Examination Scheme and Syllabus

for

Post Graduate Diploma in Cyber Security and Law (PGDCSL)

w.e.f. 2021-22

(Choice Based Credit System)

CH. BANSI LAL UNIVERSITY

BHIWANI

Chaudhary Bansi Lal University, Bhiwani

(Established under Govt of Haryana Act No 25 of 2014)

Study & Evaluation Scheme of PGDCSL

Summary

- **Programme: Post Graduate Diploma in Cyber Security and Law (PGDCSL)**
- **Eligibility: Graduation with 50% marks with Mathematics as one of the subject**
- **Duration: One Year full time (Two Semesters)**
- **Medium: English**
- **Minimum Required Attendance: 75%**
- **Total Credits: 54**

Assessment/ Evaluation

Internal Marks	External Marks	Total Marks
20	80	100

Internal Evaluation

Minor Test	Attendance	Assignment(s)
10	05	05

Duration of Examination

External	Minor Test (Internal)
3 hrs	$1^1/_2$hr

To qualify the course, a student is required to secure a minimum of 40% marks in aggregate including the end semester examination and internal evaluation (i.e. both internal and external). A candidate who secures less than 40% of marks in a course shall be deemed to have failed in that course. The student should have at least 40% marks in aggregate to clear the semester.

Note: Students should be involved in extracurricular activities through Hobbies Club (Non-credit) such as Poetry, Science, Club, Drama etc. and will be awarded a letter grade at the competition of Diploma.

Question Paper Structure

1. *The paper shall consist of 9 questions. Out of which, first question shall be of short answer type and will be compulsory. Question No. 1 shall contain 8 parts representing all units of the syllabus and students shall have to answer all parts.*
2. *The remaining 8 questions shall have internal choice. The weightage for each question shall be 16 marks.*

Program Outcomes for Post Graduate Program (CBCS) in the Faculty of Sciences

PO1	Knowledge	Capable of demonstrating comprehensive disciplinary knowledge gained during course of study
PO2	Communication	Ability to communicate effectively on general and scientific topics with the scientific community and with society at large
PO3	Problem Solving	Capability of applying knowledge to solve scientific and other problems
PO4	Individual and Team Work	Capable to learn and work effectively as an individual, and as a member or leader in diverse teams, in multidisciplinary settings.
PO5	Investigation of Problems	Ability of critical thinking, analytical reasoning and research based knowledge including design of experiments, analysis and interpretation of data to provide conclusions
PO6	Modern Tool usage	Ability to use and learn techniques, skills and modern tools for scientific practices
PO7	Science and Society	Ability to apply reasoning to assess the different issues related to society and the consequent responsibilities relevant to the professional scientific practices
PO8	Life-Long Learning	Aptitude to apply knowledge and skills that are necessary for participating in learning activities throughout the life
PO9	Environment and Sustainability	Ability to design and develop modern systems which are environmentally sensitive and to understand the importance of sustainable development.
PO10	Ethics	Apply ethical principles and professional responsibilities in scientific practices
PO11	Project Management	Ability to demonstrate knowledge and understanding of the scientific principles and apply these to manage projects

Program Specific Outcomes for Post Graduate Diploma in Cyber Security and Law (CBCS)

After successful completion of the program, a student will be able to:

PSO1	Develop competency to administer knowledge and awareness in the cyber security discipline along with learning aptitude for lifelong endurance in professional realm.
PSO2	Develop proficiency to adapt to contemporary technologies, skills and models for computing practice required for Cyber Security and Law.
PSO3	Acquire expertise to adopt skills realized during research, experimentation and trending technology cognizance to solve industrial problems.
PSO4	Promote professional competence to aspire careers in Commercial/ Government Sectors, Academics/ consultancy/ Research and Development for technological innovations, and collateral fields related to Cyber Crime and Cyber Security.
PSO5	Foster analytical skills for programming and adept computer based designing of systems in the domains concordant to Algorithm Design, System Software, Web and Application Security, Data Security, Cryptography, Cloud Security, etc.

Outline of Type of courses

- **Core Course**: A course, which should compulsorily be studied by a candidate as a core requirement is termed as a Core course.
- **Discipline Specific Elective (DSE) Course**: Elective courses may be offered by the main discipline/subject of study is referred to as Discipline Specific Elective. The University/Institute may also offer discipline related Elective courses of interdisciplinary nature (to be offered by main discipline/subject of study).
- **Skill Enhancement Courses (SEC):** courses are the courses based upon the content that leads to Knowledge enhancement. These courses are value-based and/or skill-based and are aimed at providing hands-on-training, competencies, skills. These courses may be chosen from a pool of courses designed to provide value-based and/or skill-based knowledge.
- **Open Elective Courses (OEC):** For Open Elective courses, students will have to choose a course from the list of open electives offered by other Departments of University.
- **Ability Enhancement Courses (AEC):** These courses enhance the ability of a student which includes Communication Skills course.

