HINDUSTAN
INSTITUTE OF TECHNOLOGY & SCIENCE
(DEEMED TO BE UNIVERSITY)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CURRICULUM

Under CBCS

(Applicable for Students admitted from Academic Year 2018-19)

B. Tech. Computer Science Engineering
With Specialization in Cyber Security and Forensics
(In Collaboration with IBM)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING SCIENCES

HINDUSTAN INSTITUTE OF TECHNOLOGY & SCIENCE
VISION AND MISSION

MOTTO

"To Make Every Man A Success And No Man A Failure"

VISION

To be an International Institute of Excellence, providing a conducive environment for education with a strong emphasis on innovation, quality, research and strategic partnership blended with values and commitment to society.

MISSION

- To create an ecosystem for learning and world class research.
- To nurture a sense of creativity and innovation.
- To instill highest ethical standards and values with a sense of professionalism.
- To take up activities for the development of Society.
- To develop national and international collaboration and strategic partnership with industry and institutes of excellence.
- To enable graduates to become future leaders and innovators.

VALUE STATEMENT

- Integrity, Innovation, Internationalization

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING
VISION AND MISSION

VISION

To excel in Computer Science and Engineering education, research and project management by empowering the students with strong conceptual knowledge.

MISSION

M1: To educate the students with basic foundation blocks of core and allied disciplines of Computer Science and Engineering.

M2: To provide practical skills in the advancements of the Computer Science and Engineering field required for the growing dynamic IT and ITES industries.

M3: To sculpt strong personal, technical, research, entrepreneurial, and leadership skills.

M4: To inculcate knowledge in lifelong learning, professional ethics and contribution to the society.

B. Tech. Computer Science and Engineering

PROGRAMME EDUCATIONAL OBJECTIVES (PEO)

The Program Educational Objectives (**PEOs**) of the **Computer Science and Engineering** are listed below:

The graduate after 3-5 years of programme completion will

PEO1: Excel in his/her professional career and/or pursue higher education including research by applying the knowledge of Computer Science and Engineering.

PEO2: Demonstrate the technical skills to analyze and design appropriate solutions for problems with social consciousness and ethical values.

PEO3: Adapt themselves to organizational needs by understanding the dynamically changing technologies.

PROGRAM OUTCOMES (ALIGNED WITH GRADUATE ATTRIBUTES) (PO)

(To be achieved by the student after every semester/year/and at the time of graduation)

At the end of this program, graduates will be able to

PO1: **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2: **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3: **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4: **Conduct investigations of complex problems:**Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5: **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6: **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7: **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8: **Ethics:**Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9: **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10: **Communication:**Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11: **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12: **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES (PSO)

On completion of the B.Tech. Computer Science & Engineering degree the graduates will be able to

PSO1: Apply mathematical, conceptual knowledge of computing and analytical skills to solve complex problems.

PSO2: Design and develop computer systems based on the domains of Cyber Physical Systems, Algorithm Design Techniques and Enterprise systems security.

PSO3: Do innovative system design with analytical knowledge by developing modern tools and techniques.

HINDUSTAN
INSTITUTE OF TECHNOLOGY & SCIENCE
(DEEMED TO BE UNIVERSITY)

SCHOOL OF COMPUTING SCIENCES

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CURRICULUM AND SYLLABUS – R2018

B.TECH – COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN – CYBER SECURITY AND FORENSICS (IN COLLABORATION WITH IBM)									
(176 CREDIT STRUCTURE)									
SEMESTER – I									
SL. NO	**COURSE CATEGORY**	**COURSE CODE**	**NAME OF THE COURSE**	**L**	**T**	**P**	**C**	**S**	**TCH**
1	HS/ES	ELA4101/ MEA4101	Professional English and Soft Skills /Engineering Graphics and Computer Aided Design	1	1	2	3	1	4
2	BS	MAA4101	Matrices and Calculus	3	0	2	4	0	5
3	BS	PHA4102/CYA4101	Engineering Physics/Engineering Materials	3	0	0	3	1	3
4	PC	CSA4101	Problem Solving Using C	2	0	2	3	1	4
5	ES	EEB4101 /CSB4101	Introduction to Digital Systems / Engineering and Design	3	0	0	3	1	3
6	ES	GEA4131	Engineering Immersion Lab	0	0	2	0.5	2	2
7	BS	PHA4131/CYA4131	Engineering Physics Lab/ Materials Chemistry Lab	0	0	2	1	0	2
Total				12	1	10	**17.5**	6	23
SEMESTER – II									
SL. NO	**COURSE CATEGORY**	**COURSE CODE**	**NAME OF THE COURSE**	**L**	**T**	**P**	**C**	**S**	**TCH**
1	BS	MAA4117	Analytical Mathematics	3	0	2	4	1	5
2	BS	PHA4102/CYA4101	Engineering Physics/ Engineering Materials	3	0	0	3	1	3
3	HS/ES	ELA4101/	Professional English and Soft Skills /Engineering Graphics and Computer	1	1	2	3	1	4

		MEA4101	Aided Design						
4	ES	EEB4101 / CSB4101	Introduction to Digital Systems / Engineering and Design	2	0	2	3	1	4
5	ES	GEA4102	Sustainable Engineering Systems	2	0	0	2	1	3
6	PC	CSB4117	Data Structures using C	3	0	0	3	1	3
7	PC	CSB4118	Object Oriented Programming using C++	3	0	2	4	1	5
8	PC	CSB4146	Data Structures Lab	0	0	3	1	0	3
9	ES	GEA4131	Engineering Immersion Lab	0	0	2	0.5	2	2
10	BS	PHA4131/CYA4131	Engineering Physics Lab/ Materials Chemistry Lab	0	0	2	1	0	2
11	**PC**	**IBC4101**	**Introduction to Open Source Software and Open Standards**	**2**	**0**	**0**	**2**	**0**	**2**
Total				19	1	15	**26.5**	9	36

