## Format for the Syllabus of Vocational Course

**Paper Name – Cyber Security Vocational Course** **VOC160**

**Paper Code –**

**Course Objectives** – This course explores the most critical elements of cybersecurity. It covers systems, applications, networks, cryptography, and OS security. This fully online course provides students with fundamental knowledge and hands-on experience in cybersecurity. An integral part of the program is the customized labs, which will be provided at every student's desk through our virtual labs.

**Course Content –**

1. Introduction to Cybersecurity
    a. Intro to Cyber Security
        i. Basic security concepts: Confidentiality, Integrity, Availability
        ii. Importance of Cyber security
    b. Cyber Security vs. Cyber Crime
        i. Types of modern Cyber threats: malware, phishing, MITM attacks, Dos/DDoS
    c. Introduction to MITRE TTPs and Cyber Kill Chain
    d. Discussion on real-world cyber attacks
        i. Some real-world Cyber Fraud and Cyber Crime Cases
2. Cyber Threat Landscape
    a. Types of Malware: Viruses, Worms, Trojans, Ransomware
    b. Phishing Attacks: Techniques and Prevention
    c. Social Engineering: Recognizing and Responding to Social Engineering Attempts
    d. Various Cyber Fraud/Cyber Crime Methods
        i. OTP fraud, Deepfake based Frauds, Voice Cloning, Cyber Bullying, Cyber Extortion
        ii. Various Cyber Crime Reporting numbers and websites.
    e. Cyber warfare concept and concerns
    f. Outlines of IT Act 2008, and DPDP Act 2023
3. Data Protection and Encryption
    a. Importance of Data Backup and Recovery
    b. Data Encryption: Understanding Encryption Techniques
    c. Securing Online Transactions and Financial Information
4. Securing Digital Devices and Networks
    a. Device Security: Protecting Computers, Smartphones, and Tablets
    b. Network Security Basics: Wi-Fi Security, Firewalls, etc.
    c. Secure Web Browsing Practices

d. Understanding https, SSL certificate, Creating your own SSL certificates and its limitations, the need for PKI

5. Application security
    a. Secure coding principles
    b. Common coding vulnerabilities: SQL Injection, XXS, CSRF etc.
    c. Intro to OWASP Top 10, Burp Suite
6. OS protection Fundamentals
    a. Understanding User accounts (Linux and Windows)
    b. File and Directory Permissions
    c. Antivirus and it's usage.
    d. Application and Execution Control
    e. Update and Patching
    f. Understanding threats to DNS hijacking, DNS poisoning and problem of using public Wi-Fi or public open networks

**Total weightage of Theory** - 40% of marks, 15 hours (1 Credit)

**Total weightage of Practical** - 60% of marks, 30 hours (Lecture for conducting practical sessions) + 30 hours (Virtual Labs for students for hands-on experience) (2 Credit)

**Practicum Work** - At least 4 activities should be given. Two activities will be selected by the students for their assessment of Practicum Work

**Practical sessions will be in conjunction with the above modules. Some sample sessions –**

1. Understanding packet capturing and understanding use of Wireshark
2. Understanding File Permissions in Linux and in Windows
3. Understanding creating public/private keypair, creating a digital certificate, analyzing digital certificates of websites
4. Examples of Buffer overflow
5. Example examples of privilege escalation to obtain a root shell.
6. DVWA based web security exercises.
7. Example on ARP protocol and ARP poisoning
8. Example on setting up Firewall on Linux and Windows

**Learning Outcomes –**

- Introduces real-time cybersecurity techniques and methods within the context of protocol suites, highlighting the necessity for network security solutions.
- Deepens understanding of the technical foundations of cyberspace and related cyber issues.
- Equips learners with foundational knowledge of common cybersecurity threats, vulnerabilities, and risks.

- Teaches the configuration and management of essential security tools such as firewalls, intrusion detection systems (IDS), and antivirus software to protect systems from malicious attacks.
- Encourages ongoing professional development and staying current with evolving cybersecurity trends and best practices through certifications, training programs, and participation in cybersecurity communities.

**Job Prospects –**

**Skill Partner –**

**Suggested Reading –**