Outline of Mode of Learning

- **Self-Learning (SL):** Self learning by students using prescribed open learning resource.
- **Guided Self Learning (GSL):** Guided Self learning-teachers to brief students about the open learning resources.
- **Blended Learning (BL):** Blended learning in the classroom-using traditional teaching combined with digital learning.
- **Classroom Learning (CL):** Only classroom, lab or field learning.

Self-Learning Courses (SL)

Guidelines:

Objective: These courses intend to create habits of reading books and to develop writing skills in a manner of creativity and originality. The students are to emphasis his/her own ideas/words which he/she has learnt from open learning resources, different books, journals and newspapers and deliberate the same by adopting different ways of communication techniques and adopting time scheduling techniques in their respective fields of research.

Aims:

- To motivate the students for innovative, research and analytical work
- To inculcate the habit of self-study and comprehension
- To infuse the sense of historical back ground of the problems
- To assess intensity of originality and creativity of the students

Instructions for Students

- Each student has to select a topic related to title of the course.
- Each student has to prepare a manuscript related to title of the course.
- Expected to be creative and original in approach.
- Submit handwritten manuscript of A4 size 8-10 pages.
- Organize manuscript in three broad steps:
    - Introduction
    - Main Body
    - Conclusions
- Use headings and sub-headings.
- Use graphics wherever necessary.
- Give a list of books/references cited/used.

The examiner will assess the students as follows:

Maximum Marks-25

- Manuscript :10 Marks
- Viva-Voce :15 marks.

Guided Self-Learning Courses (GSL)

Guidelines:

Each student has to select a topic and prepare a presentation related to title of the course based on guided self-learning. Head of the department will create a mentor-mentee group (ten students per group). A mentor will guide mentees in choosing topic and preparing presentation. Each student will have to deliver a presentation of 15 minutes' duration before the students and teachers of the department. **A three-member committee (mentor of student and two teachers of the department of different branches) duly approved by the departmental council will be constituted to evaluate the presentation.** The following factors will be taken into consideration while evaluating the students.

Maximum Marks-25

Presentation: 10 marks
Depth of the subject matter: 10 marks
Viva-Voce: 05 marks

w.e.f. 2021-2022

Scheme of Examination for PGDCSL

Semester: 1st (w.e.f. 2021-22) **Credits – 27** **Marks – 825**

Sr. No.	Course Code	Title of the Course	Mode of Learning	Course Type	Credit			Contact Hours per week			Examination Scheme			Total Marks
					Theory	Practical/ Seminar	Total	Theory	Practical/ Seminar	Total	External Marks	Internal Marks	Practical/ Seminar Marks	
1	21PGDCSL101	Fundamentals of Computer Security	CL/BL	CC	4	--	4	4	--	4	80	20	--	100
2	21PGDCSL102	Network Basics	CL/BL	CC	4	--	4	4	--	4	80	20	--	100
3	21PGDCSL103	Fundamentals of Web Designing	CL/BL	CC	4	--	4	4	--	4	80	20	--	100
4	21PGDCSL104	Cryptography	CL/BL	CC	4	--	4	4	--	4	80	20	--	100
5	21PGDCSL105	Cloud Fundamentals	CL/BL	CC	4	--	4	4	--	4	80	20	--	100
6	21PGDCSL106	Lab-I (Based on 20PGDCSL102)	CL	SEC	--	2	2	--	4	4	--	20	80	100
7	21PGDCSL107	Lab-II (Based on 20PGDCSL103)	CL	SEC	--	2	2	--	4	4	--	20	80	100
8	21PGDCSL108	Seminar	GSL	SEC	1	--	1	1	--	1	--	25	--	25
		Open Elective/MOOCs Courses	BL	OEC	2	--	2	2	--	2	80	20	--	100
	Total				--	--	27	--	--	31	--	--	--	825

CC - Core Course; **SEC-Skill Enhancement Course;** **AEC- Ability Enhancement Course;**

Scheme of Examination for PGDCSL

Semester: 2nd (w.e.f. 2021-22) **Credits – 27** **Marks – 850**

Sr. No.	Course Code	Title of the Course	Mode of Learning	Course Type	Credit			Contact Hours per week			Examination Scheme			Total Marks
					Theory	Practical/ Seminar	Total	Theory	Practical/ Seminar	Total	External Marks	Internal Marks	Practical/ Seminar Marks	
1	21PGDCSL201	Information Security	CL/BL	CC	4	--	4	4	--	4	80	20	--	100
2	21PGDCSL202	Web Application Security	CL/BL	CC	4	--	4	4	--	4	80	20	--	100
3	21PGDCSL203	Cloud Security	CL/BL	CC	4	--	4	4	--	4	80	20	--	100
4	21PGDCSL204	Internet of Things Security	CL/BL	CC	4	--	4	4	--	4	80	20	--	100
5	21PGDCSL205	Cyber Law and Forensics	CL/BL	CC	4	--	4	4	--	4	80	20	--	100
6	21PGDCSL206	Lab-III (Based on 20PGDCSL201)	CL	SEC	--	2	2	--	4	4	--	20	80	100
7	21PGDCSL207	Lab-IV (Based on 20PGDCSL204)	CL	SEC	--	2	2	--	4	4	--	20	80	100
8	21PGDCSL208	Minor Project	GSL	SEC	--	2	2	--	2	2	--	20	80	100
9	21CS100	Communication Skills	BL	AEC	--	1	1	--	2	2	--	50	--	50
	Total				--	--	27	--	--	32	--	--	--	850

CC - Core Course; **SEC-Skill Enhancement Course;** **AEC- Ability Enhancement Course;**

PGDCSL
Semester-I

21PGDCSL101
Fundamentals of Computer Security

Maximum Marks-100
External Examination-80
Internal Assessment-20
Max. Time- 3 hrs.