B.TECH – COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN – CYBER SECURITY AND FORENSICS (IN COLLABORATION WITH IBM)

(176 CREDIT STRUCTURE)

SEMESTER – III

SL. NO	COURSE CATEGORY	COURSE CODE	NAME OF THE COURSE	L	T	P	C	S	TCH
1	BS	MAA4201	Partial Differential Equations and Transforms	3	0	2	4	0	5
2	PC	CSB4201	Design and Analysis of Algorithms	2	1	2	4	1	5
3	PC	CSB4202	Database Management Systems	3	0	0	3	1	3
4	PC	CSB4203	Java Programming	3	0	2	4	0	5
5	**DE**	**IBS4201**	**Information Security Fundamentals**	**2**	**0**	**0**	**2**	**0**	**2**
6	NE	CSD42**	Non-Department Elective- I	2	0	0	2	0	2
7	PC	CSB4231	Python Programming Lab	0	0	3	1	0	3
8	PC	CSB4232	Database Management Systems Lab	0	0	3	1	0	3
Total				15	1	12	**21**	2	28

B.TECH – COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN – CYBER SECURITY AND FORENSICS (IN COLLABORATION WITH IBM)

(176 CREDIT STRUCTURE)									
SEMESTER – IV									
SL. NO	**COURSE CATEGORY**	**COURSE CODE**	**NAME OF THE COURSE**	**L**	**T**	**P**	**C**	**S**	**TCH**
1	BS	MAA4219	Discrete Mathematics	3	1	0	4	0	4
2	PC	CSB4216	Computer Organization and Architecture	3	0	0	3	1	3
3	PC	CSB4217	Computer Networks	3	0	0	3	1	3
4	PC	CSB4218	Operating Systems	3	0	0	3	1	3
5	**DE**	**IBS4216**	**IT Physical And Systems Security**	**3**	**0**	**2**	**4**	**0**	**3**
6	**DE**	**IBS4217**	**IT Data And Application Security**	**3**	**0**	**2**	**4**	**0**	**3**
7	NE	CSD42**	Non-Department Elective–II	2	0	0	2	0	2
8	PC	CSB4241	Networking Lab	0	0	3	1	0	3
9	PC	CSB4242	Operating Systems Lab	0	0	3	1	0	3
10	PC	CSB4243	Design Project-I	0	0	2	1	0	2
11	-	-	Internship	0	0	0	1	0	0
Total				20	1	12	**27**	3	29

B.TECH – COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN – CYBER SECURITY AND FORENSICS (IN COLLABORATION WITH IBM)									
(176 CREDIT STRUCTURE)									
SEMESTER – V									
SL. NO	**COURSE CATEGORY**	**COURSE CODE**	**NAME OF THE COURSE**	**L**	**T**	**P**	**C**	**S**	**TCH**
1	BS	MAA4302	Probability and Statistics	3	0	2	4	0	5
2	**PC**	**IBC4303**	**Web Programming through PHP & HTML**	**3**	**0**	**2**	**4**	**0**	**5**
3	PC	CSB4302	Theory of Computation	3	1	0	4	1	4
4	PC	CSB4303	Artificial Intelligence	3	0	0	3	0	3
5	**DE**	**IBS4301**	**IT Network Security**	**3**	**0**	**2**	**4**	**0**	**3**

6	HS	GEA4216	Professional Ethics and Life Skills	2	0	0	2	1	2
7	NE	CSD43**	Non-Department Elective–III	2	0	0	2	0	2
8	PC	CSB4331	Skill Development in Programming	0	0	2	1	0	2
9	PC	CSB4332	Design Project with IoT	0	0	3	1	0	3
Total				19	1	11	**25**	2	29

B.TECH – COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN – CYBER SECURITY AND FORENSICS (IN COLLABORATION WITH IBM)

(176 CREDIT STRUCTURE)

SEMESTER – VI

SL. NO	COURSE CATEGORY	COURSE CODE	NAME OF THE COURSE	L	T	P	C	S	TCH
1	PC	CSB4316	Principles of Compiler Design	3	1	0	4	1	4
2	PC	CSB4318	Data Warehousing and Data Mining	3	0	0	3	1	3
3	PC	CSB4317	Machine Learning	3	0	2	4	1	5
4	HS	GEA4304	Business Economics	2	0	0	2	1	2
5	**DE**	**IBS4316**	**Digital Forensics**	**3**	**0**	**2**	**4**	**0**	**5**
6	**DE**	**IBS4317**	**Information Technology Security Evaluation Criteria (ITSEC)**	**3**	**0**	**0**	**3**	**0**	**3**
7	NE	CSD43**	Non-Department Elective–IV	2	0	0	2	0	2
8	PC	CSB4341	Compiler Design lab	0	0	3	1	0	3
9	PC	CSB4342	Design Project-II	0	0	2	1	0	2
10	-	-	Internship	0	0	0	1	0	0
Total				19	1	9	**25**	4	29

B.TECH – COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN – CYBER SECURITY

