KALINGA UNIVERSITY

RAIPUR | INDIA

SCHEME & SYLLABUS FOR

Bachelor of Vocational Studies (B.Voc) Cyber Security

NAAC GRADE B+ Accredited University

nirf RANKING 2024 Ranked in Top 151-200 Universities

Kalinga University, Naya Raipur, Chhattisgarh

KALINGA UNIVERSITY
RAIPUR | INDIA

B.VOC IN CYBER SECURITY

Semester - I								
Course Code	**Course Title**	**Credits**	**L**	**T**	**P**	**Internal Marks**	**End Semester Exam Marks**	**Total**
BVCS101	Communication Skills	3	3	0	0	30	70	100
BVCS102	Fundamentals of Information Technology	3	3	0	0	30	70	100
BVCS103	Digital Interface Development	3	3	0	0	30	70	100
BVCS104	Fundamentals of Information Security	3	3	0	0	30	70	100
BVCS105P	**Industrial Training/ On Job Training/ Workshop**	18	0	0	36	50	150	200
Total		**30**	**12**	**0**	**36**	**170**	**430**	**600**

Semester - II								
Course Code	**Course Title**	**Credits**	**L**	**T**	**P**	**Internal Marks**	**End Semester Exam Marks**	**Total**
BVCS201	Fundamentals of Cyber Forensics	3	3	0	0	30	70	100
BVCS202	Environmental Studies	3	3	0	0	30	70	100
BVCS203	Operating Systems	3	3	0	0	30	70	100
BVCS204	Data structures	3	3	0	0	30	70	100
BVCS205P	**Industrial Training/ On Job Training/ Workshop**	18	0	0	36	50	150	200
Total		**30**	**12**	**0**	**36**	**170**	**430**	**600**

Semester - III								
Course Code	**Course Title**	**Credits**	**L**	**T**	**P**	**Internal Marks**	**End Semester Exam Marks**	**Total**
BVCS301	Ethical Hacking	3	3	0	0	30	70	100
BVCS302	Data Analytics	3	3	0	0	30	70	100
BVCS303	Mathematics and Statistics for Computing	3	3	0	0	30	70	100
BVCS304	Cyber Threat Intelligence	3	3	0	0	30	70	100
BVCS305P	**Industrial Training/ On Job Training/ Workshop**	18	0	0	36	50	150	200
Total		**30**	**12**	**0**	**36**	**170**	**430**	**600**

Semester - IV								
Course Code	**Course Title**	**Credits**	**L**	**T**	**P**	**Internal Marks**	**End Semester Exam Marks**	**Total**
BVCS401	Cybersecurity Risk Management and Auditing	3	3	0	0	30	70	100
BVCS402	Free and Open Source Softwares (FOSS)	3	3	0	0	30	70	100
BVCS403	Threats in Social Media	3	3	0	0	30	70	100
BVCS404	Principles of Secure Coding	3	3	0	0	30	70	100
BVCS405P	**Industrial Training/ On Job Training/ Workshop**	18	0	0	36	50	150	200
Total		**30**	**12**	**0**	**36**	**170**	**430**	**600**

Semester - V								
Course Code	**Course Title**	**Credits**	**L**	**T**	**P**	**Internal Marks**	**End Semester Exam Marks**	**Total**
BVCS501	Statistical Analysis with R	3	3	0	0	30	70	100
BVCS502	Digital Forensics	3	3	0	0	30	70	100
BVCS503	Security Architecture and Engineer-ing	3	3	0	0	30	70	100
BVCS504	Data and Cyber Security	3	3	0	0	30	70	100
BVCS505P	**Industrial Training/ On Job Train-ing/ Workshop**	18	0	0	36	50	150	200
Total		**30**	**12**	**0**	**36**	**170**	**430**	**600**

Semester - VI								
Course Code	**Course Title**	**Credits**	**L**	**T**	**P**	**Internal Marks**	**End Semester Exam Marks**	**Total**
BVCS601	Biometrics Security	3	3	0	0	30	70	100
BVCS602	Cloud architecture and security	3	3	0	0	30	70	100
BVCS603	Internet of Things(IoT)	3	3	0	0	30	70	100
BVCS604	Network Security	3	3	0	0	30	70	100
BVCS605P	**Industrial Training/ On Job Train-ing/ Workshop**	18	0	0	36	50	150	200
Total		**30**	**12**	**0**	**36**	**170**	**430**	**600**

KALINGA UNIVERSITY
RAIPUR|INDIA

SEMESTER-01

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS101
COMMUNICATION SKILLS

Course Objective:

- The purpose of this course is to introduce students to the theory, fundamentals and tools of communication and to develop in them vital communication skills which should be integral to personal, social and professional interactions. One of the critical links among human beings and an important thread that binds society together is the ability to share thoughts, emotions and ideas through various means of communication: both verbal and non-verbal. In the context of rapid globalization and increasing recognition of social and cultural pluralities, the significance of clear and effective communication has substantially enhanced.

Course outcomes:

- The purpose of this course is to introduce students to the theory, fundamentals and tools of communication
- To develop vital communication skills which should be integral to personal, social and professional interactions.
- One of the critical links between human beings.
- An important thread that binds society together is the ability to share thoughts, emotions and ideas through various means of communication: both verbal and non-verbal.
- In the context of rapid globalization and increasing recognition of social and cultural pluralities, the significance of clear and effective communication has substantially enhanced.

Unit 1: **06**

- **Introduction:** Theory of communication, types and modes of communication, mediums and channels of communication, barriers to communication, English as a global language, the lingua franca, social influences on English

Unit 2: **06**

- **Language of Communication:** Verbal and non-verbal (spoken and written) personal, social and business barriers and strategies intra-personal, inter-personal and group communication, varieties of English, language, accent, dialect, colloquialism, historical influences on English

Unit 3: **06**

- **Speaking Skills:** Monologue dialogue group discussion effective communication/ mis-communication interview public speech, regional influences on English, convergence and divergence, linguistic imperialism

Unit 4: **06**

- **Reading and Understanding** Close reading, reading analysis of a text - audience and purpose, content and theme, tone and mood, stylistic devices, structure comprehension- analysis and interpretation translation(from Indian language to English and vice-versa) literary/knowledge texts

Unit 5: **06**

- **Writing Skills**: Documenting report writing making notes letter writing, writing tabloids, diary entry, open letters, essays, newsletter and magazine articles, skits, short stories, impersonating characters it will enhance language of communication, various speaking skills such as personal communication, social interactions and communication in professional situations such as interviews, group discussions and office environments, important reading skills as well as writing skills such as report writing, note taking etc. while, to an extent, the art of communication is natural to all living beings, in today's world of complexities, it has also acquired some elements of science. it is hoped that after studying this course, students will find a difference in their personal and professional interactions.

References:

- Fluency in English - Part II, Oxford University Press, 2006.
- Business English, Pearson, 2008.
- Language, Literature and Creativity, Orient Blackswan, 2013.
- Language through Literature (forthcoming) ed. Dr. Gauri Mishra, Dr. Ranjana Kaul, Dr. Brati Biswas

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS102
FUNDAMENTALS OF INFORMATION TECHNOLOGY

Course objective:

- This is a basic course for commerce students to familiarize with computer and it's applications in the relevant fields and exposes them to other related courses of IT.

Course Outcomes:

- Gain a foundational understanding of key IT concepts, including hardware, software, and networks.
- Develop proficiency in using common computer applications, such as word processing and spreadsheet software.
- Explore the ethical and security considerations in IT, emphasizing responsible digital behavior.
- Acquire problem-solving skills by applying IT knowledge to real world scenarios.
- Prepare for further studies in IT or related fields by establishing a strong IT knowledge base.

Unit-1: **06**

- **Computer characteristics:** Speed, storage, accuracy, diligence; digital signals, binary system, ASCII; historic evolution of computers;
- **Classification of computers:** microcomputer, minicomputer, mainframes, supercomputers;
- **Personal computers:** desktop, laptops, palmtop, tablet; hardware & software; von Neumann model.

Unit-2: **06**

- **Hardware:** CPU, memory, input devices, output devices.
- **Memory units:** RAM (SDRAM, DDR RAM, RDRAM etc. feature wise comparison only); ROM-different types: Flash memory;
- **Auxiliary storage:** Magnetic devices, optical devices; floppy, hard disk, memory stick, CD, DVD, CD/DVD-Writer**;**
- **Input devices -** keyboard, mouse, scanner, speech input devices, digital camera, touch screen voice input, joystick, optical readers, bar code reader;
- **Output devices:** Display device, size and resolution; CRT, LCD, LED;
- **Printers:** Dot-matrix, inkjet, laser; plotters, sound cards & speaker.