Objective: This course will lay the foundation for creating comprehensive understanding of cyber security. This paper will set the level field for all the students to be able to come at par and move together as they must go deeper into hard-core cyber security topics during the course duration.

Note: There shall be nine questions in all. Question no. 1 shall be compulsory, consisting of eight short answer type questions covering the entire syllabus. Two questions will be asked from each unit. Student will have to attempt one question from each unit. Each question shall carry equal marks.

Unit-I

Introduction to Computers, History of Computers, Software and Hardware, Classification, Computer Input-Output Devices, Windows, DOS Prompt Commands, Linux/Mac Terminal and Commands, Basic Computer Terminology, Computer Security models, Computer Security Terms, Computer Ethics, Business and Professional Ethics, Need for cyber security; Cyber Frauds and crimes, Digital Payments, Various Search Engines, Introduction to Auditing, Deep Web, VAPT.

Unit-II

Python Scripting and PHP Basics Python Basics, Variables and Types, Lists, Basic Operators, String Formatting, Basic String Operations, Conditions, Loops, Functions, Classes and Objects, Dictionaries, Modules and Packages.

Unit-III

Cyber Laws Need for Cyber Regulations; Scope and Significance of Cyber laws: Information Technology Act 2000; Network and Network Security, Access and Unauthorised Access, Data Security, E Contracts and E Forms. Penal Provisions for Phishing, Spam, Virus, Worms, Malware, Hacking, Trespass and Stalking; Human rights in cyberspace, International Co-operation in investigating cybercrimes.

Unit-IV

Encoding Encoding: Charset, ASCII, UNICODE, URL Encoding, Base64, Illustration: ISBN/ QR Code/ Barcode, Binary hamming codes.Web Application Architecture HTML Basics, XAMPP Server Setup, Hosting Websites Linux, Apache, Virtualisation, Server Configurations, Web Application Firewalls.

Course Outcomes:

After completion of course, students would be able to understand:

- Fundamentals of Cyber Security
- Python Scripting and python programming
- Cyber Laws and Regulations
- Various types of Encoding

Suggested Readings:

1. Langtangen, H.P. (2012). Python Scripting for Computational Science (4th Ed.). Springer
2. Behrouz A. Forouzan (2004). Data communication and Networking. Tata McGraw-Hill.
3. Kurose, James F. & Ross, Keith W. (2003). Computer Networking: A Top-Down Approach Featuring the Internet (3rd Ed.). Pearson Education.
4. Shklar, L. & Rosen, R. (2009). Web Application Architecture: Principles, Protocols and Practices (2nd Ed.). John Wiley & Sons.
5. Craig, B. (2012). Cyber Law: The Law of the Internet and Information Technology. Pearson.
6. Sharma J. P. & Kanojia S. (2016). Cyber Laws. New Delhi: Ane Books Pvt Ltd.

PGDCSL

Semester-I

21PGDCSL102
Network Basics

Maximum Marks-100
External Examination-80
Internal Assessment-20
Max. Time- 3 hrs.

Objective: This course aims at teaching students about the fundamentals of network building. The course aims at acquainting students with the techniques used by hackers for network attacks.

Note: There shall be nine questions in all. Question no. 1 shall be compulsory, consisting of eight short answer type questions covering the entire syllabus. Two questions will be asked from each unit. Student will have to attempt one question from each unit. Each question shall carry equal marks.

Unit-I

Types of networks, IP Address, NAT, IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP IP Model, Routers, Switches, Endpoint solutions, Access Directory, TOR Network. Networking Devices.

Unit-II

Different types of network layer attacks–Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trails) – IDS, IPS and its types. Wireless LANs and PANs –IEEE 802.11 Standard – Architecture –Services –Network –HiperLAN –BlueTooth-Wi-Fi –WiMAX.

Unit-III

Mobile TCP–WAP –Architecture –WWW Programming Model–WDP –WTLS –WTP –WSP –WAE –WTA Architecture –WML –WMLScripts, WAP.
Mobile IP –DHCP –AdHoc–Proactive and Reactive Routing Protocols –Multicast Routing

Unit-IV

Network Sniffing, Wireshark, packet analysis, display and capture filters, DNS and ARP Poisoning, Denial of services, Vulnerability scanning, Nessus, Network Policies, SSL Striping, Setup network IDS/IPS, Router attacks. Types of authentication, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP, WPA and WPA-2 Encryption.