AND FORENSICS (IN COLLABORATION WITH IBM)									
(176 CREDIT STRUCTURE)									
SEMESTER – VII									
SL. NO	**COURSE CATEGORY**	**COURSE CODE**	**NAME OF THE COURSE**	**L**	**T**	**P**	**C**	**S**	**TCH**
1	PC	CSB4401	Software Project Management	3	0	0	3	1	3
2	PC	CSB4402	Big Data and Analytics	3	0	2	4	1	5
3	PC	CSB4403	Applied Cryptography and Network Security	3	1	0	4	1	4
4	PC	CSB4404	Programming Paradigms	3	0	0	3	1	3
5	**DE**	**IBS4401**	**Information Security Audit & Monitoring**	**2**	**0**	**2**	**3**	**0**	**3**
6	**DE**	**IBS4402**	**Information Security Intelligence And Compliance Analytics Using Big Data**	**3**	**0**	**0**	**3**	**0**	**3**
7	DE	CSD44**	Non-Department Elective-V	2	0	0	2	0	2
8	PC	CSB4431	Cloud Deployment Lab	2	0	2	3	0	4
9	PC	CSB4432	Design Project-III	0	0	2	1	0	2
Total				21	1	8	**26**	4	29

B.TECH – COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN – CYBER SECURITY AND FORENSICS (IN COLLABORATION WITH IBM)									
(176 CREDIT STRUCTURE)									
SEMESTER – VIII									
SL. NO	**COURSE CATEGORY**	**COURSE CODE**	**NAME OF THE COURSE**	**L**	**T**	**P**	**C**	**S**	**TCH**
1	PC	CSB4441	Project & Viva – voce	0	0	16	8	0	16
Total				0	0	16	**8**	0	16
Total							**176**		

SYLLABUS

SEMESTER II

IBC4101	INTRODUCTION TO OPEN SOURCE SOFTWARE AND OPEN STANDARDS	L T P C 2 0 0 2
Goal	To provide wide knowledge on Open source and its standards	

OBJECTIVES	OUTCOMES
The course should enable the students to 1. Understand the Open Source Software and Open Standards 2. Learn the adoption of open source standards. 3. Realize the role of open source community. 4. Learn the Adoption of open source. 5. Learn the fundamentals of Linux	The student should be able to 1. Have Gained knowledge of Open Source Software and Open Standards. 2. Learn the Open Source Evolution along with case studies. 3. Have understood the significance of open source. 4. Work with Linux. 5. Contribute to open source community.

UNIT I INTRODUCTION TO STANDARDS AND EVOLUTION 6

Introduction to Standards; Types of Standards; Open Standard, Closed Standard; Summary and examples. Evolution of Standards; Life Cycle; Importance of Standards and Benefits of Open Standards

Standard Organizations, De Jure standard setters - International Organization for Standardization, International Electro Technical Commission, International Telecommunication Union, ASEAN, Bureau of Indian Standards, De Facto Standard Setters -Bluetooth Special Interest group, USB Implementers forum; Testing and certification, Summary. Introduction, Drivers for adoption - Network effects, Lower costs, Impending benefits; Adoption methods and Process - Degree of association, Methods, process; Examples of Open Standards adoption in the world - SCOSTA, Web Standards; Adoption barriers, Early adopters.

UNIT II ADOPTION OF OPEN STANDARDS&CASESTUDIES 6

Introduction; Drivers of Adoption; Adoption Methods and Process; examples of Open Standard Adoptions in the World; Adoption Barriers; Early adopters

Open Standards Case Study 1 - Transfer Account Procedure (TAP), Open Standards Case Study 2 - Open Document Format (ODF) Major Principles of Open Standards - Openness, Consensus, Due Process, Open IPR, Open World, Open Access, Open meetings, Ongoing support, Open interfaces, Open use.

UNIT III INTRODUCTION TO OPEN SOURCE & HISTORY 6

Introduction to Open Source Software - History of Open Source Software, Initiation of Open Source project start; Open Source Software examples: The Origins, The GNU projects, The Operating System GNU/Linux, The Graphical User Interface KDE/GNOME, Apache Web Server, Application Software; Strengths and Advantages of Open Source Software - Network effects, Lower cost, Availability, Maintainability. Drivers for Adoption - Lower cost of ownership, Quality, Innovation reuse, Technical competence; Open Source Software Assessment, Examples of Open Source Adoption in the World, Open Source Challenges.

History, evolution and benefits of Open Source. History of Open Source - Evolution of UNIX, GNU General Public License - Genesis of GNU, Copyleft- All Rights reserved; Benefits of Open Source.

UNIT IV OPEN SOURCE COMMUNITIES AND DEVELOPMENT PROCESS 6

Open Source Initiative (OSI); Open Source definition; Free Software foundation; Open source development process – Call for Contributions, MythBuster, Brook's law; Open Source Community; Apache Web Server; Apache Software Foundation (ASF); How to contribute to Open source projects.

Introduction; Drivers for Open Source adoption; Adoption Methods and Process; examples of Open Standard Adoptions in the World; Open Source Challenges.

UNIT V CASE STUDIES ON OPEN STANDARDS - INTRODUCTION TO LINUX 6

Introduction; Open Standards Case Study 1 - Mozilla, Open Standards Case Study 2 - Linux

The Operating System – an Overview, Linux Basics, Various Linux distributions available, Working with the System, Shells and Utilities, An Introduction to Linux, Booting – Building the Linux kernel image, Overview, booting BIOS POST, Bootsector and setup, Using LILO as a boot loader, High level initialization, SMP bootup on x86, freeing initialization data and code, Processing kernel command line, Run levels, Changing RUNLEVELS, Init scripts, Creating your own init scripts, Stopping the System- Shutdown(reboot, halt), Preparing for Installation – Installation Checklist, Hardware Requirements, Partitioning, Installation problems.

