:

KRISHNA UNIVERSITY

BOARD OF STUDIES (BoS) – DEPARTMENT OF COMPUTER SCIENCE

MINUTES OF THE BOARD OF STUDIES MEETING

Agenda:

Framing and Approval of Curriculum and Syllabus for I, II, III and IV Semesters of Diploma Programmes

- Diploma in Computer Applications
- Diploma in Artificial Intelligence and Robotics
- Diploma in Artificial Intelligence and Machine Learning
- Diploma in Cybercrime and Cyber Security
- Diploma in 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 proposal for introducing the above **Diploma programmes** was placed before the Board for detailed discussion.

The members discussed the proposed **curriculum, syllabus course structure, credits, teaching scheme, practical components, Course Outcomes, and assessment pattern** of the five Diploma programmes.

The Board members emphasized the importance of providing students with **practical, skill-oriented, and industry-relevant knowledge** in emerging areas of Computer Applications, Artificial Intelligence, Robotics, Machine Learning, Cyber Security, Cybercrime, and Data Analytics.

The members also suggested incorporating adequate **laboratory work, hands-on training, project-based learning, and application-oriented components** to enhance the employability and technical skills of students.

Resolution

After detailed discussion, the **Board of Studies approved/recommended the introduction of the following Diploma programmes**:

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

The Board recommended that the proposed **curriculum and syllabus , course structure, credits, Course Outcomes, teaching scheme, practical components, and assessment pattern** be finalized by incorporating the suggestions given by the members.

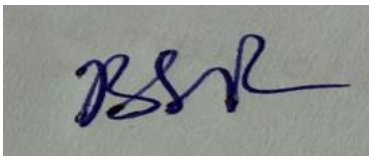
The Board further recommended that the finalized curriculum and syllabi be submitted to the **competent academic authority of Krishna University** for approval and implementation.

Conclusion

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

Chairman, Board of Studies
Prof. R. Kiran Kumar
Signature: _____











Model Syllabus for Diploma in Cyber Crime & Cyber Security

COURSESTRUCTURE

Year	Semester	Course	Title of the Course	No.of Hrs /Week	No. of Credits
1	I	1	Computer Network and Security	3	3
			Computer Network and Security Lab	2	1
	II	2	Introduction to Cyber Security	3	3
			Introduction to Cyber Security Lab	2	1
2	III	3	Information Security	3	3
			Information Security Lab	2	1
	IV	4	Cryptography	3	3
			Cryptography Lab	2	1

SEMESTER-I

COURSE1:Computer Networks and Security

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

UNIT I: Fundamentals of Computer Networks

Introduction to Computer Networks •Introduction to Computer Networks • Types of Computer Networks (LAN, MAN, WAN, PAN) • Network Topologies • Network Devices: Hub, Switch, Router, Modem, Access Point, Gateway •Transmission Media (Guided and Unguided)

UNIT II: Network Models and Communication Protocols

Network Models and Protocols •OSI Reference Model •TCP/IP Model •Comparison of OSI and TCP/IP Models •Data Encapsulation • Network Protocols • MAC Address and IP Address

UNIT III: IP Addressing and Network Services

IP Addressing and Internet Services • IPv4 Addressing •Public and Private IP Addresses • Subnet Mask (Basic Concepts) •DNS (Domain Name System) •DHCP (Dynamic Host Configuration Protocol) NAT(Network Address Translation)

UNIT IV: Internet Protocols and Communication Security

Internet Protocols and Network Security • HTTP and HTTPS • FTP and SFTP • SMTP, POP3, and

IMAP •SS Hand Telnet •VPN (Introduction) •Common Port Numbers: 20,21,22,23,25,53,80,110,

143,443

UNIT V: Network Security Fundamentals

Network Security Fundamentals •Firewalls •Antivirus Software • Intrusion Detection System (IDS) • Intrusion Prevention System(IPS) • Proxy Server •Secure Wi-Fi Practices • Basic Network Trouble shooting

TEXTBOOK:

1. **William Stallings**–*Network Security Essentials: Applications and Standards*, 7th Edition, Pearson.
2. **Behrouz A.Forouzan–*Data Communications and Networking*, 5th Edition, McGrawHill.**

SEMESTER-I

COURSE1: Computer Networks and Security

Practical **Credits: 1** **2hrs/week**

List of Experiments:

1. Identify networking devices and create simple LAN in Cisco Packet Tracer.
2. Study OSI/TCP-IP models using Packet Tracer simulations.
3. Configure IPv4 addressing and test connectivity with ping.
4. Capture HTTP, DNS, and ICMP traffic using Wire shark.
5. Configure Windows Firewall and perform basic network trouble shooting.