Unit-3: **06**

- **Software:** System software, application software; concepts of files and folders, introduction to operating systems, different types of operating systems: single user, multitasking, time-sharing multi-user; booting, POST;
- **Basic features of two GUI operating systems:** Windows & Linux (Basic desk top management); Programming Languages, Compiler, Interpreter, Databases;
- **Application software:** Generic features of word processors, spread sheets and presentation software; generic introduction to latex for scientific typesetting; utilities and their use; computer viruses & protection, free software, open source.

Unit-4: **06**

- **Computer Networks and Internet:** Connecting computers, requirements for a network: server, workstation, switch, router, network operating systems; internet: brief history, world wide web, websites, URL, browsers, search engines, search tips; internet connections: isp, dial-up, cable modem, well, dsl, leased line wireless and Wi-Fi connectivity ; email, email software features (send receive, filter, attach, forward, copy, blind copy); characteristics of web-based systems, web pages, web programming languages.

Unit-5: **06**

- **Information Technology and Society:** Indian IT Act, intellectual property rights, issues. application of information technology in railways, airlines, banking, insurance, inventory control, financial systems, hotel management, education, video games, telephone exchanges, mobile phones, information kiosks, special effects in movies.
- **Programming Concepts & Techniques:** Program concept, characteristics of programme, stages in program development, tips for program designing, programming aids, algorithms, pseudo code, notations, design, flowcharts, symbols, rules, compiler & interpreter. introduction to programming techniques, top-down & bottom-up approach, unstructured, & modular programming, cohesion, coupling, debugging, syntax & logical errors, linking and loading, testing and debugging, documentation.

References:

- Programming in C, R.S. Salaria, Khanna Publishing House
- Computer Concepts and Programming in C, R.S. Salaria, Khanna Publishing House
- Handbook of Computer Fundamentals, N.S. Gill, Khanna Publishing House

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS103
DIGITAL INTERFACE DEVELOPMENT

Course Outcomes:

After successful completion of this course, the students should be able to:

- Learn the HTML and CSS syntax and semantics to build web pages.
- Construct and visually format tables and forms using HTML and CSS.
- Analyze Develop Client-Side Scripts using Java Script.
- Familiarize with Server-Side Scripts using PHP to generate and display the contents dynamically.

Unit 1: **08**

HTML&CSS:

- Introduction of HTML, Dynamic HTML, HTML Syntax & Semantic Markup, Structure of HTML Documents, HTML5 Semantic Structure Elements, Hyperlinks, Images and Multimedia, Forms and controls, Marquee tags, GUI HTML Editors, Image Inserting Techniques.
- **Basics of cascading style sheets (CSS):** CSS syntax & Properties, CSS Selectors, Lists and Tables, CSS Styling (Background, Text Format, and Controlling Fonts), The Cascade: Box Model, CSS Text Styling.

Unit 2: **08**

Introduction to Forms & HTML Tables:

- HTML Tables and Forms, Create Frames, Introducing Tables, Styling Tables, Introducing Forms, Create Web Forms, Form Control Elements, Table and Form Accessibility, Micro formats.
- Advanced Cascading styles (CSS): Creating page Structure and Site Designs, Elements Positions, Floating Elements, Designing, Multicolumn Structure, Approaches to CSS Layout, CSS Frameworks.

Unit 3: **07**

JavaScript:

- **JavaScript:** Client-Side Scripting, Features of JavaScript, and its design and principles, Java “vs” JavaScript, Variables, JavaScript Objects, Data Types, Array, Functions, String, Loops, Decision Making Form Validation
- The Document Object Model (DOM), Building Blocks of Forms, Properties & Methods of Forms, Button, Text, Text area, Radio buttons, Select elements,
- **Form events:** Mouse & key events, changing attribute value dynamically, Changing Option list dynamically, evaluating checkbox selection.

Unit 4: **07**

Basics of PHP:

- Introduction of PHP, PHP features, Syntax, data types, variables, PHP echo and print Statements Casting, PHP Math, PHP Operators, PHP If...Else.... Elseif statements, PHP Loops, PHP Switch, PHP, PHP Functions, Arrays, PHP Global Variables- Superglobals, PHP Form Handling & Validation, Session and Cookie.
- Database Connectivity with MySQL, Introducing JQuery, JQuery Forms, JQuery Examples.

References:

- Robin Nixon, “Learning PHP, MySQL &JavaScript with jQuery, CSS and HTML5”, 4th Edition, O’Reilly Publications, 2015. (ISBN:978-9352130153)
- Luke Welling, Laura Thomson, “PHP and MySQL Web Development”, 5th Edition, Pearson Education, 2016. (ISBN:978-9332582736)
- Nicholas C Zakas, “Professional JavaScript for Web Developers”, 3rd Edition, Worx/Wiley India, 2012. (ISBN:978-8126535088)
- David Sawyer McFarland, “JavaScript & jQuery: The Missing Manual”, 1st Edition, O’Reilly/Shroff Publishers & Distributors Pvt Ltd, 2014

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS104
FUNDAMENTALS OF INFORMATION SECURITY

Course Objective:

- To introduce the basic terminology of information security.

Unit 1: **08**

- Introduction to Information Security, The history of Information security, Why is security needed, security principles, Components of an Information system-Confidentiality, integrity, authentication, security policy, basic network security terminology.

Unit 2: **08**

- **Introduction to security attacks-** Compromises to individual property, Deliberate software attacks, Espionage, Sabotage, Theft, Attacks- DOS,DDOS, Information Leakage, Regular File Access, Misinformation, Special File/Database Access, Remote Arbitrary Code Execution, Elevation of privileges, Man-in-the-middle, Spam, Social Engineering (Concepts only)

Unit 3: **07**

- **Cryptography-** cryptography, symmetric encryption, substitution ciphers, transposition ciphers, steganography, Block ciphers, modes of operation, Data Encryption Standard, Public key cryptography, applications, strength and weakness, RSA algorithm, Authentication, authentication methods, message digest, digital signatures, digital signature algorithm, DSS, E-mail security: Pretty Good Privacy, working of PGP, S/MIME, MIME, IP Security, Architecture, IPSec: strengths and benefits, IPv4, IPv6, ESP protocol, Web Security: Secure Socket layer, SSL session and connection

Unit 4: **07**

- Firewall, characteristics of firewall, packet filters, application level gateways, firewall architecture, trusted systems. IDS-infrastructure, classification, host based IDS, network based IDS, anomaly, signature detection, Intrusion detection tools-snort, tripwire

References:

- Principles of Information Security- Michael E. Whitman, Herbert J. Mattord, Cengage Learning, Fourth edition, 2011
- Computer Security basics- Rick Lehtinen, O'Reilly, 2nd edition, 2006
- Absolute beginner's guide to Security, Spam, Spyware & Viruses- Andy Walker, Que publishers, 2005
- Information Security Management Principles- Andy Taylor, David Alexander, Amanda Finch, David Sutton, BCS publishers, 2008
- Guide to Computer forensics and Investigations- B. Nelson, A. Phillips, F. Enfinger, C. Steuart, Cengage Learning, 4th edition, 2010

KALINGA UNIVERSITY
RAIPUR|INDIA

BVCS105P
INDUSTRIAL TRAINING/ON JOB TRAINING/ WORKSHOP

KALINGA UNIVERSITY
RAIPUR|INDIA

SEMESTER-02

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS201
FUNDAMENTALS OF CYBER FORENSICS

Course Objective:

- Understanding of cyber forensics concept such as acquisition and analysis

Unit 1: **08**

- **Introduction to Computer Forensics:** Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques – Incident and incident response methodology – Forensic duplication and investigation. Preparation for IR: Creating response tool kit and IR team. – Forensics Technology and Systems – Understanding Computer Investigation – Data Acquisition.

Unit 2: **08**

- **Evidence Collection and Forensics Tools:** Processing Crime and Incident Scenes – Working with Windows and DOS Systems. Current Computer Forensics Tools: Software/ Hardware Tools.

Unit 3: **07**

- **Analysis and Validation:** Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics

Unit 4: **07**

- **Ethical Hacking:** Introduction to Ethical Hacking – Foot printing and Reconnaissance – Scanning Networks – Enumeration – System Hacking – Malware Threats – Sniffing:
- **Ethical Hacking in Web:** Social Engineering – Denial of Service – Session Hijacking – Hacking Web servers – Hacking Web Applications – SQL Injection – Hacking Wireless Networks – Hacking Mobile Platforms.