TOTAL: 30

TEXT BOOK

1. Introduction to Open Source Software & Open Standards by IBM ICE Publications.

SEMESTER III

IBS4201	INFORMATION SECURITY FUNDAMENTALS	L	T	P	C
		2	0	0	2
Goal	To learn about the fundamentals of Information security				

OBJECTIVES	OUTCOMES
The course should enable the student to: 1.Understand the 4 Factors of Security. 2.Learn Security Goals. 3. Learn about physical security and network security	The student should be able to: 1.Abide the 4 factors of security 2. Have an overview on cryptography. 3.Know the basic tools of information security

UNIT I THE CIA TRIAD 6

Confidentiality, Integrity & Availability, what is Information Security? Identification and Authentication, Authorization and Access Control, Auditing and Accountability

UNIT II CRYPTOGRAPHY, OPERATIONS SECURITY 6

Modern Cryptography Tools, Protecting Data at rest, In motion, And In Use, Origins Of Operations Security, The Operations Security Process, Laws Of Operations Security, Operations Security in our Personal Lives

UNIT III PHYSICAL SECURITY AND NETWORK SECURITY 6

Introduction, Physical Security Controls, Protecting People, Data and Equipment. Protecting Networks, Protecting Network Traffic. Network Security Tools

UNIT IV OPERATING SYSTEM AND APPLICATION SECURITY 6

Operating System Hardening, Protecting Against Malware, Software Firewalls and Host Intrusion Detection, Operating System Security Tools, Software Development Vulnerabilities, Web Security, Database Security, Application Security Tools.

UNIT V INFORMATION SECURITY - AUDIT AND MONITORING, INTELLIGENCE, COMPLIANCE, MANAGEMENT AND GOVERNANCE. 6

Change and Security Implications, System Models, Targets and Methods, Log Management, Data Aggregation and Reduction, Notifications and Reporting, Monitoring and Control Challenges, Auditing Standards, SAS 70 Audits, Sarbanes-Oxley, Addressing Multiple Regulations for Information Security Technical Frameworks for IT Audits, Intelligence and Compliance, Management and Governance.

TOTAL: 30

TEXT BOOK

1. Information Security Fundamentals by IBM ICE Publications.

SEMESTER IV

IBS4216	IT PHYSICAL & SYSTEMS SECURITY	L	T	P	C
		3	0	2	4
Goal	To impart knowledge on Physical and Systems Security				

OBJECTIVES	OUTCOMES
The course should enable the students to: 1.Learn about the importance of physical security' 2.Provide an insight on security surveys and the Audit 3. Learn about IT security overview and host security.	The student should be able to: 1.Provide physical security to devices. 2.Know the best time to conduct security surveys and the Audit. 3.Have a basic knowledge on vulnerabilities and how to overcome them.

UNIT I PHYSICAL SECURITY OVERVIEW, VULNERABILITY ASSESSMENT 12

Importance of Physical Security, Relationship Between Physical and Cyber Security, Guard Against Disgruntled Employees and Angry Former Employees, How Activists and Corporate Foes Can Hurt You, Vandals Who Damage for Fun, Saboteurs Who Work for Profit, Thieves and Spies Are Everywhere, Domestic Terrorists Are Still a Threat, International Terrorist Are a Growing Threat, Physical Security for Natural Disasters, Security for Random Incidents, Steps to Improve Physical IT Security, Influence of Physical Design - Defensible Space, Crime Prevention Through Environmental Design, Risk Management and the Vulnerability Assessment, Risk Assessment and the Vulnerability Assessment Process, Statistics and Quantitative Analysis, Vulnerability Process Overview, Reporting and Using of Vulnerability Assessment, System Engg and Vulnerability Assessment.

UNIT II SECURITY SURVEYS AND THE AUDIT 12

Overview, the best time to conduct the survey, why conduct a security review, classification of survey recommendations, developing security points, nine points of security concern, personality of the complex, positive and negative aspects of making recommendations, crime analysis, key control, digital closed-circuit television, intrusion alarms, lighting and security, other security aspects, security survey follow-up, residential security, home security checklist, top ten security threats, the audit. Site survey and risk assessment physical security survey - exterior physical characteristics: perimeter grounds Plant security checklist; security officers checklist; office security checklist; home security checklist - exterior, doors, windows, general home security, miscellaneous; fire safety inspection - administrative and planning phase; bullet-resistant glazing for a secure workplace, bullet-resistant fiberglass wall panels, bullet-resistant doors, bullet-resistant windows; Window film

UNIT III APPROACHES TO PHYSICAL, SECURITY LIGHTING, ALARMS—

INTRUSION DETECTION SYSTEMS **12**

Overview, levels of physical security, the value of planning, physical barriers, the security plan Protective & physical barriers - perimeter entrances, barrier planning, fence standards, types of security fences; Doors, roofs, floors, fences, walls and moats, topography; Use of locks in physical crime prevention - lock terminology and components, key-operated mechanisms, combination locks, lock bodies, door lock types, strikes, attacks and countermeasures, locks and the systems approach to security. Safes, vaults, and accessories - choose the right container, ul-rated combination locks, re-locking devices, locking dials, lockable handles, time locks, time-delay combination locks, alarmed combination locks, vision-restricting and shielded dials, combination changing, safe burglaries, hidden combinations, overcoming safe-opening problems, Rating files, safes, and vaults.

