KRISHNA UNIVERSITY

BOARD OF STUDIES (BoS) – DEPARTMENT OF COMPUTER SCIENCE

MINUTES OF THE BOARD OF STUDIES MEETING

Agenda:

To discuss and approve the proposed **curriculum, course structure and syllabus for I and II Semesters of the following PG programmes**:

- **Computer Applications**
- **Artificial Intelligence and Robotics**
- **Artificial Intelligence and Machine Learning**
- **Cybercrime and Cyber Security**
- **Data Analytics**

Members Present:

S. No.	Name	Designation	Role
1	Prof. R. Kiran Kumar	Dept. of Computer Science, Krishna University	Chairman
2	Smt. P. Durga Bhavani	HOD, Dept. of Computer Science, Nalanda Degree College, Vijayawada	Member
3	Kondapalli Ramkumar	HOD, Dept. of Electronics and Internet of Things, Nalanda Degree College, Vijayawada	Member
4	Bommareddy Sudheer Reddy	Lecturer, Dept. of Computer Science, Nalanda Degree College & PG Centre, Vijayawada	Member
5	Prof. P. Suresh Varma	Dept. of CSE, Adikavi Nannaya University, Rajahmundry	Member
6	Dr. M.H.M. Krishna Prasad	Dept. of CSE, JNTUK, Kakinada	Member
7	Prof. D. Lalitha Bhaskari	Dept. of CS & Systems Engineering, Andhra University	Member
8	Assoc. Prof. M. Babu Reddy	HOD, Dept. of Computer Science, Krishna University	Member

Proceedings

The meeting commenced with the Chairman welcoming all the members. The proposed curriculum and syllabi for the **I and II Semesters of the PG programmes** were placed before the Board for discussion and consideration.

The members discussed the proposed **course structure, syllabus , credits, teaching scheme, practical components, Course Outcomes and assessment pattern** of the above programmes. The members suggested that the curriculum should be practical, application-oriented and aligned with current technological and industry requirements.

Resolution

After detailed discussion, the **Board of Studies approved/recommended the proposed curriculum and syllabus for the I and II Semesters** of the following PG programmes:

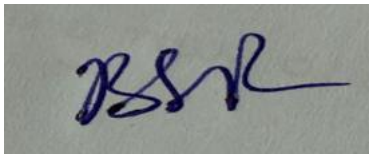
1. **Computer Applications**
2. **Artificial Intelligence and Robotics**
3. **Artificial Intelligence and Machine Learning**
4. **Cybercrime and Cyber Security**
5. **Data Analytics**

The Board recommended that the curriculum, syllabus, Course Outcomes, credits, teaching scheme and assessment pattern be finalized by incorporating the suggestions of the members and submitted to the competent academic authority for approval and implementation.

Conclusion

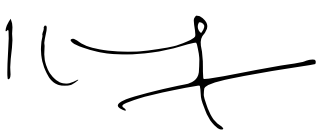
The Chairman thanked all the members for their valuable suggestions and active participation. The meeting concluded with a vote of thanks.











Model Syllabus for PG Diploma in Cyber Crime & Cyber Security

COURSE STRUCTURE

Year	Semester	Course	Title of the Course	No.of Hrs /Week	No. of Credits
I	I	1	Ethical Hacking	**3**	**3**
			Ethical Hacking Lab	**2**	**1**
	II	2	Digital Forensics and Incident Response	**3**	**3**
			Digital Forensics and Incident Response Lab	**2**	**1**

EMESTER-I

COURSE1: ETHICAL HACKING

Theory **Credits:3** **3hrs/week**

UNIT I: Fundamentals of Ethical Hacking

Introduction to Ethical Hacking •Introduction to Ethical Hacking •Information Gathering •Types of Hackers (White Hat, Black Hat, Grey Hat) •Ethical Hacking Methodology •Legal and Ethical Considerations • Cyber Security Standards and Best Practices

UNIT II: Foot printing and Reconnaissance

Foot printing and Scanning •Foot printing •Reconnaissance •Open Source Intelligence (OSINT) •Network Scanning • Port Scanning • Service Identification • Banner Grabbing (Introduction)

UNIT III: Vulnerability Assessment

Vulnerability Assessment •Vulnerability, Threat, and Risk • Vulnerability Assessment Process •Security Misconfigurations • Introduction to CVE and CVSS • Basic Security Auditing

UNIT IV: Ethical Hacking Tools

Security Tools • Kali Linux Overview • Nmap • Wire shark • Burp Suite Community Edition • Nikto (Introduction) • OWASP ZAP (Introduction)

UNIT V: Penetration Testing and Reporting

Reporting and Defensive Practices •Penetration Testing Life Cycle •Documentation and Report Writing •Responsible Disclosure •Security Recommendations •Cyber Hygiene •Case Studies of Cyber Incidents

TEXTBOOKS:

1. **Georgia Weidman–*Penetration Testing:*** *A Hands-On Introduction to Hacking*, No Starch Press.
2. **Michael T .Simpson & Scott T .Hoffman–***Hands-On Ethical Hacking and Network Defense*, Cengage Learning**.**