Course Outcomes:
After completion of course, students would be able to understand:

- Types of Networks and their basic structures
- Different types of Network layers attacks

- Architecture of TCP, WAP, WML

Suggested Readings:

1. Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network Security, Private communication in public world* (2nd Ed.). PHI
2. Monte, M. (2015). *Network Attacks and Exploitation: A Framework*. Wiley.
3. Perez, Andre. (2014). *Network Security*. Wiley.
4. Stallings, W. (2006). Cryptography and Network Security: Principles and Practice (5th Ed.). Prentice Hall

PGDCSL

Semester-I

21PGDCSL103
Fundamental of Web Designing

Maximum Marks-100
External Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Objectives of the course: This course aims to impart the basic knowledge of Web designing and web programming. It also acquaints the students the fundamental concepts of client side and server side programming.

Note: There shall be nine questions in all. Question no. 1 shall be compulsory, consisting of eight short answer type questions covering the entire syllabus. Two questions will be asked from each unit. Student will have to attempt one question from each unit. Each question shall carry equal marks.

UNIT-I

Introduction to HTML, XHTML, DHTML, XML – HTML Vs XML – Creating XML documents – Parsing an XML document: Writing well-formed documents, Declaring elements and attributes in a DTD. Overview of HTML - basic formatting tags - heading, paragraph, underline break, bold, italic, underline, superscript, subscript, font and image. Attributes - align, color, bgcolor, font face, border, size. Navigation Links using anchor tag - internal, external, mail and image links. Lists - ordered, unordered and definition. Table tag. HTML Form controls - form, text, password, text area, button, checkbox, radio button, select box, hidden controls.

Unit II

Cascading Style Sheets: Introduction, Inline, Internal, External CSS, Linking CSS to Web Page. Client–Side Programming: Introduction to JavaScript, Basic Syntax, Variables and Data types, Statements, Operators, Literals, Functions, Objects, Arrays. XML: Relation between XML and HTML, Goals of XML, Structure and Syntax of XML, Well Formed XML, DTD and its Structure.

Unit III

Web Application and Information Gathering: HTTP Request, Response, Header Fields and HTTPS, Understanding Same Origin, Sessions, Web Application Proxies. Web server – role - Apache Web Server – Introduction – Architecture – Features - Apache's Role in the Internet – LAMP – WAMP - Installation and Configuration - Build and Install Apache Web Server - Verify Initial Configuration Start, Stop, and Status the Apache Server Process.

UNIT-IV

Server side programming – server side scripts – PHP – Designing dynamic web pages using PHP - Defining PHP variables – variable types – operators – control flow constructs in PHP – passing form data between pages - Establishing connection with MySQL database – managing database

Course Outcomes:

After completion of course, students would be able to understand:

- Concepts of web designing using HTML and CSS
- Configure Apache server and connecting web application to the Database.
- Server and client side scripting

Suggested Readings:

1. Dick Olive. *Tech Yourself HTML 4 in 24 Hours*. Techmedia.
2. Satish Jain. *"O" – Level Information Technology*.
3. Achyut Godbole. *Web Technologies*, Tata McGraw Hill, India.
4. Craig Zacker. *10 minutes Guide to HTML Style Sheets*, PHI.

PGDCSL
Semester-I

21PGDCSL104
Cryptography

Maximum Marks-100
External Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Objective: The paper starts with fundamentals of cryptography and working of cryptography algorithms and their implementation in the real world scenarios. Further, the paper enables the students to use cryptography in the most extensive and elaborate manner.

Note: There shall be nine questions in all. Question no. 1 shall be compulsory, consisting of eight short answer type questions covering the entire syllabus. Two questions will be asked from each unit. Student will have to attempt one question from each unit. Each question shall carry equal marks.

Unit-I

Ceaser Cipher, Vegnere Cipher, Rail-fence Cipher, Row Transposition Cipher.
Requirement and Basic Properties, Main Challenges, Confidentiality, Integrity, Availability, Non-Repudiation,

Unit-II

Data Encryption Standard-Symmetric Ciphers (Stream Cipher &Block cipher) Advanced Encryption Standard (AES)-Triple DES-Blowfish, RC4, RC5/RC6 family.

Unit-III

Principles of public key cryptosystems-The RSA algorithm, Diffie Hellman Key exchange, Elgamal Algorithm, Polynomial Arithmetic, Elliptic curve arithmetic-Elliptic curve cryptography, cryptanalysis.
Bitcoin introduction, working, blockchain crucial to bitcoin, block chain operation with bitcoins, bitcoin glossary, bitcoin wallets, setup for bitcoin payments, bitcoin mining.

Unit-IV

Message authentication code Authentication functions, Hash Functions-Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital signature Standard). Digital Certificate and Public Key Infrastructure.

Course Outcomes:
After completion of course, students would be able to understand:

- Understand basics of Cryptography
- Concepts of Public key and private key cryptosystems
- Message authentication process and digital signature

Suggested Readings:

1. Delfs, H. & Knebl, H. (2001). *Introduction to Cryptography: Principles and Applications*. Springer-Verlag Berlin and Heidelberg GmbH & Co.
2. Stallings, W. (2010). *Cryptography and network security: Principles and practice* (5th ed.) Boston: Prentice Hall.
3. Menezes, A.J., Oorschot, P. Van & Vanstone, S.A. (1997). *The Handbook of Applied Cryptography*. CRC Press.
4. Schneier, B. (1995). *Applied cryptography, Protocols, algorithms and source code in C* (2nd ed.). New York: John Wiley & Sons.