Illumination, types of lamps, things needed to know about lighting, energy management, lighting definitions, lighting description; Components of alarm systems, application, alarm equipment overhaul, A smoke detector's; Alarm certificate services - definitions, standards; Fire classifications, use of fire extinguishers

UNIT IV VIDEO TECHNOLOGY OVERVIEW, BIOMETRICS CHARACTERISTICS, ACCESS CONTROL AND BADGES, FENCE STANDARDS, FIRE AND FIRE SAFETY INSPECTION **12**

Video system, camera function, scene illumination, scene characteristics, lenses, cameras, transmission, switchers, quads and multiplexers, monitors, recorders, hard-copy video printers, Ancillary equipment, cctv, Biometrics characteristics; Access control, designated restricted areas, degree of security, considerations, employee screening, identification system, id methods, mechanized/automated systems, card/badge specifications, visitor identification and control, visitors, enforcement measures, sign/countersign and code word, duress code, access control rosters, control methods, security controls of packages, personal property, and vehicles, tactical-environment considerations; Fence standards - recommendations, security planning, material specifications, design features and considerations, typical design example. How Fire Spreads? Four Ways To Put Out A Fire, Classifying Fire, Ul Standard 217, Water Supply For Sprinklers And Tanks. Fire Safety Inspection - Administrative and Planning Phase, General Physical Inspection Phase, Extinguisher Inspection Phase, Stand Pipe, Fire Hose, And Control Valve Inspection Phase, Sprinkler System Inspection Phase, Hazardous Materials Inspection Phase, Alarm System Inspection Phase

UNIT V STANDARDS, REGULATIONS, AND GUIDELINES **12**

Introduction, Standards, Regulations, Guidelines, Managing Compliance, Resources, Number and function of Guards, Uniform, Firearms, Vehicles, guardhouses, communication, rounds, logbooks, Hazard Assessment, command structure, emergency drills & crisis

management Introduction, Network security, Hardware/Downloadable devices/Data storage, Physical security

Software updates to reduces vulnerabilities, Firewall, Account Management - Authentication, One Time passwords, System Threats - Antivirus software, Worms, Trojan horse, Root kits, Port Scanning, Denial of service attack, Distributed Denial of Service attack.

TOTAL: 60

TEXT BOOK

1. IT Physical & Systems Security by IBM ICE Publications.

IBS4217	**IT DATA & APPLICATION SECURITY**	**L**	**T**	**P**	**C**
		3	**0**	**2**	**4**
Goal	To impart thorough knowledge on Data & Application Security				

OBJECTIVES	**OUTCOMES**
The course should enable the students to : 1.Brief the introduction on data security threats and it's techniques. 2. Learn about session management and configuration management	The student should be able to : 1. Work on data security threats and it's techniques 2. Work on DB activity monitoring tools 3. Have an overview of code analysis

UNIT I DATA SECURITY THREATS, DATA SECURITY THREAT TECHNIQUES 12

Introduction, Data breach, Identity Theft, Bank fraudPhysical or Digital theft (Stolen laptops, removable media, impersonation), Malware, SQL Injection, Dumpster diving, Phishing and Pre-Phishing, Denial of Service attack, Social Engineering.

UNIT II COUNTER MEASURES& DATABASE ACTIVITY MONITORING TOOL 12

Introduction, Disk Encryption, Hardware based mechanisms for protecting data, Backups, Data masking, Data Erasure, Database Activity Monitoring using IBM Infosphere Guardium.

UNIT III APPLICATION SECURITY & AUTHENTICATION & AUTHORIZATION 12

Input Validation - Buffer overflow; cross-site scripting; SQL injection; canonicalization, Sensitive information Access sensitive data in storage; network

eavesdropping; data tampering Network eavesdropping; Brute force attack; dictionary attacks; cookie replay; credential theft Elevation of privilege; disclosure of confidential data; data tampering; luring attacks; Phishing.

UNIT IVCONFIGURATION MANAGEMENT & SESSION MANAGEMENT 10

Unauthorized access to administration interfaces; unauthorized access to configuration stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts. Hijacking; session replay; man in the middle.

UNIT V CRYPTOGRAPHY, PARAMETER 14

Cryptography Poor key generation or key management; weak or custom encryption Parameter manipulation; Query string manipulation; form field manipulation; cookie manipulation;

HTTP header manipulation, Exception management Information disclosure; denial of service Auditing and logging, User denies performing an operation; attacker exploits an application withouttrace; attacker covers his or her tracks, Countermeasures Introduction to code analysis using IBM Rational AppScan

TOTAL: 60

TEXT BOOK

1. IT Data security & Application Security (IBM ICE Publication)

SEMESTER V

IBC4303	**WEB PROGRAMMING THROUGH PHP &HTML**	**L** **3**	**T** **0**	**P** **2**	**C** **4**
Goal	The course emphasizes on the basics of web programming through PHP and html.				

OBJECTIVES	**OUTCOMES**
The course should enable the student to 1. Understand PHP Basics. 2. Learn operators, structures and functions in PHP. 3. Learn arrays and PHP file handling 4. Object Oriented programming features of PHP. 5. Learn advanced PHP	The students should be able to 1. Do PHP programming 2. Embed PHP in HTML 3. Have learnt Javascript 4. Have understood advanced concepts in PHP programming.

UNIT I PHP BASICS 9

Introduction to PHP, Support for Database, PHP Installation, Working with PHP, Why PHP?, Basic Syntax of PHP, PHP statement terminator and case insensitivity, Embedding PHP in HTML, Comments, Variables, Assigning value to a variable, Constants, Managing Variables.

UNIT II OPERATORS, CONTROLS STRUCTURES AND FUNCTIONS IN PHP 9

Arithmetic Operators, Bit-wise Operators, Comparison Operators, Logical Operators, Concatenation Operator, Incrementing/Decrementing Operator, Ternary Operator, Operator Precedence, String Manipulation: strtoupper(), strtolower(), ucfirst(), ucwords(), strcmp(), strlen(), substr(), trim(), Conditional Control Structures: If statement, If- else statement, If-else if statement, Nested If, Switch statement, Looping Control Structures: For loop, While loop, Do- While loop, For-each, Loop control: Break and Continue. Functions, User-Defined function, Function Definition, Function Call, Function with arguments, Function with return value, Call by value and call by references, Understanding variable scope, Global Variables, Static Variables, Include and Require, Built-in functions in PHP.