SEMESTER-II

COURSE2: INTRODUCTION TO CYBERSECURITY

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

Unit 1.Cyber space and Internet Fundamentals:

Cyber Space Cyber space: Definition, Architecture and Regulation ; Overview of Web technology; Internet : Advent of internet, World Wide Web, Internet infrastructure for data transfer and governance.

Unit 2.Cyber Crimes and Cyber Threats:

Cyber Crimes History & Development, Classification of cyber crimes-Cyber Terrorism, Cyber Threats, Cyber Stalking, Pornography, Child Pornography, Hacking, Viruses, Worms, Trojans, Malware, Scare ware, Adware, Command and Control, Botnet, Cyber Trespass, Cyber Theft, Cyber Fraud, Password Cracking, Malware, Hunk Mail, Stegano graphy, Cyber Terrorism, Cyber Warfare, Phishing. Impact of cybercrimes - Effect of cybercrimes on society, Cybercrimes against people, property, business and nation. Evaluation of cyber crimes, Definition of cybercriminals, Trends in cyber crime across India & the world.

Unit 3.Cyber Security Fundamentals:

Need and Importance, Overview, Cyber security Domains and Growth, The Cyber security Cube-Three Dimensions, CIA Triad, Confidentiality, The Principle of Confidentiality, Protecting Data Privacy, Controlling Access-Laws and Liability; Data Integrity: Principle, Need and Integrity Checks, Availability, The Principle of Availability, Ensuring Availability.

Unit 4. Social Media Security:

Social Media and Security Social networks: Introduction and Overview, Opportunities, Pitfalls ;Social media: Types, Platforms, Monitoring, Hash tag, Viral content, Marketing, Privacy, Challenges, Security issues, Flagging and reporting of in appropriate content, Laws regarding posting of inappropriate content, Best practices, Case studies.

Unit 5. E-Commerce and Digital Payment Security:

E-Commerce and Digital Payments E- Commerce: Definition, Components, Security Elements, Threats, Security best practices. Digital payments: Introduction, Components, Modes (Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar enabled payments),Frauds and Preventive measures. RBI guide lines on digital payments and customer protection in unauthorized banking transactions. Relevant provisions of Payment Settlement Act, 2007.

Text Books:

1. Cyber Crime Impact in the New Millennium, by R.C Mishra, Auther Press.Edition2010.

2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina God bole, Wiley India Pvt. Ltd. (First Edition, 2011) 3

3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by HenryA. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)

4. Electronic Commerce by Elias M.Awad, Prentice Hall of India Pvt Ltd.

5. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.

6. Network Security Bible, Eric Cole, Ronald Krutz, James W.Conley, 2nd Edition, Wiley India Pvt. Ltd. 7. Fundamentals of Network Security by E. Maiwald, McGraw Hill.

SEMESTER-II

COURSE 2 : Introduction to Cyber Security

Practical **Credits:1** **2hrs/week**

List of Experiments:

1. V M Ware installations
2. Configuring security settings in Mobile Wallets and UPIs
3. Applying patches, fixing vulnerability(experiments)
4. Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User).
5. Setting and configuring two factor authentication in the Mobile phone.
6. Security patch management and updates in Computer and Mobiles.
7. Managing Application permissions in Mobile phone.
8. Installation and configuration of computer Anti-virus.
9. Installation and configuration of Computer Host Fire wall.
10. Wi-Fi security management in computer and mobile.
11. Basic check list, privacy and security settings for popular social media platforms.
12. Reporting and redressal mechanism for violations and misuse of social media platforms.
13. Windows memory acquisition using Dump it Tool.

SEMESTER-III COURSE 3:

INFORMATION SECURITY

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

UNIT I: Introduction to Information Security-Information Security concepts, CIA Triad, Information Assets, Threats, Vulnerabilities, Risk Assessment, Security Policies, ISO/IEC27001 overview.