PGDCSL
Semester-I

21PGDCSL105
Cloud Fundamentals

Maximum Marks-100
External Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Objective: The purpose of the paper is to make students understand concept of CLOUD in the cyber world with a view to enable them to achieve cloud security. It also develops cloud architecture as well as the security concerns for organization implementing Cloud architecture.

Note: There shall be nine questions in all. Question no. 1 shall be compulsory, consisting of eight short answer type questions covering the entire syllabus. Two questions will be asked from each unit. Student will have to attempt one question from each unit. Each question shall carry equal marks.

Unit-I

Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vsprivate clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture. Application availability, performance, security and disaster recovery; next generation Cloud Applications.

Unit-II

Technologies and the processes required when deploying web services; Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages. Cloud delivery model - SPI framework, SPI evolution, SPI vs. tradition al IT Model,

Unit-III

Collaborating on Calendars, Schedules and Task Management – Collaborating on Event Management, Contact Management, Project Management.
Reliability, availability and security of services deployed from the cloud.
Performance and scalability of services, tools and technologies used to manage cloud services deployment;

Unit-IV

Cloud Economics: Cloud Computing infrastructures available for implementing cloud based services. Economics of choosing a Cloud platform for an organization, based on application requirements, economic constraints and business needs. Discuss industry cases including open sources.

Course Outcomes:

After completion of course, students would be able to understand:

- Understand the concepts of cloud computing
- Technologies involved in Cloud computing
- Cloud computing infrastructures.

Suggested Readings:

1. Rittinghouse, J.W. & Ransome, J.F. (2010). *Cloud Computing: Implementation, Management, and Security*. CRC Press.
2. Rountree, D. & Castrillo, I. (2013). *The Basics of Cloud Computing: Understanding The Fundamentals of Cloud Computing In Theory And Practice*. Syngress, Elsevier
3. Stallings (2016). *Cryptography & Network Security*. Paperback.
4. Vacca, J. (2016). *Cloud Computing Security: Foundations and Challenges*. CRC Press

PGDCSL
Semester-I

21PGDCSL106
Lab-I (Based on 21PGDCSL102)

Maximum Marks-100
External Practical Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Note: Every student shall individually prepare a practical file consisting of 10 practical related to Network basics. A panel consisting of two teachers (internal and External) should take the practical examination after the end of the semester. Marks are distributed as under:

Practical Record: 10 Marks

Viva-voce: 40 Marks

Written exam/executing the practical on the PC: 30 Marks

PGDCSL
Semester-I

20PGDCSL107
Lab-II (Based on 21PGDCSL103)

Maximum Marks-100
External Practical Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Note: Every student shall individually prepare a practical file consisting of 10 practical related to Fundamental of Web Designing. A panel consisting of two teachers (internal and External) should take the practical examination after the end of the semester. Marks are distributed as under:

Practical Record: 10 Marks

Viva-voce: 40 Marks

Written exam/executing the practical on the PC: 30 Marks

PGDCSL
Semester-I

21PGDCSL108
Seminar

Maximum Marks-25
Internal Assessment-25

Note: Each student shall individually prepare and submit a seminar report within stipulated time. Students have to present their topic through PPTs. A panel consisting of two teachers (internal and External) should evaluate the seminar report and the presentation. Marks should be distributed considering report writing, presentation, technical content, depth of knowledge, brevity and references and their participation in seminar. The time allotted for presentation is 15 minutes.

PGDCSL
Semester-II

21PGDCSL201
Information Security

Maximum Marks-100
External Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Objective: This course aims to provide technical knowledge about the Information security concepts.

Note*: There shall be nine questions in all. Question no. 1 shall be compulsory, consisting of eight short answer type questions covering the entire syllabus. Two questions will be asked from each unit. Student will have to attempt one question from each unit. Each question shall carry equal marks.*

Unit-I

Introduction to Information Security Management System: Critical Appraisal of ISO 9000, Normative, regulatory and legal framework related to information security Fundamental principles of information security, ISO/IEC 27001 certification process, Information Security Management System (ISMS).

Unit-II

ISO/IEC 27001 audit: Fundamental audit concepts and principles, Audit approach based on evidence and on risk, Preparation of an ISO/IEC 27001 certification audit, ISMS documentation audit, Conducting an opening meeting.

Unit-III

Intellectual Property Rights: Types and Issues related to IPR, Policy framework in India and Abroad, Bitcoin and law enforcement.
Security Management Process, Risk Analysis Risk Management, Information System Activity Review, Assigned Security Responsibility, Authorization and/or Supervision, Termination Procedures, Access Authorization, Access Establishment and Modification, Protection from Malicious Software.