UNIT III ARRAYS AND PHP FILE HANDLING 9

Introduction to Array, Array in PHP, Creating an Array, Accessing Elements of an Array, Modifying Elements of an Array, Finding the Size of an Array, Printing an Array in the readable Way, Iterating Array Elements, Modifying Array while iteration, Iterating Array with Numeric index, Removing Element from an Array, Converting an Array to String, Converting String to an Array, Array Sorting, Multidimensional Array, Accessing elements of a Multidimensional Array,Iterating Multidimensional Array. Introduction, File Open, File Creation, Writing to files, Reading from File, Searching a record from a file, Closing a File, Using PHP With HTML Forms.

UNIT IV CLASS, OBJECT AND EXCEPTION HANDLING, JAVA SCRIPT6

Introduction, Object, Class, Defining Class in PHP, Object in PHP, Usage of $this variable, Constructor, Constructor with Parameters. Introduction to Exception, Exception Handling mechanisms, Creating Custom Exceptions, Multiple Catch Blocks, Exception Propagation, Error Handling in PHP. Java Introduction, JavaScript Basics.

UNIT V INTRODUCTION TO ADVANCE PHP, SET UP PHP DEVELOPMENT ON ECLIPSE CREATING AND DEBUGGING PHP PROJECTS 12

Advanced functions in PHP, Serializing data for persistence, Pattern matching with PHP, Object-oriented Programming and PHP, PHP frameworks - CakePHP, Symfony, & Zend Framework, Manage PEAR modules, Install prebuilt PHP applications, Eclipse installation –

All in one, PDT runtime, installation via Update Manager Eclipse, Installing a debugger, Running the code inside the web server**.**

Install the local Web Server, Install the PHP engine. Create and Run PHP Project, Understanding Debug View, The PHP debug perspective – the Variables view, the breakpoints view, the editor view, the console view, the debug output view, the browser output view; Installing and Configuring the debuggers – Install the Zend debugger, Install XDebug, Configure the debuggers, Setting up PDT (PHP Development Tools) – Set up PHP servers, Set up PHP executables, Debug Web Application, Inserting other languages e.g. SQL, HTML, Java Script in PHP Code. SQL – PHP SQL Script Installing PHP Projects on Web Server

TOTAL: 45

TEXT BOOK

1. Web Programming Thru PHP (IBM ICE Publications)
2. PHP Bible - Tim Converse

REFERENCE BOOKS

1. PHP A beginner's guide - Bill McCarthy
2. PHP and MySQL Web Development - Luke Welling
3. Learning PHP - OReilly Press
4. http://in.php.net/quickref.php
5. http://www.w3schools.com/php/default.asp
6. http://www.tizag.com/php/

Practical Component:

LIST OF EXPERIMENTS

Basics Programming:

1. Branching Statements using number Exercise
2. Looping Statement
3. String Functions
4. String Manipulation
5. Calculator

Practicals using Functions

1. Generate Employee ID
2. Calculate Tax
3. Reverse a string
4. Call by value and Call by reference
5. Find Grade

Practicals using Arrays

1. Sorting
2. Find grade
3. Sort Array
4. Multidimensional Array
5. Population Details

File Handling programs

1. Writing into an existing file
2. Read from a file
3. Filter the contents from the file
4. File Copy

PHP programming thru HTML

1.PHP with HTML

Programs related with PHP Classes and Objects

1. Student Registration
2. Online Examination System
3. Online Feedback System

Exception Handling in PHP

1. User Defined Exception
2. Exception Propagation
3. Error Handling in PHP

Java Scripting

1. Arithmetic Operation
2. Html and java script

IBS4301	**IT NETWORK SECURITY**	**L**	**T**	**P**	**C**
		3	**0**	**2**	**4**
Goal	To learn the basics of IT network security				
OBJECTIVES		**OUTCOMES**			

The course should enable the student to:	The students should be able to:
1. Know the types of topologies, network cabling, OSI layer and the basic protocols. 2. Learn about the physical network types. 3. Learn penetration testing.	1. Apply these protocols in real time projects 2. Gain immense knowledge on networking concepts. 3. Acquire knowledge on penetration testing.

UNIT I SECURING COMMUNICATIONS AND LAN/WAN NETWORKS 12

International Organization for Standardization/Open Systems Interconnection (ISO/OSI) Layers and Characteristics, LANs vs. WANs, Network Cabling, Wireless, LAN Technologies (Ethernet, Token Ring, and FDDI), Network Topologies, Network Protocols, Lan Manager / Microsoft Network / NT Domains, TCP/IP, Weaknesses, Routing Protocols , PPP (Point to Point Protocol), DNS (Domain Name Service), NIS, NIS + (Network Information Service), DHCP (Dynamic Host Configuration Protocol), NFS (Network File System), Apple talk, SNA, IPX/SPX, OSI protocols, X.25, Decnet, Telephone/Fax Network

UNIT II PHYSICAL NETWORK TYPES 12

Ethernet, Leased lines, FDDI, ATM, Hubs, Bridges, Routers, Modems, Gateways, Firewalls, Internet Email Gateway, Permission for external connections, Remote Access Security Management. Network and Protocol Security Mechanisms (VPN, Secure Communications Protocols, E-Mail Security Solutions, Dial-Up Protocols, Authentication Protocols)

UNIT III NETWORK SERVICES 12

Remote Access and Telecommuting Techniques (Frame Relay), Other WAN Technologies (SMDS, X.25, ATM, HSSI, SDLC, HDLC, ISDN), Avoiding Single Points of Failure (Redundant Servers, Failover, RAID)

UNIT IV NETWORK MANAGEMENT / MONITORING 12

IBM Netview, HP Openview, Sun NetManager

UNIT V INTRODUCTION TO PENETRATION TESTING 12

Introductions, types, methods,assessment, tools

TOTAL : 60

TEXT BOOK

1. IT Network Security by IBM ICE Publications

SEMESTER VI

IBS4316	DIGITAL FORENSICS	L	T	P	C
		3	0	2	4
Goal	To impart on Digital Forensics				

OBJECTIVES	OUTCOMES
The course should enable the student to: 1. Have an overview on the basics of Digital forensics 2. Learn about malware analysis	The students should be able to: 1. Understand the importance of digital forensics 2. Understand the different types of digital forensics and work on them.