References:

- Computer Forensics and Investigations- Bill Nelson, Amelia Phillips, Frank Enfinger, Christopher Steuart, Second Indian Reprint 2009, Cengage Learning India Private Limited.
- Digital Evidence and Computer Crime – Eoghan Casey, Edition 3, Academic Press, 2011
- Computer Forensics and Cyber Crime: An Introduction – MarjieBritz, Edition 2, Prentice Hall, 2008
- Practical guide to Computer Forensics- David Benton and Frank Grindstaff, 2006, Book Surge Publishing, 2006
- Computer Evidence: Collection & Preservation- Christopher L.T Brown Charles River Media publishing, Edition 1, 2005
- Computer Investigation (Forensics, the Science of crime-solving) – Elizabeth Bauchner, Mason Crest Publishers, 2005

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS202
ENVIRONMENTAL STUDIES

Course Outcomes:

- Master core concepts and methods from ecological and physical sciences and their application in environmental problem solving.
- Appreciate the ethical, cross-cultural, and historical context of environmental issues and the links between human and natural systems.
- Apply systems concepts and methodologies to analyze and understand interactions between social and environmental processes.
- Reflect critically about their roles and identities as citizens, consumers and environmental actors in a complex, interconnected world.
- Master core concepts and methods from economic, political, and social analysis as they pertain to the design and evaluation of environmental policies and institutions.

Unit 1: **06**

Introduction to Environmental Studies:

- Multidisciplinary nature of environmental studies, Scope and importance; concept of sustainability and sustainable development.

Ecosystems:

- What is an ecosystem? Structure and function of the ecosystem;
- **Energy flow in an ecosystem:** food chains, food webs and ecological succession.
- **Case studies of the following ecosystems**: Forest ecosystem, grassland ecosystem, desert ecosystem, aquatic ecosystems (ponds, streams, lakes, rivers, oceans, estuaries)

Unit-2: **06**

Natural Resources:

- **Renewable and Non-renewable Resources:** Land resources and land use change; Land degradation, soil erosion and desertification.
- **Deforestation:** Causes and impacts due to mining, dam building on environment, forests, biodiversity and tribal populations.
- **Water:** Use and over--exploitation of surface and ground water, floods, droughts, conflicts over water (international & inter--state).
- **Energy resources:** Renewable and non-renewable energy sources, use of alternate energy sources, growing energy needs, case studies.

Unit-3: **06**

Biodiversity and Conservation:

- **Levels of biological diversity:** genetic, species and ecosystem diversity; Biogeographic zones of India; Biodiversity patterns and global biodiversity hot spots, India as a mega--biodiversity nation; Endangered and endemic species of India
- **Threats to biodiversity:** Habitat loss, poaching of wildlife, man--wildlife conflicts, biological invasions;
- **Conservation of biodiversity:** In--situ and Ex--situ conservation of biodiversity.
- **Ecosystem and biodiversity services:** Ecological, economic, social, ethical, aesthetic and Informational value.

Unit-4: **06**

Environmental Pollution:

- Types, causes, effects and controls; Air, water, soil and noise pollution, Nuclear hazards and human health risks
- **Solid waste management:** Control measures of urban and industrial waste. Pollution case studies.

Environmental Policies & Practices:

- Climate change, global warming, ozone layer depletion, acid rain and impacts on human communities and agriculture
- **Environment Laws:** Environment Protection Act; Air (Prevention & Control of Pollution) Act; Water (Prevention and control of Pollution) Act; Wildlife Protection Act; Forest Conservation Act. International agreements: Montreal and Kyoto protocols and Convention on Biological Diversity (CBD).
- Nature reserves, tribal populations and rights, and human wildlife conflicts in Indian context.

Unit-5: **06**

Human Communities and the Environment:

- **Human population growth:** Impacts on environment, human health and welfare. Resettlement and rehabilitation of project affected persons; case studies.
- **Disaster management:** floods, earthquake, cyclones and landslides.
- **Environmental movements:** Chipko, Silent valley, Bishnois of Rajasthan.
- **Environmental ethics:** Role of Indian and other religions and cultures in environmental conservation. Environmental communication and public awareness, case studies (e.g., CNG vehicles in Delhi).

References:

- Carson, R. 2002. *Silent Spring*. Houghton Mifflin Harcourt.
- Gadgil, M., & Guha, R.1993. This Fissured Land: An Ecological History of India. Univ. of California Press.
- Gleeson, B. and Low, N. (eds.) 1999.Global Ethics and Environment, London, Routledge.
- Gleick, P. H. 1993. Water in Crisis. Pacific Institute for Studies in Dev., Environment & Security. Stockholm Env. Institute, Oxford Univ. Press.
- Groom, Martha J., Gary K. Meffe, and Carl Ronald Carroll.Principles of Conservation Biology. Sunderland: Sinauer Associates, 2006.
- Grumbine, R. Edward, and Pandit, M.K. 2013. Threats from India's Himalaya dams. Science, 339: 36--37.
- McCully, P. 1996. Rivers no more: the environmental effects of dams(pp. 29--64). Zed Books.
- McNeill, John R. 2000. Something New Under the Sun: An Environmental History of the Twentieth Century.
- Odum, E.P., Odum, H.T. & Andrews, J. 1971.Fundamentals of Ecology. Philadelphia: Saunders.
- Pepper, I.L., Gerba, C.P. & Brusseau, M.L. 2011. Environmental and Pollution Science. Academic Press.
- Rao, M.N. & Datta, A.K. 1987. Waste Water Treatment. Oxford and IBH Publishing Co. Pvt. Ltd.
- Raven, P.H., Hassenzahl, D.M. & Berg, L.R. 2012.Environment. 8th edition. John Wiley & Sons.
- Rosencranz, A., Divan, S., & Noble, M. L. 2001. Environmental law and policy in India. Tripathi 1992.
- Sengupta, R. 2003. Ecology and economics: An approach to sustainable development. OUP.
- Singh, J.S., Singh, S.P. and Gupta, S.R. 2014. Ecology, Environmental Science and Conservation. S. Chand Publishing, New Delhi.
- Sodhi, N.S., Gibson, L. & Raven, P.H. (eds). 2013. Conservation Biology: Voices from the Tropics. John Wiley & Sons.
- Thapar, V. 1998. Land of the Tiger: A Natural History of the Indian Subcontinent.
- Warren, C. E. 1971. Biology and Water Pollution Control. WB Saunders.
- Wilson, E. O. 2006.The Creation: An appeal to save life on earth. New York: Norton.
- World Commission on Environment and Development. 1987.Our Common Future. Oxford University Press.

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS203
OPERATING SYSTEMS

Course Objectives:
To introduce students to:
- Fundamental concepts of systems software
- Functions of operating systems as a resource manager
- Strategies for constrained resource allocation
- Memory and I/O Management techniques

Unit 1: **08**
- **Introduction to Operating System:** Introduction, Operating system structures- operating system operations, operating system services, user operating system interface, system programs, system calls, Types of System Calls, operating system structure.
- **Process Management:** Process concept, Process Scheduling, Operations on processes, Inter-process communication, Threads-Overview, Multithreading model, Thread Libraries, Threading issues; CPU
- **Scheduling:** Basic concepts, scheduling criteria, scheduling algorithms.

Unit 2: **08**
- **Process synchronization:** Background, Critical section problem, Peterson's solution, Semaphore, Classical synchronization problem- bounded buffer problem, reader/writer problem, The Dining Philosopher's problem.
- **Deadlocks:** deadlock characterization, methods for handling deadlock- deadlock prevention, deadlock avoidance, deadlock detection, deadlock recovery.

Unit 3: **07**
- **Memory Management & Protection:** Basic Hardware, Address binding, logical versus physical address space, Swapping, Contiguous memory allocation memory mapping and protection, memory allocation, fragmentation,
- **Non-contiguous allocation-** paging, segmentation. Virtual memory-Demand Paging, page replacement, Allocation of frames, Thrashing, Allocating Kernel Memory.
- **Protection and Security:** Protection -principles of protection, domain of protection, access matrix, access control; Security- threats, user authentication.

Unit 4: **07**
- **Storage management:** File system Interface — file concept, access methods, directory structure, File Sharing. File system implementation- file system structure & implementation, directory implementation, allocation methods, free space management; Mass storage management - disk structure, disk scheduling, RAID; I/O Systems- I,/O hardware, Application I/O interface, kernel I/O subsystem.