Unit-IV

Log-in Monitoring, Password Management, Response and Reporting, Contingency Plan Evaluation, Facility Access Control and Validation Procedures, Unique User Identification, Emergency Access Procedure, Automatic Logoff Encryption and Decryption, Audit Controls, Data Integrity, Person or Entity Authentication, Integrity Controls Encryption.

Course Outcomes:

After completion of course, students would be able to understand:

- Information Security management techniques
- Audit concepts and principles
- Intellectual Property Rights and their issues
- Authentication methods

Suggested Readings:

1. Godbole, N. *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*. Wiley
2. Calder, A. (2009*). Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide* (2nd Ed.). Van Haren Publishing
3. Humphreys, E. (2007). *Implementing the ISO / IEC 27001 Information Security Management System Standard*. Artech House Publishers.
4. Watkins, S. G. (2013). *An Introduction to Information Security and ISO 27001: A Pocket Guide*. IT Governance Publishing.

PGDCSL
Semester-II

21PGDCSL202
Web Application Security

Maximum Marks-100
External Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Objective: The paper cope with the essentials of building secure software applications with focus on real loopholes while coding and removing real world possible attacks on applications.

Note*: There shall be nine questions in all. Question no. 1 shall be compulsory, consisting of eight short answer type questions covering the entire syllabus. Two questions will be asked from each unit. Student will have to attempt one question from each unit. Each question shall carry equal marks.*

Unit-I

Web Designing and Penetration Testing Process: Scope Understanding, Liabilities and Responsibilities, Allowed Techniques, Deliverables, OWASP Top 10 Attack Testing Guidelines, Reporting- Executive Summary, Risk Exposure over time, Successfully Attacks by whom, Vulnerability causes, Vulnerability report, Remediation report, Report Design Guidelines, Malware Analysis.

Unit-II

Web Application and Information Gathering: HTTP Request, Response, Header Fields and HTTPS, Understanding Same Origin, Cookies, Sessions, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration, fingerprinting frameworks, hidden resource enumeration, security misconfigurations, google hacking database, Shodan HQ.

Unit-III

SQL Injections: SQL Statements, Finding SQL Injections, Exploiting SQL Injections, Bypass Authentication, Xpath Injection, Error Based Injection, Double Query Injection, Time Based injections, Union Based Injections, SQL Map, Mitigation plans, SQLi to Server Rooting, Advance MY-SQL and MS-SQL Exploitation. Cross Site Scripting: Anatomy of an XSS Exploitation, Reflected XSS, Persistent XSS, DOM based XSS, Browsers and XSS, Cookie Stealing, Defacements, Advanced Phishing attacks, BeEF Framework, Mitigation.

Unit-IV

Single factor and two factor authentication, dictionary and brute force attacks, storing hashes, blocking malicious request, user enumeration, random password guessing, remember me functionality, no limit attempts, password reset feature, logout flaws, CAPTCHA, insecure direct object reference and security, missing function level access control, unvalidated redirects and forwards, Session ID, LFI and RFI ,Session Attacks via packet sniffing or accessing via web server and Fixation, CSRF (Cross Site Request Forgery), Pentesting Flash -based applications, Cross Windows Messaging, Web Storage, Web Sockets, Sandbox, Path Traversal, Arbitrary file uploading, Clickjacking, HTTP Response Splitting, Business Logic Flaws, denial of services attacks.

Course Outcomes:

After completion of course, students would be able to understand:

- Web Designing and Penetration testing process
- Web application and Information Gathering
- Various SQL injection attacks

Suggested Readings:

1. Shema, M. & Adam. (2010). *Seven deadliest web application attacks*. Amsterdam: Syngress Media.
2. Stuttard, D. & Pinto, M. (2011). *The web application hacker's handbook: Discovering and exploiting security flaws* (2nd ed). Indianapolis, IN: Wiley, John & Sons.
3. Heiderich, M., Nava E.A.V., Heyes, G., & Lindsay, D. (2011). *Web application obfuscation*. Amsterdam: Syngress Media,U.S.
4. Sullivan, Bryan (2012). *Web Application Security, A Beginner's Guide*. McGraw- Hill Education.

PGDCSL
Semester-II

21PGDCSL203
Cloud Security

Maximum Marks-100
External Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Objective: The purpose of the paper is to make students understand the concept of Cloud Security in the cyber world. It also raises security concerns for organizations planning to move towards Cloud architecture and planning to enhance their cloud security.

Note*: There shall be nine questions in all. Question no. 1 shall be compulsory, consisting of eight short answer type questions covering the entire syllabus. Two questions will be asked from each unit. Student will have to attempt one question from each unit. Each question shall carry equal marks.*

Unit-I

Cloud Application Development: Service creation environments to develop cloud based applications. Development environments for service development; Amazon, Azure, Google App. Applicability of laws to data stored outside the nation's boundary.

Unit-II

Cloud IT Model: Analysis of Cases while deciding to adopt secure cloud computing architecture. Appropriate cloud requirements. Secure Cloud based service, Applications and development platform deployment so as to improve the total cost of ownership (TCO).