UNIT I COMPUTER FORENSICS & NETWORK FORENSICS 12

Standard Procedure, Incident Verification, System identification, Recovery of Erased and damaged data, Disk imaging and preservation, Data encryption and compression, Automated search techniques, Forensic software.

Tracking network traffic, Reviewing Network Logs, Tools, Performing Live Acquisitions, Order of volatility, Standard Procedure

UNIT II INTERNET FORENSICS 12

Internet & World wide web threats (Email, Chat-rooms, Search Engines, Hacking & illegal access, Obscene and indecent transmission, Extortion & threats), Domain Name Ownership Investigation, Reconstructing Past Internet Activities and Events, Email Forensics: E-mail Analysis, Email Forensics: Email Headers and Spoofing, Email Forensics: Laws Against Email Crime, Messenger Forensics: AOL, Yahoo, MSN, and Chats, Browser Forensics: Analyzing Cache and Temporary Internet Files, Browser Forensics: Cookie Storage and Analysis

Browser Forensics: Web Browsing Activity Reconstruction.

UNIT III FORENSIC INVESTIGATION AND EVIDENCE 12

Authorization to collect the evidence, Acquisition of evidence, Authentication of the evidence, Analysis of the evidence, Reporting on the findings, Testimony.
Laws & regulations - Information Technology Act, Giving evidence in court

UNIT IV MOBILE FORENSICS, MEMORY FORENSICS & STEGANOGRAPHY 12

Collecting and Analyzing Cell Phone, PDA, Blackberry, iPhone, iPod, iPad,and MP3 Evidence, Analyzing CD, DVD, Tape Drives, USB, Flash Memory, and other Storage Devices, Digital Camera Forensics, Reconstructing Users Activities, Recovering and Reconstructing Deleted Data. Memory Data Collection and Examination, Extracting and Examining Processes. Steganography Tools and Tricks, Data Hiding & Data Recovery.

UNIT V MALWARE ANALYSIS 12

Analyzing Live Windows System for Malware, Analyzing Live Linux System for Malware, Analyzing Physical and Process Memory Dumps for Malware, Discovering and Extracting Malware from Windows Systems, Discovering and Extracting Malware from Linux Systems, Rootkits and Rootkit Detection and Recovery, Reverse Engineering Tools and Techniques

TOTAL : 60

TEXT BOOK
1.Digital Forensics by IBM ICE Publications.

IBS4317	**INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA (ITSEC)**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**
Goal	To impart knowledge on the basics of ITSEC				

OBJECTIVES	**OUTCOMES**
The course should enable the student to: 1. Learn about SCOPE, Functionality, 2. Learn about Effectiveness and correctness of assurances	The students should be able to: 1. Have a basic knowledge on SCOPE and Functionality 2. Have an understanding on effectiveness and correctness of assurances and Human factors prevention.

UNIT I SCOPE 9

Technical Security Measures, Systems and Products, Functionality and Assurance, Classes and Levels, Assurance Profiles, The Evaluation Process, The Certification Process,

Relationship to the TCSEC

UNIT II FUNCTIONALITY 9

Introduction, The Security Target, Generic Headings, Predefined Classes, Specification Style, Formal Models of Security Policy

UNIT III ASSURANCE – EFFECTIVENESS 9

Introduction, Description of the Approach, Systems and Products, Effectiveness Criteria – Construction - Aspect 1 - Suitability of Functionality, -Aspect 2 - Binding of Functionality, -Aspect 3 - Strength of Mechanisms, -Aspect 4 - Construction Vulnerability Assessment, Effectiveness Criteria – Operation -Aspect 1 - Ease of Use, -Aspect 2 - Operational Vulnerability Assessment

UNIT IV ASSURANCE – CORRECTNESS 9

Introduction, Characterization, Summary of Requirements, Approach to Descriptions, Layout of Correctness Criteria

UNIT V PREVENTION: HUMAN FACTORS 9

Ethical Decision Making and High Technology - Introduction: The ABCs of Computer Ethics -Introduction: Awareness, Basics, Considerations, Security Policy Guidelines - Introduction, Terminology, Resources for Policy Writers, Writing the Policies, Organizing the Policies, Presenting the Policies, Maintaining Policies, Security Policy Guidelines - Introduction, Terminology, Resources for Policy Writers, Writing the Policies, Organizing the Policies, Presenting the Policies, Maintaining Policies. Employment Practices and Policies - Introduction, Hiring, Management, Termination of Employment. Vulnerability Assessment - Scorekeeper of Security Management, Taxonomy of Vulnerability Assessment Technologies, Penetration Testing. Operations Security and Production Controls - Introduction, Operations Management, Providing a Trusted Operating System, Protection of Data, Data Validation. E-Mail and Internet Use Policies - Introduction, Damaging the Reputation of the Enterprise, Threats to People and Systems, Threats to Productivity, Legal Liability. Implementing a Security Awareness Program - Introduction, Awareness as a Survival Technique, Critical Success Factors, Obstacles and Opportunities, Approach. Content, Techniques and Principles, Tools, Measurement and Evaluation, Using Social Psychology to Implement Security Policies - Introduction, Rationality is Not Enough, Beliefs and Attitudes, Encouraging Initiative, Group Behavior, Technological Generation Gaps. Security Standards for Products - Introduction Nonstandard Product Assessment Alternatives Security Assessment Standards for Products Standards for Assessing Product Builders Combined Product and Product Builder Assessment Standards Common Criteria Paradigm Overview Details About the Common Criteria Standard Using the CC to Define Security Requirements and Security Solutions Common Test Methodology for CC Tests and Evaluations Global Recognition of CEM/CC-Based Assessments Example National Scheme: CCEVS Validated Profiles and Products Benefits of CC Evaluation.