References:

- Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Operating System Principles
- Achyut S Godbole, Operating systems, Mc-GRawhill, Third Edition

Assignments and Activities:

- case study of popular Operating Systems like Android, Windows, Sim Solaris, IOS etc

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS204
DATA STRUCTURES

Course Objectives:
By the end of the course, students should:
- Be able to write well-structured programs in C
- Be familiar with data structures like array, structures, lists, stacks, queues, trees and graphs
- Able to appreciate various searching and sorting strategies

Unit 1: **08**
- Sequential searching, binary searching, Hashing-linear hashing, hash functions, hash table searching, sorting: bubble sort, selection sort.
- **Stacks and Queues:** FIFO and LIFO data structures-stacks using
  i) pointers and
  ii) arrays.
- **Queues using:**
  i) pointers and
  ii) arrays,

- Operations on stack and queues, applications, polish notation.

Unit 2: **08**
- **Linked Lists:** Concept of static versus dynamic data structures, implementation of linked lists using pointers, operations on linked lists: insertion, deletion and traversing. Doubly linked lists and circular linked lists, applications of linked lists.

Unit 3: **07**
- **Trees:** Concept of linear versus non-linear data structures, various types of trees -biliary, binary search trees. Creating a binary search tree, traversing a binary tree (in-order, pre-order and post order), operations on a tree -insertion, deletion and processing, expression trees, implementation using pointers, applications.

Unit 4: **07**
- **Graphs, graph traversal—** Depth first and Breadth first traversal of graphs, applications.

References:

- A.K.Sharma, Data Structures Using C, Pearson, Second edition, 2011
- Nair A.S., Makhalekshmi, Data Structures in C, PHI, Third edition 2011.

Assignments and Activities:
- Multi-way search trees, B-trees, Hauffman trees, case studies

KALINGA UNIVERSITY
RAIPUR|INDIA

BVCS205P
INDUSTRIAL TRAINING/ON JOB TRAINING/ WORKSHOP

KALINGA UNIVERSITY
RAIPUR|INDIA

SEMESTER-03

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS301
ETHICAL HACKING

Course Objectives:

- To describe Ethical hacking and fundamentals of computer Network.
- To understand about Network security threats, vulnerabilities assessment and social engineering.
- To discuss cryptography and its applications.
- To implement the methodologies and techniques of Sniffing techniques, tools, and ethical issues.

Course Outcomes:

- Articulate the fundamentals of Computer Networks, IP Routing and core concepts of ethical hacking in real world scenarios.
- Apply the knowledge of information gathering to perform penetration testing and social engineering attacks
- Demonstrate the core concepts of Cryptography, Cryptographic checksums and evaluate the various biometric authentication mechanisms.
- Apply the knowledge of network reconnaissance to perform Network and web application-based attacks.
- Apply the concepts of hardware elements and endpoint security to provide security to physical devices.
- Simulate various attack scenarios and evaluate the results.

Unit 1: **08**

- **Introduction to Ethical Hacking:** Fundamentals of Computer Networks/IP protocol stack, IP addressing and routing, Routing protocol, Protocol vulnerabilities, Steps of ethical hacking, Demonstration of Routing Protocols using Cisco Packet Tracer
- **Self-learning Topics:** TCP/IP model, OSI model
- **Introduction to Cryptography:** Private-key encryption, public key-encryption, key Exchange Protocols, Cryptographic Hash Functions & applications, steganography, biometric authentication, lightweight cryptographic algorithms. Demonstration of various cryptographic tools and hashing algorithms
- **Self-learning Topics:** Quantum cryptography, Elliptic curve cryptography

Unit 2: **08**

- **Introduction to network security:** Information gathering, reconnaissance, scanning, vulnerability assessment, Open VAS, Nessus, System hacking: Password cracking, penetration testing, Social engineering attacks, Malware threats, hacking wireless networks (WEP, WPA, WPA- 2), Proxy network, VPN security, Study of various tools for Network Security such as Wireshark, John the Ripper, Metasploit, etc.
- **Self-learning Topics**: Ransomware (Wannacry), Botnets, Rootkits, Mobile device security

Unit 3: **07**

- **Introduction to web security and Attacks:** OWASP, Web Security Considerations, User Authentication, Cookies, SSL, HTTPS, Privacy on Web, Account Harvesting, Web Bugs, Sniffing, ARP poisoning, Denial of service attacks, Hacking Web Applications, Clickjacking, Cross-Site scripting and Request Forgery, Session Hijacking and Management, Phishing and harming Techniques, SSO, Vulnerability assessments, SQL injection, Web Service Security, OAuth 2.0, Demonstration of hacking tools on Kali Linux such as SQLMap, HTTrack, hping, burp suite,Wireshark etc.
- **Self-learning Topics:** Format string attacks

Unit 4: **07**

- **Elements of Hardware Security:** Side channel attacks, physical unclonable functions, Firewalls, Backdoors and trapdoors, Demonstration of Side Channel Attacks on RSA, IDS and Honeypots.
- **Self-learning Topics**: IoT security
- **Case Studies:** Various attacks scenarios and their remedies. Demonstration of attacks using DVWA.
- **Self-learning Topics:** Session hijacking and man-in middle attacks

References (Textbooks):

- Computer Security Principles and Practice --William Stallings, Seventh Edition, Pearson Education, 2017
- Security in Computing -- Charles P. Pfleeger, Fifth Edition, Pearson Education, 2015
- Network Security and Cryptography -- Bernard Menezes, Cengage Learning, 2014
- Network Security Bible -- Eric Cole, Second Edition, Wiley, 2011
- Mark Stamp's Information Security: Principles and Practice --Deven Shah, Wiley, 2009

References:

- UNIX Network Programming –Richard Steven,Addison Wesley, 2003
- Cryptography and Network Security -- Atul Kahate, 3rd edition, Tata Mc Graw Hill, 2013 3.TCP/IP Protocol Suite -- B. A. Forouzan, 4th Edition, Tata Mc Graw Hill, 2017
- Applied Cryptography, Protocols Algorithms and Source Code in C -- Bruce Schneier, 2nd Edition / 20th Anniversary Edition, Wiley, 2015
- Cryptography and Network Security -- Atul Kahate, 3rd edition, Tata Mc Graw Hill, 2013 3.TCP/IP Protocol Suite -- B. A. Forouzan, 4th Edition, Tata Mc Graw Hill, 2017

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS302
DATA ANALYTICS

Course Objectives:
The Student should be familiarized:

- Be Exposed To Big Data.
- Learn Different Ways of Data Analysis.
- Be Familiar with Data Streams.
- Learn Mining and Clustering techniques.
- Be Familiar with Visualization techniques.

Unit 1: **08**

- **Introduction to Big Data:** Introduction to Big Data Platform – Challenges Of Conventional Systems – Web Data – Evolution Of Analytic Scalability, Analytic Processes And Tools, Analysis Vs Reporting – Modern Data Analytic Tools, Stastical Concepts: Sampling Distributions, Resampling, Statistical Inference, Prediction Error.

Unit 2: **08**

- **Data Analysis:** Regression Modeling, Multivariate Analysis, Bayesian Modeling, Inference And Bayesian Networks, Support Vector And Kernel Methods, Analysis Of Time Series: Linear Systems Analysis, Nonlinear Dynamics – Rule Induction – Neural Networks: Learning and Generalization, Competitive Learning, Principal Component Analysis and Neural Networks; Fuzzy Logic: Extracting Fuzzy Models from Data, Fuzzy Decision Trees, and Stochastic Search Methods.

Unit 3: **07**

- **Mining Data Streams:** Introduction to Streams Concepts – Stream Data Model And Architecture – Stream Computing, Sampling Data In A Stream – Filtering Streams – Counting Distinct Elements in a Stream – Estimating Moments – Counting Oneness In A Window – Decaying Window

Unit 4: **07**

- **Real time Analytics Platform (RTAP) Applications –** Case Studies – Real Time Sentiment Analysis, Stock Market Predictions.