COURSE 1: ETHICAL HACKING

Practical **Credits: 2** **2hrs/week**

Experiments List

1. Install and Explore Kali Linux

2. Basic Network Scanning Using Nmap

3. Network Traffic Analysis Using Wire shark

4. Vulnerability Scanning Using OWASPZAP(or Nikto)

5. Prepare a Basic Security Assessment Report

SEMESTER-II

COURSE 2: DIGITAL FORENSICS

Theory **Credits:3** **3hrs/week**

UNIT I: Computer Forensics and Investigations
Computer Forensics and Investigations Computer Forensics: Introduction, Investigation Process, Systematic Approach. Data Recovery Work stations and Software. Investigator's Office and Laboratory: Forensics Lab Certification Requirements, Physical Requirements for a Computer Forensics Lab, Basic Forensic Workstation.

UNIT II: Data Acquisition Data Acquisition Storage Formats for Digital Evidence, Acquisition Methods, Contingency Planning for Image Acquisitions, Validating Data Acquisition, RAID Data Acquisition, Acquisition Tools, Remote Network Acquisition Tools.

UNIT III: Digital Evidence Collection and Processing Identifying, Processing Crime and Incident Scenes Digital Evidence: Search, Collection, Preparation, Isolation, Storage, Process, Verification, Documentation, Report, Archiving. Computer Forensics Tools: Evaluating Needs, Hardware & Software Tools.

UNIT IV: Forensic Analysis and Validation Validating and Testing Forensics Forensic Analysis of Soft ware and Validation: Data Analysis, Hiding techniques, Carving, Compression; Graphics file: Recognition, Location, Recovery, Live Memory Forensics (RAM)

UNIT V: Email Forensics and Investigation
Introduction to Email Investigation E-mail Investigations, Role of E-mail in Investigations, Role of Client and Server in E-mail, Email Crimes and Violations, E-mail Servers, Special E-mail Forensics Tools.

TEXTBOOK:

1. **Bill Nelson, Amelia Phillips & Christopher Steuart**–*Guide to Computer Forensics and Investigations*, 6th Edition, Cengage Learning.
1.**EC-Council**–*Computer Forensics: Investigating Network Intrusions and Cyber Crime*, Cengage Learning.

COURSE 2: DIGITAL FORENSICS

Practical **Credits:2** **2hrs/week**

List of Experiments

1. Disk Imaging(2types)
2. FTK Imager
3. Cyber check suite and other forensic tools from CDAC
4. Forensic Imaging of Virtual Machines
5. Live Acquisition
6. Live Incident Response
7. Live Memory Forensics(Volatility framework)
8. Scalpel, Autopsy
9. Network Minor
10. Comparison of various software.

KRISHNA UNIVERSITY

P.G. Diploma Model Paper for Core Subjects

Semester: I

Paper Title: Ethical Hacking

Time : 3hrs **Max. Marks:70**

Section –A (20 Marks)

Answer any *Five* questions. All questions carry equal marks. **5X4=20M**

1. Define Ethical Hacking
2) Write about types of Hackers
3) Define foot printing
4) Define Port scanning
5) Define security auditing
6) Define Nmap
7) Explain SPZAP
8) Define Cyber Hygiene

Section–B (50Marks)

Answer ALL Questions. All questions carry equal marks. **5 X 10 = 50M**

9 a). Explain about Ethical Hacking Methodology

OR

b). Explain about Legal and Ethical Considerations

10 a) .Explain about Open Source Intelligence (OSIN)

OR

b). Explain about Reconnaissance

11 a) Explain about Vulnerability Assessment

OR

b) Explain about Vulnerability Assessment Process

12 a) Explain about various security tools

OR

b) . Explain about Nikto

13 a) . Explain about Penetration Testing Life Cycle

OR

b) Explain about Security Recommendations

KRISHNA UNIVERSITY

P.G. Diploma Model Paper for Core Subjects

Semester: II

Paper Title: DIGITAL FORENSICS

Time : 3hrs **Max. Marks:70**

Section –A (20 Marks)

Answer any *Five* questions. All questions carry equal marks. 5X4=20M

1. List the steps involved in an investigation process.
2. Define RAID.
3. What is documentation in evidence processing?
4. What are the common storage formats for digital evidence?
5. What is meant by isolation of evidence?
6. Name any two data hiding techniques
7. What is the role of an email server?
8. Define email forensics.

Section–B (50Marks)

Answer ALL Questions. All questions carry equal marks. 5 X 10 = 50M

9. a) Explain the systematic approach to computer forensics investigations.

OR

b) Discuss the physical requirements for setting up a computer forensics lab

10. a) Explain the process of validating data acquisition.

OR

b) Explain the different storage formats used for digital evidence.

11. a) Explain the steps involved in identifying and processing a crime scene

OR

b) Explain the hardware and software tools used in computer forensics

12. a), Explain the concept of data carving and compression in forensic analysis

OR

b) Explain the recognition, location and recovery of graphics files

13. a) Explain the role of email in investigations with the email investigation process.

OR

b) Discuss the various email crimes and violations.