TOTAL : 45

TEXT BOOK

1.Information Technology Security Evaluation Criteria (ITSEC) by IBM ICE Publications.

SEMESTER VII

IBS4401	INFORMATION SECURITY AUDIT & MONITORING	L	T	P	C
		2	0	2	3
Goal	To have an understanding about Information security Audit & Monitoring				

OBJECTIVES	OUTCOMES
The course should enable the student to: 1. Learn about the Auditing and Auditing trails 2. Learn about penetration testing and vulnerability assessment .	The students should be able to: 1. Have the desired knowledge on penetration testing and vulnerability assessment. 2. Come up with counter measure techniques .

UNIT I AUDITING AND AUDIT TRAILS 9

Accountability, Compliance, Audit Trails, Reporting timeline, Record Retention, External Auditors, Laws

UNIT II MONITORING 9

Monitoring tools, Warning banner, Traffic analysis, Trend analysis

UNIT III PENETRATION TESTING & VULNERABILITY ASSESSMENT -1 9

Customers and Legal Agreements, Rules of Engagement, Penetration Testing Planning and Scheduling, Pre-Penetration Testing Checklist, Information Gathering, Vulnerability Analysis, External Penetration Testing.

UNIT IV PENETRATION TESTING & VULNERABILITY ASSESSMENT -2 9

Internal Network Penetration Testing, Penetration testing for Denial of Service, Password

Cracking, Social-Engineering, Stolen Laptop, PDAs and Cell phones, Application, Physical Security, Database, VoIP, VPN, War Dialing, Virus and Trojan Detection, Log Management, File Integrity Checking, BlueTooth and Handheld Device, Telecommunication and Broadband Communication.

UNIT V COUNTER MEASURES **9**

Email Security, Security Patches, Data Leakage, Penetration Testing Deliverables and Conclusion, Penetration Testing Report and Documentation Writing, Penetration Testing Report Analysis, Post Testing Actions, Ethics of a Penetration Tester, Standards and Compliance.

TOTAL : 45

TEXT BOOK

1.Information Security Audit & Monitoring by IBM ICE Publications.

IBS4402	**INFORMATION SECURITY INTELLIGENCE AND COMPLIANCE ANALYTICS USING BIG DATA**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**
Goal	To have an basic knowledge on IS intelligence and compliance analytics using Big Data				

OBJECTIVES	**OUTCOMES**
The course should enable the student to: 1. Learn briefly about Big Data 2. Learn about the Sources of Big data and analytics.	The students should be able to: 1. Have a knowledge on Big data 2. Know the security and compliances of Big Data. 3. Know about big Data Analytics

UNIT I INTRODUCTION TO BIG DATA **9**

What Is Big Data?, The Arrival Of Analytics, Where Is The Value?, More To Big Data Than Meets The Eye, Dealing With The Nuances Of Big Data, An Open Source Brings Forth Tools, Caution: Obstacles Ahead; Why Big Data Matters - Big Data Reaches Deep, Obstacles Remain, Data Continue To Evolve, Data And Data Analysis Are Getting More Complex, The Future Is Now; Big Data And The Business Case - Realizing Value, The Case For Big Data, The Rise Of Big Data Options, Beyond Hadoop, With Choice Come Decisions

UNIT II BUILDING THE BIG DATA TEAM **9**

The Data Scientist, The Team Challenge, Different Teams, Different Goals, Don’t Forget the Data, Challenges Remain, Teams Versus Culture, Gauging Success

UNIT III BIG DATA SOURCES AND THE NUTS AND BOLTS OF BIG DATA 9

Hunting for Data, Setting the Goal, Big Data Sources Growing, Diving Deeper Into Big Data

Sources, A Wealth Of Public Information, Getting Started With Big Data Acquisition, Ongoing Growth, No End In Sight; The Storage Dilemma, Building A Platform, Bringing Structure To Unstructured Data Processing Power, Choosing Among In-house, Outsourced, Or Hybrid Approaches

UNIT IV SECURITY, COMPLIANCE, AUDITING, AND PROTECTION AND THE EVOLUTION OF BIG DATA 9

Pragmatic Steps to Securing Big Data, Classifying Data, Protecting Big Data Analytics, Big Data and Compliance, The Intellectual Property Challenge; Big Data: The Modern Era, Today, Tomorrow, And The Next Day, Changing Algorithms

UNIT V BEST PRACTICES FOR BIG DATA ANALYTICS 9

Start Small with Big Data, Thinking Big, Avoiding Worst Practices, Baby Steps, The Value of Anomalies, Expediency Versus Accuracy, In-memory Processing; The Path to Big Data, The Realities Of Thinking Big Data, Hands-on Big Data, The Big Data Pipeline In Depth, Big Data Visualization, Big Data Privacy

TOTAL : 45

TEXT BOOK

1.Information Security intelligence and compliance analytics by IBM ICE Publications.