References:

- Michael Berthold, David J. Hand, Intelligent Data Analysis, Springer, 2007.
- Anand Rajaraman and Jeffrey David Ullman, Mining Of Massive Datasets, Cambridge University Press, 2012.
- Bill Franks, Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analystics, John Wiley & Sons, 2012.
- Glenn J. Myatt, Making Sense Of Data, John Wiley & Sons, 2007 Pete Warden, Big Data Glossary, O‟Reilly, 2011.
- Jiawei Han, MichelineKamber “Data Mining Concepts and Techniques”, Second Edition, Elsevier, Reprinted 2008

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS303
MATHEMATICS AND STATISTICS FOR COMPUTING

Course Objectives:

- To understand concepts of counting
- To understand concepts of functions
- To understand basic concepts of cryptography

Unit 1: **08**

- **Counting-** Basic counting-, Permutations and Subsets- Binomial coefficients-Pascal's Triangle, A proof using the Sum Principle, The Binomial Theorem, Labeling and trinomial coefficients, equivalence relations and counting-The Symmetry Principle, Equivalence Relations, The Quotient Principle, Equivalence class counting

Unit 2: **08**

- Functions, Functions as relations, One -to-One, Onto and Invertible functions, Mathematical Induction, Graphs , Spanning trees, Rooted Trees, Warshall'salgorithm: Shortest paths, Linked representation of directed graphs, Pruning algorithm for shortest path, Dijkstra's shortest path algorithm

Unit 3: **08**

- Introduction to Cryptography, Private Key cryptography, Public-key Cryptosystems, Arithmetic modulo n, Cryptography using multiplication mod n, Solutions to Equations and Inverses mod n, Inverses mod n, GCD, Euclid's Division Theorem, The GCD Algorithm, Computing Inverses, Exponentiation mod n, The RSA Cryptosystem, The Chinese Remainder Theorem, Finding large primes.

Unit 4: **08**

- Recursion Trees, Three Different Behaviors, Master Theorem, Solving More General Kinds of Recurrences

References:

- Discrete Mathematics for Computer Science- Kenneth Bogart, Clifford Stein, Key Curriculum Press, 2006
- Discrete Mathematics with Algorithms- M.O. Albertson, J.P.Hutchinson, John Wiley & Sons, 1988
- Miquel A. Lerma, Notes on Discrete Mathematics.

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS304
CYBER THREAT INTELLIGENCE

Course Objectives:

- Provide a comprehensive understanding of the cyber threat landscape and the importance of threat intelligence.
- Equip students with essential skills in gathering, analyzing, and interpreting threat data.
- Develop proficiency in utilizing threat intelligence tools and frameworks through hands-on exercises.
- Introduce advanced methods for predicting and mitigating cyber threats.
- Enhance the ability to effectively communicate threat intelligence findings and collaborate with cybersecurity teams.

Course Outcomes:

On Successful completion of course, learner will be able to

- Demonstrate a thorough understanding of cyber threats, threat actors, and their tactics, techniques, and procedures (TTPs).
- Apply various methodologies to gather and analyze cyber threat intelligence data.
- Utilize threat intelligence platforms and tools to identify and assess threats.
- Develop strategies to predict and mitigate potential cyber threats based on intelligence data.
- Produce comprehensive threat intelligence reports and effectively communicate findings to various stakeholders.

Unit 1: **08**

Introduction to Cyber Threat Intelligence:

- Definition and Importance of CTI, History and Evolution of Cyber Threat Intelligence, Types of Threat Intelligence (Strategic, Operational, Tactical, Technical)
- Understanding Key CTI Concepts and Terminology, The Intelligence Lifecycle, Practical Exercise: CTI Scenario Analysis
- Types of Cyber Threats, Common Attack Vectors, Threat Actors and Their Motivations

Threat Data Collection and Sources:

- Threat Data Collection Techniques:- Passive and Active Data Collection Methods, Open Source Intelligence (OSINT), Human Intelligence (HUMINT)
- Practical Exercise: Collecting Threat Data, Hands-on Exercise in Collecting Data from Various Sources, Ensuring Data
  Quality and Relevance
- Overview of Popular TIPs, Integrating Data Sources with TIPs, Practical Exercise: Setting Up a TIP

Unit 2: **08**

Analyzing Cyber Threat Intelligence:

- **Threat Analysis Techniques:** Qualitative and Quantitative Analysis Methods, Indicators of Compromise (IoCs), Analyzing Tactics, Techniques, and Procedures (TTPs)
- **Practical Exercise:** Threat Analysis, Hands-on Analysis of Collected Threat Data, Using Analytical Tools and Techniques
- **Advanced Threat Analysis:** Pattern Recognition and Trend Analysis, Attribution and Profiling Threat Actors, Case Studies of Major Cyber Incidents

Unit 3: **07**

Threat Intelligence Frameworks and Models:

- Introduction to Popular CTI Frameworks
- (MITRE ATT&CK, Diamond Model), Understanding the Kill hain Model
- Conducting Threat Intelligence Operations, Planning and Executing CTI Operations, Threat Hunting and Incident Response Integration, Case Studies of Successful CTI Operations

Communicating Threat Intelligence:

- **Reporting and Disseminating Intelligence**: Writing Effective Threat Intelligence Reports, Visualizing Data for Better Understanding, Communicating Findings to Different Audiences
- **Practical Exercise:** Reporting Threat Intelligence:- Creating and Presenting Threat Intelligence Reports, Peer Review and Feedback
- **Collaboration and Sharing Intelligence:** Information Sharing and Analysis Centers (ISACs), Legal and Ethical Considerations in Sharing Intelligence, Best Practices for Collaboration

Unit 4: **07**

Advanced Threat Intelligence Techniques:

- **Predictive Intelligence and Threat Forecasting**: Predictive Analytics in CTI, Tools and Techniques for Threat Forecasting, Practical Exercise: Predicting Future Threats
- **Cyber Threat Intelligence Automation:** Leveraging AI and Machine Learning in CTI, Automating Data Collection and Analysis, Practical Exercise: Implementing Automation in CTI
- **Capstone Project:** Real-World CTI Analysis, Comprehensive Threat Intelligence Analysis Project, Presentation of Findings and Recommendations, Whole Review and Doubts Session

References:

- Cyber Threat Intelligence: From Strategy to Implementation by Henry Dalziel, 1st Edition
- The Threat Intelligence Handbook: A Practical Guide for Security Teams to nlocking the Power of Intelligence by Chris Poulin, et al., 1st Edition

Useful Link for E-Resources:

- Certified Cyber Threat Intelligence Analyst | Udemy
- Cyber Threat Intelligence Course by IBM | Coursera
- Threat Intelligence Training | CTIA Certification | EC-Council (eccouncil.org)
- https://medium.com/@ivancmoliveira/reverse-engineering-and-analyzingmalware-wannacry-3ce8b3f6406a
- https://www.lockheedmartin.com/content/dam/lockheedmartin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

KALINGA UNIVERSITY
RAIPUR|INDIA

BVCS305P
INDUSTRIAL TRAINING/ON JOB TRAINING/ WORKSHOP

KALINGA UNIVERSITY
RAIPUR|INDIA

SEMESTER-04

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS401
CYBERSECURITY RISK MANAGEMENT AND AUDITING

Course Objectives:

- Gain a solid understanding of essential cyber security principles and their importance in protecting organizational assets.
- Learn the risk management lifecycle and effectively apply risk assessment methodologies, both qualitative and quantitative.
- Recognize various types of cyber threats and common attack vectors, and analyze vulnerabilities through real-world case studies.
- Create and enforce comprehensive cyber security policies and procedures, ensuring compliance and regular updates.

Course Outcomes:

On Successful completion of course, learner will be able to:

- Demonstrate a strong grasp of essential cyber security concepts and their role in protecting organizational assets.
- Perform risk assessments using qualitative and quantitative methods, applying frameworks like NIST and ISO/IEC 27005.
- Recognize various cyber threats and attack vectors, and analyze vulnerabilities through real-world case studies.
- Create, implement, and enforce comprehensive cyber security policies and procedures, ensuring compliance and regular updates.
- Develop a robust incident response plan, manage incidents from detection to recovery, and conduct post-incident reviews to enhance resilience.

Unit 1: **08**

Introduction to Cyber Security and Risk Management:

- Introduction to Cyber Security, Understanding Cyber Security, Importance of Risk Management.
- Key Concepts and Terminology, the Risk Management Lifecycle, Practical Exercise: Risk Management Scenario Analysis.
- Types of Cyber Threats, Common Attack Vectors.