UNIT II: Access Control and Authentication

Identification, Authentication, Authorization, Access Control Models, Password Security, Multi-Factor Authentication (MFA), Biometrics.

UNIT III: Security Operations Center(SOC)

Introduction to SOC, Purpose and Importance, SOC Architecture, SOC Team Roles(L1, L2, L3 Analysts, Incident Responder, Threat Hunter, SOC Manager), Security Monitoring, Log Management, SIEM Basics, Threat Intelligence, Indicators of Compromise (IoCs), Alert Triage, Incident Detection, Security Reporting, Career Opportunities.

UNIT IV: Network and Web Security

Firewalls, IDS, IPS, VPN, HTTPS, Email Security, Wireless Security, Malware Protection, Secure Web Practices.

UNIT V: Incident Response and Security Management

Incident Response Lifecycle, Business Continuity, Disaster Recovery, Security Auditing, Digital Evidence, Cyber Laws, Future Trends in Information Security.

Textbooks:

1. Michael E.Whitman &Herbert J.Mattord- Principles of Information Security
2. Charles P.Pfleeger- Security in Computing
3. Nina God bole & Sunit Belapure-Cyber Security
4. Chris Sanders-Blue Team Field Manual(Reference)

EC- Council – Certified SOC Analyst (CSA) Study Guide (Reference)

SEMESTER-III

COURSE 3: INFORMATION SECURITY

Practical **Credits:1** **2hrs/week**

List of Experiments:

1. Configure user accounts and password policies
2. Analyze Windows Event Viewer logs.
3. Explore Linux log files.
4. Perform basic network traffic analysis using Wire shark.
5. Study SIEM dashboards(demo)
6. Identify Indicators of Compromise (IoCs)
7. Prepare a basic incident response report
8. Configure Windows Fire wall and review security events

SEMESTER-IV

COURSE 4: CRYPTOGRAPHY

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

UNIT I: Fundamentals of Cryptography

Introduction to Cryptography • Introduction to Cryptography • Need for Cryptography • History of Cryptography • Plaintext and Cipher text • Encryption • Decryption • Cryptographic Goals: Confidentiality, Integrity, Authentication, Non-Repudiation

UNIT II: Classical Cryptographic Techniques

Classical Cryptography •Caesar Cipher • Mono alphabetic Cipher • Play fair Cipher • Vigenere Cipher • Rail Fence Cipher • Transposition Cipher

UNIT III: Modern Crypto graphic Algorithms

Modern Cryptography •Symmetric Key Cryptography •Asymmetric Key Cryptography • AES (Introduction) • DES (Introduction) • RSA (Introduction) • Key Management

UNIT IV: Hashing and Authentication

Hashing and Authentication • Hash Functions • MD5 •SHA Family •Message Authentication Codes (MAC) •Digital Signatures •Digital Certificates • Public Key Infrastructure (PKI)

UNIT V: Secure Communication and Applications Secure Communication • SSL /TLS • HTTPS • VPN •Email Security • Secure File Transfer • Applications of Cryptography • Future Trends in Cryptography

TEXTBOOK:

1. **William Stallings**–*Cryptography and Network Security: Principles and Practice*, 8th Edition, Pearson.
2. **Behrouz A.Forouzan**–*Cryptography and Network Security*, Mc Graw Hill Education.

SEMESTER-IV

COURSE4: CRYPTOGRAPHY

Practical	**Credits:1**	**2hrs/week**

Details of Lab/Practical/ Experiments/Tutorials syllabus:

1. Demonstrate plaintext, cipher text, encryption and decryption concepts.
2. Implement Caesar, Play fair and Vigenere ciphers.
3. Demonstrate AES encryption and generate RSA public/private keys.
4. Generate SHA-256 hashes, verify file integrity and demonstrate digital signatures.
5. Examine SSL /TLS certificates, verify HTTPS communication and develop a simple file encryption/decryption mini project.

KRISHNAUNIVERSITY

Diploma (CC&CB) Examinations Model Paper for Core Subjects

Semester: I

Paper Title: Computer Networks and Security

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

Section–A(20Marks)

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

1. Types of Computer Networks.
2. Explain about Switch, Router?
3. Describe Data Encapsulation.
4. What is NAT?
5. Explain about POP3?
6. Differences between OSI and TCP/IP models.
7. Define IP Addressing?
8. Explain Secure Wi-Fi Practices.

