Four Year Under Graduate Programme (FYUGP)

As per provisions of NEP-2020

Vinoba Bhave University Hazaribag

Subject Name: **Cyber Defense**

Under

Introductory Vocational Studies

Subject Code: -**IVS-1B**

To be implemented from the Academic Year **2022-23**

(From session 2022-26)

Syllabus for Semester -II

Members of the Board of Study

Dr. M. Alam (Dean, Commerce)	Dr. R. N. Sinha (Dean, Science)	Dr. P. C. Deogharia (Dean, Soc. Science))	Prof. M. K. Singh (Dean, Humanities)
Dr. Indrajit Kumar (NEP-Coordinator)	Dr. R. K. Dwivedi (HOD, Mathematics)	Dr. A. K. Saha (Director, UCET)	Principal (Govt. ITI, H.Bag)

SEMESTER II Cyber Defense 1 Paper

Introductory Vocational Studies

Subject Code: IVS-1B

(Credits: Theory-03, Practicals-0)

The paper '**Cyber Defense**' is under Introductory Vocational Studies. It is to be studied by the Students of all the four disciplinary areas viz. Natural Sciences, Humanities, Social Sciences and Commerce.

Marks: 25 (5 Attendance & others + 20 SIE: 1.5Hr) + 75 (ESE: 3Hrs) = 100	Pass Marks: Th (MSE + ESE) = 40

Instruction to Question Setter

<u>Semester Internal Examination (SIE 20+5=25 marks):</u>

The Semester Internal Examination shall have two components. (a) One Semester Internal Assessment Written Test (SIA) of 20 Mark (b) Class Attendance Score (CAS) including the behaviour of the student towards teachers and other students of the College of 5 marks. The Semester Internal Assessment Written Test will be based on the practical portion of the syllabus.

<u>End Semester Examination (ESE 75 marks):</u>

It will be OMR sheet-based examination consisting of 30 Multiple-Choice Questions (MCQ), each question carrying 2 ½ marks. All the questions are to be answered. There will be no negative marking. The allotted time will be 1 ½ hours.

Theory: 45 Lectures

Course Content:

Module	Module Name	Module Content	Learning Outcomes
Module I	**Introduction to Cyber security**	Defining Cyberspace and Overview of Computer and Web-technology, Architecture of cyberspace, Communication and web technology, Internet, World wide web, Advent of internet, Internet infrastructure for data transfer and governance, Internet society, Regulation of cyberspace, Concept of cybersecurity, Issues and challenges of cybersecurity.	After completion of this module, students would be able to understand the concept of Cybersecurity and issues and challenges associated with it.

Module	Module Name	Module Content	Learning Outcomes
Module II	**Cybercrime and Cyber law**	Classification of cybercrimes, Common cybercrimes- cybercrime targeting computers and mobiles, cybercrime against women and children, financial frauds, social engineering attacks, malware and ransomware attacks, zero day and zero click attacks, Cybercriminals modus-operandi, Reporting of cybercrimes, Remedial and mitigation measures, Legal perspective of cybercrime, IT Act 2000 and its amendments, Cybercrime and offenses, Organizations dealing with Cybercrime and Cyber security in India, Case studies.	Students, at the end of this module, should be able to understand the cybercrimes, their nature, legal remedies and as to how to report the crimes through available platforms and procedures.

Practical	1. Checklist for reporting cybercrime at Cybercrime Police Station. 2. Checklist for reporting cybercrime online. 3. Reporting phishing emails. 4. Demonstration of email phishing attack and preventive measures.

Module	Module Name	Module Content	Learning Outcomes
Module III	**Social Media Overview and Security**	Introduction to Social networks. Types of Social-media, social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social network, Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices for the use of Social media, Case studies.	On completion of this module, students should be able to appreciate various privacy and security concerns on online Social media and understand their porting procedure of inappropriate content, underlying legal aspects and best practices for the use of Social media platforms.

Practical	1. Basic checklist, privacy and security settings for popular Social media platforms. 2. Reporting and redressal mechanism for violations and misuse of Social media platforms

Module	Module Name	Module Content	Learning Outcomes
Module IV	**Digital Devices Security, Tools & Technologies for Cyber Security**	End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third party software, Device security policy, Cyber Security best practices, Significance of host firewall and Ant-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.	Students, after completion of this module will be able to understand the basic security aspects related to Computer and Mobiles. They will be able to use basic tools and technologies to protect their devices.

Practical	1. Setting and configuring two factor authentications in the Mobile phone. 2. Security patch management and updates in Mobiles. 3. Managing Application permissions in Mobile phones. 4. Installation and configuration of Mobile Anti-virus. 5. Installation and configuration of Open-Source VPN 6. Wi-Fi security management in mobile.