Identifying Threats and Vulnerabilities:

- Understanding Vulnerabilities, Case Studies of Major Cyber Incidents
- Practical Exercise: Identifying Threats and Vulnerabilities
- Introduction to Risk Assessment, Qualitative vs. Quantitative Risk Assessment

Unit 2: **08**

Risk Assessment Methodologies:

- Risk Assessment Frameworks:- NIST, ISO/IEC 27005,etc
- Practical Exercise: Understanding Different Frameworks
- Conducting Risk Assessments

Identifying, Analyzing, and Mitigating Risks:

- Identifying and Analyzing Risks, Practical Exercise: Performing a Risk Assessment
- Risk Mitigation Strategies, Risk Avoidance, Risk Reduction
- More on Risk Mitigation, Risk Sharing and Transfer, Risk Acceptance

Unit 3: **07**

Implementing Security Controls and Policies:

- Implementing Security Controls, Practical Exercise: Developing a Risk Mitigation Plan
- Developing Cyber Security Policies, Implementing Cyber Security Procedures
- Policy Enforcement and Compliance, Regular Review and Updates, Practical Exercise: Drafting Cyber Security Policies

Unit 4: **07**

Cyber Security Frameworks and Incident Response:

- Overview of Key Cyber Security Frameworks, NIST Cybersecurity Framework
- More on Frameworks and Standards, ISO/IEC 27001 and 27002, CIS Controls, Industry-Specific Standards, Practical Exercise: Mapping Organizational Controls to Frameworks
- Incident Response Planning, Incident Detection and Analysis, Containment, Eradication, and Recovery, Post-Incident Activities. Developing an Incident Response Team, Practical Exercise: Simulating an Incident Response

References:

- Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis by Mark Talabis, Jason Martin, 1st Edition
- Risk Management Framework: A Lab-Based Approach to Securing Information Systems by James Broad, Kelly Stewart, 1st Edition
- Cyber Security Risk Management | Udemy
- Introduction to Cybersecurity & Risk Management Specialization [3 courses] (UC Davis) | Coursera
- Cybersecurity Audit Certificate | ISACA

KALINGA UNIVERSITY
RAIPUR|INDIA

BVCS402
FREE AND OPEN SOURCE SOFTWARES (FOSS)

Course Objectives:
At the end of this course, the students will be able to

- Explain the features of free &open source software Familiarization with LINUX
- Work with PHP
- Demonstrate the working of MySQL

Unit 1: **08**

- **Open source software:** Features, advantages over proprietary software, examples, Free software: concepts, features, free software Vs Open Source software, free software movements. Policies, GPL, Free OS, History and Features of Linux, Various flavours of Linux, Linux Kernel and Shell, Graphical Desktops- GNOME, KDE, Linux File System and Directories

Unit 2: **08**

- **The building blocks of PHP:** variables, globals & superglobals Data types: Set type, type casting, test type, Operators & Expressions, Flow control functions in PHP, Functions: Defining a function variable scope, calling a function, returning values ,setting default values for arguments, passing ariable reference Arrays: creating arrays(associative & multidimensional), Array related functions Working with strings: Formatting strings, indexing, strlen() functions

Unit 3: **07**

- **Forms in PHP:** Creating a simple input form, combining HTML & PHP code on a single page, redirecting the user ,creating a send mail form, File upload form Cookies: Introduction, setting a cookie with PHP, deleting a cookie, session function overview: starting a session,working with session variables, passing session IDs in the query string, destroying sessions &unsetting variables

Unit 4: **07**

- **Database concepts:** Open source database software: MySQL features MySQL data types: Numeric, date & time, string Table creation in MySQL: insert, select, where clause, ordering the result, like operator Selecting Multiple Tables: using join, using queries Modifying records:update command, eplace command, delete command date & time functions in MySQL Interacting with MySQL using PHP :connecting to MYSQL, Executing queries, Retrieving error messages, inserting data with PHP, retrieving data with PHP

References:

- Julie C.Meloni, PHP, MySQL and Apache, Pearson Education
- Ivan Byross, HTML, DHTML, Javascript, Perl, BPB Publication

KALINGA UNIVERSITY
RAIPUR|INDIA

BVCS403
THREATS IN SOCIAL MEDIA

Course Objective:

- On successful completion of the course the student should have understood the cyber threats in Social websites, classify their types, discuss the cyber threats and its impact

Unit 1: **08**

- **Media & Journalism -** Overview – History, Types , advantages and disadvantages of various media –Journalism – Types of Journalism, Investigative Journalism – Yellow Journalism – Ethics of a Journalist

Unit 2: **08**

- **Social Media –** Print and Television media – Social Networking Sites, Types, advantages and isadvantages, Social Media ethics – Do's and Don'ts in various social medias

Unit 3: **07**

- **Victimization in social media –** Types of victimization – Profiles of social media victims - causes of victimization – trends in victimization in social media in India and other countries. Impact of Social Media threats - Harm to Brand Reputation - Lost Productivity - Strains on Bandwidth – Data Leaks & Disclosure

Unit 4: **07**

- **Threats against Organizations from Social Media -** Executive impersonations - Account takeover -Watering hole phising and malware - Customer scams - Corporate impersonations - Information Leakage – Planning of an attack - Clickbait attacks - Hashtag/ traffic Hijacking .Social media security policies – individuals - Organizational Security Policies

References:

- Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Paperback– Import Edition, Create Space Independent Publishing Platform, 11 August 2015
- Threats and anti threats Strategies for Social Networking Websites by Amir Rokiifard, volume5, International Journal of Computer networks and Communications, July 2013
- Securing the Social Media in the Enterprise by Henry Dalziel, 1st Edition, Elsevier Publication, 2015
- http://www.amazon.in/Building-Social-Applications-Gavin Bell dp/8184048327?tag=googinhydr18418-21
- https://onlinecourses.nptel.ac.in/noc16_cs07

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS404
PRINCIPLES OF SECURE CODING

Course Objective:

- Introduction to secure coding in different languages.

Unit 1: **08**

- **Introduction:** Need for secure systems- Proactive security development process Security principles to live by and threat modeling.

Unit 2: **08**

- **Secure Coding in C:** Character strings- String manipulation errors – String Vulnerabilities and exploits – Mitigation strategies for strings- Pointers – Mitigation strategies in pointer based vulnerabilities – Buffer Overflow based vulnerabilities.

Unit 3: **07**

- **Secure Coding in C++ and JAVA:** Dynamic memory management- Common errors in dynamic memory management- Memory managers- Double –free vulnerabilities –Integer security Mitigation strategies.

Unit 4: **07**

- **Database and Web Specific Input Issues:** Quoting the Input – Use of stored procedures- Building SQL statements securely-XSS related attacks and remedies.

References:

- Michael Howard, David LeBlanc, “Writing Secure Code”, Microsoft Press, 2nd Edition, 2003.
- Robert C. Seacord, “Secure Coding in C and C++”, Pearson Education, 2nd edition, 2013.

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS405P
INDUSTRIAL TRAINING/ON JOB TRAINING/ WORKSHOP

KALINGA UNIVERSITY
RAIPUR|INDIA

SEMESTER-V

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS501
STATISTICAL ANALYSIS WITH R

Course Objective:

- Introduction to programming concepts of R, probability Statistics

Unit 1: **08**

- **Probability& Statistics:** Introduction to Statistics- Descriptive Statistics, Summary Statistics Basic probability theory, Statistical Concepts (uni-variate and bi-variate sampling, distributions, re-sampling, statistical Inference, prediction error)

Unit 2: **08**

- Probability Distribution (Continuous and discrete- Normal, Bernoulli, Binomial, Negative binomial, Geometric and Poisson distribution), Bayes' Theorem, Central Limit theorem, Data Exploration & preparation, Concepts of Correlation, Regression, Covariance, Outliers etc.

Unit 3: **07**

- **R Programming:** Introduction & Installation of R, R Basics, Finding Help, Code Editors for R, Command Packages, Manipulating and Processing Data in R, Reading and Getting Data into R, Exporting Data from R, Data Objects-Data Types & Data Structure. Viewing Named Objects, Structure of Data Items, Manipulating and Processing Data in R (Creating, Accessing, Sorting data frames, Extracting, Combining, Merging, reshaping data frames), Control Structures, Functions in R (numeric, character, statistical)

Unit 4: **07**

- Working with objects, Viewing Objects within Objects, Constructing Data Objects, Building R Packages, Running and Manipulating Packages, Non parametric Tests- ANOVA, chi-Square, t-Test, U Test, Introduction to Graphical Analysis, Using Plots(Box Plots, Scatter plot, Pie Charts, Bar charts, Line Chart), Plotting variables, Designing Special Plots, Simple Liner Regression, Multiple Regression

References:

- Statistical Analysis with R for Dummies (For Dummies (Computers))
- A Handbook of Statistical Analyses Using R Brian S. Everitt and TorstenHothorn
- R Programming for Data Science Roger D Peng
- Data Analysis with R Fischetti, Tony
- Statistical Analysis of Network Data with R - Gabor Csardi Eric KolaczykCsardiKolaczyk)

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS502
DIGITAL FORENSICS

Course Objectives:

- To understand the various computer and cyber-crimes in the digital world.
- To understand a significance of digital forensics life cycle, underlying forensics rinciples and investigation process.
- To understand the importance of File system management with respect to computer forensics.
- To be able to identify the live data in case of any incident handling and application of appropriate tools and practices for the same.
- To develop the skills in application of various tools and investigation report writing with suitable evidences.
- To be able to identify the network and mobile related threats and recommendation of suitable forensics procedures for the same.

