit - IV
Cloud Security Challenges, Software-as-a-Service, Security Management People, Security Governance, Security Portfolio Management, Security Architecture Design, Virtual Machine Security, Identity Access Management (IAM), Data Security.

Unit - V
What is a Smartphone?, Mobile Operating Systems for Smartphone's (iPhone, Windows Mobile), Google(Android) Blackberry, Ubuntu Mobile Internet, Mobile Platform Virtualization (KVM, VMWare).

Text Books :

1. Toby Velte, Anthony Vote and Robert Elsenpeter, "Cloud Computing: A Practical Approach", McGraw Hill, 2002.

Reference Books :

1. George Reese, "Cloud Application Architectures: Building Applications and Infrastructures in the Cloud", O'Reilly Media, 2003.

2. Tim Matherm, Subra Kumaraswamy and Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on *Ris*ks and Compliance", O'Reilly Media, 2005.

Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 3rd
Subject: **Information Security in Industries (ELECTIVE – III)**
Total Theory Periods: **40**
Minimum number of Class tests to be conducted: 02

Branch: **Information Security**
Code: **571333 (22)**
Total Tutorial Periods: **12**
Total Marks in End Semester Exam: **100**

Unit-I INFORMATION SECURITY POLICIES

About Policies, Why Policies are Important ?, When policies should be developed?, How Policy should be developed?, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property Rights and Policies, Incidence Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support.

Unit-II INFORMATION SECURITY OBJECTIVES

Policy Definitions, Standards, Guidelines, Procedures with examples, Policy Key elements, Policy format and Basic Policy Components, Policy content considerations, Program Policy Examples, Business Goals Vs Security Goals, Computer Security Objectives, Mission statement Format, Examples, Key roles in Organization, Business Objectives, Standards, International Standards.

Unit-III WRITING SECURE POLICIES

Writing the Security Policies, Computer location and Facility construction, Contingency Planning, Periodic System and Network Configuration Audits, Authentication and Network Security, Addressing and Architecture, Access Control, Login Security, Passwords, User Interface, Telecommuting and Remote Access, Internet Security Policies, Administrative and User Responsibilities, WWW Policies, Application Responsibilities, E-mail Security Policies.

Unit-IV ESTABLISHING POLICIES

Establishing Type of Viruses Protection, Rules for Handling Third Party Software, User Involvement with Viruses, Legal Issues, Managing Encryption and Encrypted data, Key Generation considerations and Management, Software Development policies, Processes, Testing and Documentation, Revision control and Configuration management, Third Party Development, Intellectual Property Issues.

Unit-V MAINTAINING POLICIES

Maintaining the Policies, Writing the AUP, User Login Responsibilities, Organization's responsibilities and Disclosures, Compliance and Enforcement, Testing and Effectiveness of Policies, Publishing and Notification, Requirements of the Policies, Monitoring, Controls and Remedies, Administrator Responsibility, Login Considerations, Reporting of security Problems, Policy Review Process, The Review Committee, Sample Corporate Policies, Sample Security Policies.

Text / Reference Books :

1. Scott Barman, "Writing Information Security Policies", SAMS Publishing, 2002.

2. Thomas R. Peltier, "Information Policies, Procedures and Standards", CRC Press, 2004.