Unit-III

Virtualization: Need for Virtualization – Pros and cons of Virtualization – Types of Virtualization – System Vm, Process VM, Virtual Machine monitor – Virtual machine properties - Interpretation and binary translation, HLLVM - Hypervisors – Xen, KVM, VMWare, Virtual Box, Hyper-V.

Unit-IV

Security in Clouds: Cloud security challenges – Software as a Service Security, Common Standards: The Open Cloud Consortium – The Distributed Management Task Force – Standards for application Developers – Standards for Messaging – Standards for Security, End user access to cloud computing, Mobile Internet devices and the cloud.

Course Outcomes:
After completion of course, students would be able to understand:

- Cloud IT Model
- Cloud Application development
- Methods for Cloud Security

Suggested Readings:

1. Rittinghouse, J.W. & Ransome, J.F. (2010). *Cloud Computing: Implementation, Management, and Security*. CRC Press.
2. Rountree, D. & Castrillo, I. (2013). *The Basics Of Cloud Computing: Understanding The Fundamentals Of Cloud Computing In Theory And Practice*. Syngress, Elsevier
3. Stallings (2016). *Cryptography & Network Security*. Paperback.
4. Vacca, J. (2016). *Cloud Computing Security: Foundations and Challenges*. CRC Press

PGDCSL
Semester-II

21PGDCSL204
Internet of Things Security

Maximum Marks-100
External Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Objective: The paper will concern with concepts of Internet of Things and their devices with their security concerns along with potential hacks that can be performed on such devices and to ensure its security according to best global practices.

Note: ***There shall be nine questions in all. Question no. 1 shall be compulsory, consisting of eight short answer type questions covering the entire syllabus. Two questions will be asked from each unit. Student will have to attempt one question from each unit. Each question shall carry equal marks.***

Unit-I

Requirement and Basic Properties in Internet of Things, Primary challenges in security maintenance, Confidentiality, Integrity, Availability, Non-Repudiation.

Unit-II

Architecture of Internet of Things: Device - device, Device - Cloud, Device - Gateway, Gateway - Cloud, Cloud – Backend – Applications.
Security Classification and Access Control: Data classification (Public and Private), Internet of Things Authentication and Authorization, Internet of Things Data Integrity.

Unit-III

Attacks and Implementation of Internet of Things: Denial of Service, Sniffing, Phishing, DNS Hijacking, Pharming, Defacement, Firmware of the device, Web Application Dashboard, Mobile Application Used to Control, Configure and Monitor the Devices

Unit-IV

Security Protocols and Management: Firmware of the device, Web Application Dashboard, Mobile Application Used to Control, Configure and Monitor the Devices, Identity and Access Management, Key Management.

Course Outcomes:
After completion of course, students would be able to understand:

- Requirement of IOT Security
- Architecture of Internet of Things
- Various attacks on IOT
- Security mechanisms for IOT

Suggested Readings:

1. Russell, B. (2016). *Practical Internet of Things Security*. Packt Publishing Limited
2. FeiHu (2016). *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations*. CRC Press
3. Hersent, O., Boswarthick, D., & Elloumi, O. (2015). The Internet of Things: Key Applications and Protocols. Wiley
4. Pfister, C. (2011). *Getting Started with the Internet of Things*. Shroff Publisher.

PGDCSL

Semester-II

21PGDCSL205

Cyber Law and Forensic

Maximum Marks-100
External Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Objective: This paper aims to create the basic understanding of cybercrimes and cyber security laws to the professionals learning the ethical hacking programme. It will also emphasise on the activities leading to infringement of individual or organisational privacy.

Note*: There shall be nine questions in all. Question no. 1 shall be compulsory, consisting of eight short answer type questions covering the entire syllabus. Two questions will be asked from each unit. Student will have to attempt one question from each unit. Each question shall carry equal marks.*

Unit-I

Introduction to Cyberspace, Cybercrime and Cyber Law: The World Wide Web, Web Centric Business, E Business Architecture, Models of E Business, E Commerce, Threats to virtual world. Cyber Crimes& social media, Cyber Squatting, Cyber Espionage, Cyber Warfare, Cyber Terrorism, Cyber Defamation. Online Safety for women and children, Misuse of individual information. Objectives, Applicability, Non applicability and Definitions of the Information Technology Act, 2000.

Unit-II

Regulatory Framework of Information and Technology Act 2000: Digital Signature, E Signature, Electronic Records, Electronic Evidence and Electronic Governance. Controller, Certifying Authority and Cyber Appellate Tribunal. Offences and Penalties: Offences under the Information and Technology Act 2000, 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-III

Fundamentals of Cyber Forensics: Cyber Forensic Basics- Introduction to Cyber Forensics, Storage Fundamentals, File System Concepts, Data Recovery, Operating System Software and Basic Terminology Data and Evidence Recovery; Data Recovery Tools, Data Recovery Procedures and Ethics Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility, Document a Chain of Custody and its importance, Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Data Protection and Privacy,

Unit IV

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.