Course Outcomes:

- Identify and define the class for various computer and cyber-crimes in the digital world.
- Understand the need of digital forensic and the role of digital evidence.
- Understand and analyze the role of File systems in computer forensics.
- Demonstrate the incident response methodology with the best practices for incidence response with the application of forensics tools.
- Generate/Write the report on application of appropriate computer forensic tools for investigation of any computer security incident.
- Identify and investigate threats in network and mobile.

Unit 1: **08**

Prerequisite:

- **Computer Hardware:** Motherboard, CPU, Memory: RAM, Hard Disk Drive (HDD), Solid State Drive (SSD), Optical drive
- **Computer Networks:** Introduction CN Terminology: Router, Gateway, OSI and TCP/IP Layers
- **Operating Systems:** Role of OS in file management, Memory management utilities, Fundamentals of file systems used in Windows and Linux.

Introduction to Cybercrime and Computer-crime:

- **Definition and classification of cybercrimes**: Definition, Hacking, DoS Attacks, Trojan Attacks, Credit Card Frauds, Cyber Terrorism, Cyber Stalking.
- **Definition and classification of computer crimes:** Computer Viruses, Computer Worms.
- **Prevention of Cybercrime:** Steps that can be followed to prevent cybercrime, Hackers, Crackers, Phreakers.

Unit 2: **08**

Introduction to Digital Forensics and Digital Evidences:

- **Introduction to Digital Forensics:** Introduction to Digital Forensics and lifecycle, Principles of Digital Forensic.
- **Introduction to Digital Evidences:** Challenging Aspects of Digital Evidence, Scientific Evidence, Presenting Digital Evidence.
- **Digital Investigation Process Models**: Physical Model, Staircase Model, Evidence Flow Model.

Unit 3: **07**

Computer Forensics:

- **OS File Systems Review:** Windows Systems- FAT32 and NTFS, UNIX File Systems, MAC File Systems
- **Windows OS Artifacts:** Registry, Event Logs Memory Forensics : RAM Forensic Analysis, Creating a RAM Memory Image, Volatility framework, Extracting Information
- **Computer Forensic Tools:** Need of Computer Forensic Tools, Types of Computer Forensic Tools, Tasks performed by Computer Forensic Tools

Unit 4: **07**

Incident Response Management, Live Data Collection and Forensic Duplication:

- **Incidence Response Methodology:** Goals of Incident Response, Finding and Hiring IR Talent IR Process: Initial Response, Investigation, Remediation, Tracking of Significant Investigative Information.
- **Live Data Collection:** Live Data Collection on Microsoft Windows,
- **Forensic Duplication:** Forensic Duplicates as Admissible Evidence,
- **Forensic Duplication Tools:** Creating a Forensic evidence, Duplicate/Qualified Forensic Duplicate of a Hard Drive.

Forensic Tools and Report Writing:

- **Forensic Image Acquisition in Linux:** Acquire an Image with dd Tools, Acquire an Image with Forensic Formats, Preserve Digital Evidence with Cryptography, Image Acquisition over a Network, Acquire Removable Media Forensic
- **Investigation Report Writing:** Reporting Standards, Report Style and Formatting, Report Content and Organization.

References (Textbooks):

- Digital Forensics by Dr. Dhananjay R. Kalbande Dr. Nilakshi Jain, Wiley Publications, First Edition, 2019.
- Digital Evidence and Computer Crime by Eoghan Casey, Elsevier Academic Press, Third Edition, 2011.
- Incident Response & Computer Forensics by Jason T. Luttgens, Matthew Pepe and Kevin Mandia, McGraw-Hill Education, Third Edition (2014).
- Network Forensics : Tracking Hackers through Cyberspace by Sherri Davidoff and Jonathan Ham, Pearson Edu,2012
- Practical Mobile Forensic by Satish Bommisetty, Rohit Tamma, Heather Mahalik, PACKT publication, Open source publication, 2014 ISBN 978-1-78328-831-1 6. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh (Author), Andrew Case (Author), Jamie Levy (Author), AAron Walters (Author), Publisher :
- Wiley; 1st edition (3 October 2014),

References:

- Scene of the Cybercrime: Computer Forensics by Debra Littlejohn Shinder, Syngress Publication, First Edition, 2002.
- Digital Forensics with Open Source Tools by Cory Altheide and Harlan Carvey, Syngress Publication, First Edition, 2011.
- Practical Forensic Imaging Securing Digital Evidence with Linux Tools by Bruce Nikkel, NoStarch Press, San Francisco,(2016)
- Android Forensics: Investigation, Analysis, and Mobile Security for Google Android by Andrew Hogg, Elsevier Publication,2011
- Scene of the Cybercrime: Computer Forensics by Debra Littlejohn Shinder, Syngress Publication, First Edition, 2002.

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS503
SECURITY ARCHITECTURE AND ENGINEERING

Course Objectives:

- The course introduces to security engineering process and design.
- The students should get exposer to older and modern Security Models.
- They shall learn to Information Security, assess and mitigate the vulnerabilities.

Course Outcomes:

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models.
- Select controls based upon systems security requirements.
- Understand the security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution lements.
- Understand Modern Security Model and their use.

Unit 1: **08**

Secure System Design Principles:

- Secure System Design Principles, Integrated Systems, Journey Towards Zero Trust
- **Security Models:** Security Models, Biba Integrity Model Bell La Padula model, TCSEC, Common criteria.

Select System Security Controls:

- **The security controls, seven different types:** preventative(preventing unauthorized action on an information system), corrective(correcting an information system after an unauthorized action), detective(detecting unauthorized action), compensating(compensate an information system for a risk or vulnerability) , deterrent(controls that are used to deter would-be attackers), directive(controls that guide the subjects to comply with a security policy) and recovery(controls that are needed to recover from a disaster)

Unit 2: **08**

Assessment of Traditional Security Architectures:

- Assessment of Traditional Security Architectures, Distributed Systems, Assessment of Non-traditional Security Architectures Securing Embedded Devices, High Performance Systems

Unit 3: **07**

Security of Information System:

- Access control mechanisms, secure memory management, layering and virtualization which can be used to protect systems without disrupting the system.

Unit 4: **07**

Assess and mitigate the vulnerabilities:

- **Client security issues:** 'Applets', server security issues: Vulnerabilty mitigaton, database Security: Data breach, 'inference', 'aggregation' are other database risks,
- **Cryptographic systems:** DES, 3DES, AES, Blowfish, RSA, cloud-based systems, IoT and distributed systems of security architecture and knows how to mitigate them.

Modern Security Models:

- Time Based Security, Cyber Kill Chain, TBS + Kill Chain + MITRE ATT&CK, Architecting for Visibility & Detection, Architecting for Incident Response, Zero Trust Model

References:

- Securing Systems: Applied Security Architecture and Threat Models by Brook S E Schoenfield, CRC Press.
- Security Architecture How & Why by Author: Tom Madsen, Accenture, Denmark, River Publishers Series in Digital Security and Forensics
- Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition by Jan Killmeyer.
- Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architectsby Ed Moyle (Author), Diana Kelley (Author)

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS504
DATA AND CYBER SECURITY

Course Objectives:

- To understand the need of protecting sensitive and personal information
- Importance of Data rights and ownership
- Basic concepts cyber forensic investigation and evidence recovery

Unit 1: **08**

- **Data and Evidence Recovery-** Introduction to Deleted File Recovery, Formatted Partition Recovery, Data Recovery Tools, Data Recovery Procedures and Ethics, Preserve and safely handle original media, Document a "Chain of Custody", Complete time line analysis of computer files ased on file creation, file modification and file access, Recover Internet Usage Data, Recover Swap Files/ Temporary Files/Cache Files, Introduction to Encase Forensic Edition, Forensic Tool Kit (FTK) etc, Use computer forensics software tools to cross validate findings in computer evidence-related cases.

Unit 2: **08**

- **Cyber Crimes and Cyber Laws-** Introduction to IT laws & Cyber Crimes – Internet, hacking, Cracking, Viruses, Virus Attacks, Pornography, Software Piracy, Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits, and Cyber Security etc…

Unit 3: **07**

- **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

Unit 4: **07**

- **Cyber Security-** Introduction to Cyber Security, Implementing Hardware Based Security, Software Based Firewalls, Security Standards, Assessing Threat Levels, Forming an Incident Response Team, Reporting Cybercrime, Operating System Attacks, Application Attacks, Reverse Engineering & Cracking Techniques and Financial Frauds, Future scope of cyber security.