Section–B(50Marks)

Answer ALL Questions. All questions carry equal marks. **5X10 =50M**

9. a) Explain about Network Topologies.

OR

b) Discuss about Transmission Media (Guided and Unguided).

10. a) Explain about the OSI ReferenceModel.

OR

b) Explain about Network Protocols.

11. a) Explain about IPv4 Addressing.

OR

b) Write about DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol).

12. a) Explain about HTTP, FTP and SMTP.

OR

b) What is VPN? Explain about Common Port Numbers.

13. a) Briefly explain about Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

OR

b) Explain about Firewalls, Antivirus Software and Proxy Server.

KRISHNAUNIVERSITY

Diploma (CC&CB) Examinations Model Paper for Core Subjects

Semester: II

Paper Title: INTRODUCTION TO CYBER SECURITY

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

Section–A(20Marks)

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

1. Explain about Explain about Switch, Router.
2. Explain about Cyber Terrorism?
3. Describe Cyber Fraud.
4. What is Flagging and reporting of inappropriate content?
5. Explain about Data Integrity?
6. Overview of Web technology.
7. Define e-Wallets?
8. Explain about RBI guidelines on digital payments .

Section–B(50Marks)

Answer ALL Questions. All questions carry equal marks. **5X10 =50M**

9. a) Explain about Cyber Space Architecture.

OR

b) Discuss about Internet infrastructure for data transfer and governance.

10. a) Classification of Cyber Crimes.

OR

b) Explain about Impact of Cyber Crimes.

11. a) Explain about Cyber Security Cube 3-Dimensions.

OR

b) Write about CIA Trading.

12. a) Write about Social Media Types.

OR

b) What are the Laws regarding posting of inappropriate content.

13. a) Briefly explain about relevant provisions of Payment Settlement Act, 2007.

OR

b) Explain about Digital Payments.

KRISHNAUNIVERSITY

Diploma (CC&CB) Examinations Model Paper for Core Subjects

Semester: III

Paper Title: INFORMATIONSECURITY

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

Section–A(20Marks)

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

1. Define Information Security.
2. Explain about ISO/IEC27001?
3. What is meant by Authentication?
4. What is Biometrics?
5. Explain about Log management?
6. Overview of Malware Protection.
7. Define SecurityAuditing?
8. Explain about Disaster Recovery.

Section–B(50Marks)

Answer ALL Questions. All questions carry equal marks. **5X10 =50M**

9. a) Explain about Information Security concepts.

OR

b) Discuss about Security Policies.

10. a) Explain about Multi-Factor Authentication (MFA).

OR

b) What are the Access Control Models?

11. a) Explain about Security Operations Center (SOC) Architecture.

OR

b) Write about SIEM basics.

12. a) Write about Firewalls, IDS and IPS.

OR

b) Write about e-mail security.

13. a) Briefly explain about Digital Evidence.

OR

b) Explain about Cyber Laws.

KRISHNAUNIVERSITY

Diploma (CC&CB) Examinations Model Paper for Core Subjects

Semester: IV

Paper Title: CRYPTOGRAPHY

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

Section–A(20Marks)

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

1. Differences between Plaintext and Cipher text.
2. Define Encryption?
3. What is meant by Classical Cryptography?
4. What is Key Management?
5. Explain about AES?
6. Describe about Digital Certificates.
7. Define Secure File Transfer?
8. Future Trends in Cryptography.

Section–B(50Marks)

Answer ALL Questions. All questions carry equal marks. **5X10 =50M**

9. a) What is Cryptography, Need for Cryptography?

OR

b) Discuss about Cryptographic Goals.

10. a) Explain about Caesar Cipher, Mono alphabetic Cipher.

OR

b) What are the Rail Fence Cipher, Transposition Cipher?

11. a) Explain about Cryptography Types.

OR

b) Write about RSA Algorithm.

12. a) Write about Hash Functions.

OR

b) Write about Digital Signatures.

13. a) Briefly explain about the applications of cryptography.

OR

b) Explain about HTTPS and VPN.