Course Outcomes:

After completion of course, students would be able to understand:

- Cyberspace, Cybercrime and Cyber Law
- Regulatory Framework of IT Act 2000 and its associated rules
- Fundamentals of Cyber Forensics

Suggested readings:

1. Craig, B. *Cyber Law: The Law of the Internet and Information Technology*. Pearson Education
2. Paintal, D. *Law of Information Technology*. New Delhi: Taxmann Publications Pvt. Ltd.
3. Lindsay, D. (2007). *International domain name law: ICANN and the UDRP*. Oxford: Hart Publishing.
4. Sharma J. P, & Kanojia S. (2016). *Cyber Laws*. New Delhi: Ane Books Pvt. Ltd.
5. Duggal, P. *Cyber Laws*. (2016) Universal Law Publishing.
6. Kamath, N. (2004). *Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with rules, regulations and notifications (2nd ed.)*. Delhi: Universal Law Publishing Co.
7. Stephenson, P.R. & Gilbert, K. *Investigating computer- related crime a handbook for corporate investigators*. Boca Raton, FL: Taylor & Francis.
8. Prosise, C. & Mandia, K. (2003). Incident response & computer forensics (2nd ed.). New York, NY: McGraw-Hill Companies.

PGDCSL
Semester-II

21PGDCSL206
Lab-III (Based on 21PGDCSL201)

Maximum Marks-100
External Practical Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Note: Every student shall individually prepare a practical file consisting of 10 practical related to Information Security. A panel consisting of two teachers (internal and External) should take the practical examination after the end of the semester. Marks are distributed as under:

Practical Record: 10 Marks

Viva-voce: 40 Marks

Written exam/executing the practical on the PC: 30 Marks

PGDCSL
Semester-II

21PGDCSL207
Lab-IV (Based on 21PGDCSL204)

Maximum Marks-100
External Practical Examination-80
Internal Assessment-20
Max. Time- 3 hrs

Note: Every student shall individually prepare a practical file consisting of 10 practical related to Internet of Things Security. A panel consisting of two teachers (internal and External) should take the practical examination after the end of the semester. Marks are distributed as under:

Practical Record: 10 Marks

Viva-voce: 40 Marks

Written exam/executing the practical on the PC: 30 Marks

PGDCSL
Semester-II

21PGDCSL208
Minor Project

Maximum Marks-100
External Practical Examination-80
Internal Assessment-20

Note: At the beginning of the semester, the whole class will be divided into Groups. Each group will be assigned one mentor. In a group, every student shall individually prepare and submit a Minor project report at the end of the semester. A panel consisting of two teachers (internal and External) should evaluate the project report and the presentation. Marks should be distributed considering report writing, presentation, technical content, depth of knowledge, brevity and references, uniqueness and practical applications of the topic in current scenario. The time allotted for presentation is 15 minutes.

PGDCSL

Semester-II

21CS100

Communication Skills

Maximum Marks-50
Internal Assessment-50
Max. Time- 2 hrs

Objective of the course: To introduce the theory and practice of communicative skills so as to enable the students to communicate effectively and conduct themselves graciously in the business of life.

Note: One hour of classroom teaching will be devoted to the teaching of theory. In another hour, the students will be engaged in practical activities and the evaluation of their communication skills will be done by the internal examiner on the basis of classroom presentations, discussions and assignments.

Unit-I

Human Communication, Verbal and Non Verbal Communication, Barriers to communication; the seven C's of effective communication. Preparing for interviews, CV/ Bio-data, Group Discussion, Public Speaking, Mass Communication.

Unit -II

Common Courtesies, Introducing Oneself Formally and Informally; Introducing Oneself on Social Media; Speaking Strategies: Making Enquiries, Clarifications, Recommendations, Explanations, Rejections, etc.; Being Diplomatic; Telephonic Communication.

Unit-III

Conversational Practice in Various Situations:

(meeting, parting, asking/talking about daily activities, at railway station, seeking information, buying at shops, asking about buses, travelling by bus, using expressions of time, talking about money, identifying people, at the post office, at the bank, at the grocery store, immediate family and relatives, hiring a taxi, talking about weather/weather conditions, breakfast or lunch at a restaurant, ordering food, dinner conversations, at the doctors clinic, quitting and finding jobs, office conversations, conversations about school/ college/ university, the English class, driving a car).

Students shall develop dialogue-based conversations on the above-mentioned situations.

Unit-IV

Personality Development Skills: Personal Grooming; Assertiveness; Improving Self-Esteem; Significance of Critical Thinking; Confidence Building; SWOC analysis.

Emotional intelligence: Recognizing and Managing Emotions and Situations; Stress and Anger Management; Positive Thinking; Developing Sense of Humour.

Course Outcomes:

After completion of course, students would be able to understand:

- Modes of Communication including Verbal and Non-verbal communication
- To express effectively & with maximum efficiency.
- To develop Interpersonal skills

Suggested Readings:

1. Kumar, Sanjay and PushpLata. English for Effective Communication. OUP, 2016.
2. Mohan, Krishna and Meera Banerji. Developing Communication Skills 2nd ed. Trinity Press,2013
3. Dutt, P. Kirammai and GeethaRajeevan et. At. A Course in Communication Skills. Foundation Books, CUP, 2016.