References:

- Network Security Bible- Eric Cole, Ronald Krutz, James W. Conley, Edition 2, Wiley India Pvt Ltd, 2010
- Network Security Essentials – William Stallings, Edition 4, Pearson Education, 2011
- Ulysess Black, "Internet Security Protocols: Protecting IP Traffic", Prentice
- Fundamentals of Network Security- E. Maiwald, McGraw- Hill, 2004
- Managing Information Security- John R. Vacca, Elsevier Inc, 2010
- Cryptography and Network Security-William Stallings
- Horowitz E., Sahani S., "Design and Analysis of Algorithms", 3rd Edition, University Press, 2002.

KALINGA UNIVERSITY
RAIPUR|INDIA

BVCS505P
INDUSTRIAL TRAINING/ON JOB TRAINING/ WORKSHOP

KALINGA UNIVERSITY
RAIPUR|INDIA

SEMESTER-06

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS601
BIOMETRICS SECURITY

Course Objective:

- To provide students with understanding of biometrics, biometric equipment and standards applied to security.

Course Outcomes:

- Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems.
- Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications

Unit 1: **08**

- **Biometrics-** Introduction- benefits of biometrics over traditional authentication systems -benefits of biometrics in identification systems-selecting a biometric for a system –Applications - Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems

Unit 2: **08**

- **Physiological Biometric Technologies:** Fingerprints - Technical description –characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan - Technical description - characteristics - weaknesses-deployment - Iris scan - Technical description – characteristics - strengths – weaknesses – deployment - Retina vascular pattern 39 GVPCE(A)

Unit 3: **07**

- **Technical description –** characteristics - strengths – weaknesses – deployment - Hand scan - Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics. Behavioral
- **Biometric Technologies:** Handprint Biometrics - DNA Biometrics. Signature and handwriting technology - Technical description – classification – keyboard / keystroke dynamics- Voice – data acquisition - feature extraction - characteristics - strengths – weaknesses-deployment.

Unit 4: **07**

- **Multi biometrics and multi factor biometrics -** two-factor authentication with passwords - tickets and tokens – executive decision - implementation plan

References:

- Samir Nanavathi, Michel Thieme, and Raj Nanavathi: “Biometrics -Identity verification in a network”, 1st Edition, Wiley Eastern, 2002.
- John Chirillo and Scott Blaul: “Implementing Biometric Security”, 1st Edition, Wiley Eastern Publication, 2005.
- John Berger: “Biometrics for Network Security”, 1st Edition, Prentice Hall, 2004.

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS602
CLOUD ARCHITECTURE AND SECURITY

Course Objective:

- Students will be familiarized with cloud applications, technologies and cloud security concepts.

Unit 1: **08**

- **Cloud Computing Fundamentals:** Cloud computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture.

Unit 2: **08**

- **Cloud Applications:** Technologies and the processes required when deploying web services- Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages- Development environments for service development; Amazon, Azure, Google App.

Unit 3: **07**

- **Securing the Cloud Security Concepts:** Confidentiality, privacy, integrity, authentication, non-repudiation, availability, access control, defence in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. E.g. User authentication in the cloud.

Unit 4: **07**

- **Virtualization Security:** Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloud provider can provide this- Virtualization System Security Issues: e.g. ESX and ESXi Security,
- **Cloud Security Management:** Security management in the cloud – security management standards- SaaS, PaaS, IaaS

References:

- Gautam Shroff, "Enterprise Cloud Computing Technology Architecture Applications", Cambridge University Press; 1 edition [ISBN: 978-0521137355], 2010.
- Toby Velte, Anthony Velte, Robert Elsenpeter, "Cloud Computing, A Practical Approach", Tata McGraw-Hill Osborne Media; 1 edition 22, [ISBN: 0071626948], 2009.
- Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Media; 1 edition, [ISBN: 0596802765], 2009.

KALINGA UNIVERSITY
RAIPUR INDIA

BVCS603
INTERNET OF THINGS (IOT)

Course Objective:

- Understand IoT Market perspective, Data and Knowledge Management and use of Devices in IoT Technology, Understanding State of the Art – IoT Architecture, Real World IoT Design Constraints, Industrial Automation and Commercial Building Automation in IoT.

Unit 1: **08**

- **Introduction to IoT:** Genesis of IoT, Digitization, Impact, Connected Roadways - Challenges safety, mobility, environment, Connected Factory -industry – mechanical assistance, mass production, electronics and control, integration, Smart Connected Buildings – heating, ventilation, HVAC systems, BAS System, BACNet, Smart Creatures, Convergence of IT and OT, IoT Challenges – Scale, Security, Privacy, Big data and data analytics. IoT Network Architecture and Design: - Drivers Behind New Network Architectures, Comparing IoT Architectures, A Simplified IoT Architecture, The Core IoT Functional Stack, IoT Data Management and Compute Stack

Unit 2: **08**

- **Engineering IoT Networks:** Smart Objects - Sensors, Actuators, and Smart Objects, Sensor Networks, Connecting Smart Objects: Communications Criteria IoT Access Technologies

Unit 3: **07**

- **IP as the IoT Network Layer:** Business Case for IP, Need for Optimization, Optimizing IP for IoT, Profiles and Compliances, Application Protocols for IoT: Transport Layer, IoT Application Transport Methods

Unit 4: **07**

- **Securing IoT:** A Brief History of OT Security, Common Challenges in OT Security, How IT and OT Security Practices and Systems Vary, Formal Risk Analysis Structures: OCTAVE and FAIR, The Phased Application of Security in an Operational Environment

References:

- David Hanes Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry “IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things”, Pearson, 2017
- Graham Meikle “The Internet of Things”, Polity Press, 2017,
- Vijay Madisetti and Arshdeep Bahga, “Internet of Things (A Hands-on-Approach)”, 1stEdition, VPT, 2014.

KALINGA UNIVERSITY
RAIPUR | INDIA

BVCS604
NETWORK SECURITY

Course Objectives:

- To understand security related to windows and wireless systems.
- To understand need of integrated security

Unit 1: **08**

- **Introduction of Computer network:** Topologies, Classification (LAN, MAN, WAN), OSI model, TCP / IP protocol-SMTP, FTP, telenet State of Network Security, Cyber Security, New approaches to cyber security, interfacing with the organization,
- **Information security principles-** Key principles of network security, Formal Processes, Risk Management, Calculating and managing risk, Information
- **System Security Management-** Access Control Attacks and threats-Malicious code

Unit 2: **08**

- **Windows Security-** Windows Security at the heart of the defense, Out-of-the-box Operating system hardening, Attacks against the Windows workstation, Linux Security-, Hardening Linux, Web Browser and Client risk, servers, , E-mail security-, Security Issues with DNS, DNS attacks, Server security.

Unit 3: **07**

- **VoIP, Wireless Security-** The Cellular phone network, Wireless transmission systems, Pervasive Wireless Data Network Technologies, IEEE Wireless LAN specification, Bluetooth, WAP,
- **Network segments-**Perimeter Defense, NAT, Basic architecture issues, Subnetting, switching and VLANs, Firewalls, Intrusion detection systems,

Unit 4: **07**

- **Integrated Cyber Security-** Validating your security- overview, Current state of penetration testing, Formal penetration testing methodology, Steps to explore a system, Data Protection, Endpoint security, Insider threats and data protection, Critical problems facing.

References:

- Network Security Bible- Eric Cole, Ronald Krutz, James W. Conley, Edition 2, Wiley India Pvt Ltd, 2010
- Network Security Essentials – William Stallings, Edition 4, Pearson Education, 2011
- Cryptography and Network Security: Principles and Practice-William Stallings, Edition 3, Pearson education, 2003
- Hacking Exposed- Network Security secrets and solutions, Joel Scambray, McGraw Hill, Edition 5, 2005
- Wireless Security : Models, Threats and Solutions- Randall K. Nichols, Panos C. Lekkas, McGraw Hill, Edition 1, 2001

KALINGA UNIVERSITY
RAIPUR|INDIA

BVCS605P
INDUSTRIAL TRAINING/ON JOB TRAINING/ WORKSHOP

KALINGA UNIVERSITY
RAIPUR|INDIA

RAIPUR|INDIA

KALINGA UNIVERSITY

KALINGA UNIVERSITY, KOTNI , NEAR MANTRALAYA, NAYA RAIPUR - 492101, CHHATTISGARH

CALL: +91-9907252100