DEPARTMENT OF AQUACULTURE

M E S ASMABI COLLEGE, P. VEMBALLUR

CERTIFICATE COURSE IN

CYBERSECURITY AND CYBERETHICS

COURSE SYLLABUS

Module 1: Introduction to Cybersecurity (7 hours)

Topics:

- Overview of Cybersecurity
  - Definition and importance
  - Historical context and evolution of cybersecurity
- Common Cyber Threats and Vulnerabilities
  - Types of cyber attacks (phishing, malware, ransomware, etc.)
  - Common vulnerabilities in systems and networks
- Basics of Cybersecurity Measures
  - Firewalls, antivirus software, encryption
  - Introduction to intrusion detection and prevention systems

Learning Outcomes:

- Understand the fundamentals of cybersecurity and its significance.
- Identify common types of cyber threats and vulnerabilities.
- Gain basic knowledge of security measures to protect information systems.

Module 2: Network Security (7 hours)

Topics:

- Fundamentals of Networking
  - Basic network concepts and architecture
  - Network protocols and communication
- Securing Network Infrastructure
  - Network security devices (routers, switches, firewalls)
  - Network access control
- Wireless Network Security
  - Wi-Fi security protocols (WEP, WPA, WPA2)
  - Securing wireless networks

Learning Outcomes:

- Understand basic networking concepts.
- Learn how to secure network infrastructure.
- Gain knowledge of wireless network security measures.

Module 3: Cybersecurity Tools and Practices (7 hours)

Topics:

- Cybersecurity Tools
  - Overview of essential tools (antivirus, encryption, VPNs)
  - Introduction to SIEM (Security Information and Event Management) systems
- Best Practices in Cybersecurity
  - Strong passwords and authentication methods
  - Regular software updates and patch management
- Incident Response and Management
  - Steps in handling a security breach
  - Incident response planning and execution

Learning Outcomes:

- Familiarize with key cybersecurity tools and their functions.
- Implement best practices for maintaining security.
- Develop skills in incident response and management.

Module 4: Introduction to Cyberethics (7 hours)

Topics:

- Definition and Importance of Cyberethics
  - Ethical principles in the digital world
  - The role of ethics in cybersecurity
- Privacy and Data Protection
  - Understanding privacy rights and regulations (e.g., GDPR)
  - Ethical handling of personal and sensitive data
- Intellectual Property and Digital Rights
  - Copyright, trademarks, and digital rights management
  - Ethical issues related to intellectual property in cyberspace

Learning Outcomes:

- Understand the principles of cyberethics and their importance.
- Learn about privacy rights and data protection regulations.
- Gain insights into intellectual property and digital rights in the context of cybersecurity.

Module 5: Legal and Regulatory Aspects of Cybersecurity (7 hours)

Topics:

- Cyber Laws and Regulations
  - Overview of key cyber laws and regulations (e.g., CCPA, HIPAA)
  - Compliance requirements for businesses and individuals
- Ethical Hacking and Penetration Testing
  - Legal and ethical considerations of ethical hacking

    - Introduction to penetration testing methodologies
- Future Trends in Cybersecurity and Cyberethics
    - Emerging threats and technologies
    - The evolving landscape of cyber laws and ethics

Learning Outcomes:

- Gain knowledge of important cyber laws and regulatory requirements.
- Understand the legal and ethical aspects of ethical hacking.
- Stay informed about future trends in cybersecurity and cyberethics.

Sd/ Course Coordinator Sd/ Head of the Department