Module	Module Name	Module Content	Learning Outcomes
Module V	**E-Commerce and Digital Payments**	Definition of E-Commerce, Main components of E-Commerce, Elements of E-Commerce security, E-Commerce threats, E-Commerce security best practices, Introduction to digital payments, Components of digital payment and stakeholders, Modes of digital payments Banking Cards, Unified Payment Interface(UPI), e-Wallets, Unstructured Supplementary Service Data(USSD), Aadhar enabled payments, Digital payments related common frauds and preventive measures. RBI guidelines on digital payment sand customer protection in unauthorized banking transactions. Relevant provisions of Payment Settlement Act, 2007,	After the completion of this module, students would be able to understand the basic concepts related to E-Commerce and digital payments. They will become familiar with Various digital payment modes and related cyber security aspects, RBI guidelines and preventive measures against digital payment frauds.

Practical	1. Configuring security settings in Mobile Wallets and UPIs. 2. Checklist for secure net banking

Module	Module Name	Module Content	Learning Outcomes
Module VI	**Overview of Cyber security**	Cyber security increasing threat landscape, Cyber security terminologies Cyberspace, attack, attack vector, attack surface, threat, risk, vulnerability, exploit, exploitation, hacker., Non-state actors, Cyberterrorism, Protection of end user machine, Critical IT and National Critical Infrastructure, Cyber warfare, Case Studies	Students after completing this module will be able to understand the basic terminologies related to cybersecurity and current cybersecurity threat landscape. They will also develop understanding about the Cyberwarfare and necessity to strengthen the cyber security of end user machine, critical IT and national critical infrastructure.

Module	Module Name	Module Content	Learning Outcomes
Module VII	**Cyber crimes**	Cybercrimes targeting Computer systems and Mobiles- data diddling attacks, spyware, logic bombs, DoS, DDoS, APTs, virus, Trojans, ransomware, data breach, Online scams and frauds-email scams, Phishing, Vishing, Smishing, Online job fraud, Online sextortion, Debit/credit card fraud, Online payment fraud, Cyberbullying, website defacement, Cybersquatting, Pharming, Cyberespionage, Crypto jacking, Darknet- illegal trades, drug trafficking, human trafficking., Social Media Scams & Frauds- impersonation, identity theft, jobs cams, misinformation, fake news cybercrime against persons cyber grooming, child pornography, cybers talking., Social Engineering attacks, Cyber Police stations, Crime reporting procedure, Case studies.	After completion of the module, students will have complete understanding of the cyber-attacks that target computers, mobiles and persons. They will also develop understanding about the type and nature of cybercrimes and as to how report the cybercrimes through the prescribed legal and Government channels.

Practical	1. Platforms for reporting cyber-crimes. 2. Checklist for reporting cyber-crimes online.

Module	Module Name	Module Content	Learning Outcomes
Module VIII	**Cyber Law**	Cybercrime and legal landscape around the world, IT Act, 2000 and its amendments. Limitations of IT Act, 2000. Cybercrime and punishments, Cyber Laws and Legal and ethical aspects related to new technologies AI/ML, IoT, Blockchain, Darknet and Social media, Cyber Laws of other countries, Case Studies.I4C & Cyber Crime Reporting	Students after Completing this module will be able to understand the legal framework that exists in India for cybercrimes and penalties and punishments for such crimes, It will also expose students to limitations of existing IT Act, 2000 legal framework that is followed in other countries and legal and ethical aspects related to new technologies.

Module	Module Name	Module Content	Learning Outcomes
Module IX	**Data Privacy and Data Security**	Defining data, meta-data, big data, non-personal data. Data protection, Data privacy and data security, Personal Data Protection Bill and its compliance, Data protection principles, Big data security issues and challenges, Data protection regulations of other countries-General Data Protection Regulations(GDPR),2016 Personal Information Protection and Electronic Documents Act(PIPEDA)., Social media- data privacy and security issues.	After completing this module, students will understand the aspects related to personal data privacy and security. They will also get insight into the Data Protection Bill, 2019 and data privacy and security issues related to Social media platforms.

Practical	1. Setting privacy settings on social media platforms. 2. Do's and Don'ts for posting content on Social media platforms. 3. Registering complaints on a Social media platform.

Module	Module Name	Module Content	Learning Outcomes
Module X	**Cyber security Management, Compliance and Governance**	Cyber security Plan- cyber security policy, cyber crisis management plan., Business continuity, Risk assessment, Types of security controls and their goals, Cyber security audit and compliance, National cyber security policy and strategy. Intro to NIST SP 800:53	Students after completing this module will understand the main components of cyber security plan. They will also get insights into risk-based assessment, requirement of security controls and need for cyber security audit and compliance.

Practical	1. Prepare password policy for mobile device. 2. List out security controls for mobile phone and implement technical security controls in the personal mobile phone. 3. Conduct a Session at Villages or Rural areas or community to create cyber awareness among them and it must be published on daily newspaper or substantiate about the session minimum coverage 100 villagers / community people.

Suggested books:

1. Nina Godbole and Sunit Belapure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B.B. Gupta, D.P. Agrawal, Haoxiang Wang, Computer and Cybersecurity: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.
3. Cyber Security Essentials, James Graham, Rick Howard and Ryan Otson, CRC Press.
4. Introduction to Computer Network & Cyber Security, Chwan-Hwa(John) Wu, J. David Irwin, CRC Press T & F Group.