

वीर बहादुर सिंह पूर्वान्वल विश्वविद्यालय, जौनपुर (उ0प्र0)

प्रेषक,

कुलसचिव,
वीर बहादुर सिंह पूर्वान्वल वि०वि०,
जौनपुर।



वेब साईट : www.vbspu.ac.in
ई-मेल : connectpuregistrar@gmail.com
दूरभाष : 05452-252244

पत्रांक : 3150/शैक्षणिक/2023

दिनांक- 21.7.2023

सेवा में,

1. समस्त प्राचार्य/प्राचार्या एवं प्रबंधक
सम्बद्ध महाविद्यालय,
वीर बहादुर सिंह पूर्वान्वल विश्वविद्यालय, जौनपुर।
2. समस्त संकायाध्यक्ष/विभागाध्यक्ष
वीर बहादुर सिंह पूर्वान्वल विश्वविद्यालय जौनपुर।

विषय- प्रदेश स्थित विश्वविद्यालयों एवं महाविद्यालयों में स्नातक एवं परास्नातक स्तर पर साइबर सिक्योरिटी कोर्स लागू किए जाने के संबंध में।

महोदय/महोदया,

उपर्युक्त विषयक शासन (उच्च शिक्षा अनुभाग-3) के पत्र संख्या-4056/सत्तर-3-2022 दिनांक 7 दिसम्बर 2022 (छायाप्रति संलग्न) का कृपया संदर्भ ग्रहण करने का कष्ट करें, जिसके द्वारा अवगत कराया गया है कि साइबर क्राइम रोके जाने के प्रति जागरूकता बढ़ाने के उद्देश्य से स्नातक एवं परास्नातक स्तर के प्रत्येक संकाय में साइबर सिक्योरिटी कोर्स लागू कराए जाने हेतु निर्देश दिया गया है जिसके अनुपालन में समस्त संकायाध्यक्षों के प्रस्ताव पर विद्या परिषद् दिनांक 22 जून 2023 की कार्यसूची संख्या-7 के निर्णय अनुसार उक्त पाठ्यक्रम को विश्वविद्यालय स्तर पर लागू करने की संस्तुति प्रदान की गयी है।

अतः उक्त से अवगत होते हुये नियमानुसार आवश्यक कार्यवाही करने का कष्ट करें।


संलग्नक-यथोक्त

भवदीय


कुलसचिव

प्रतिलिपि- निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

- 1- परीक्षा नियंत्रक।
- 2- निजी सचिव कुलपति, कुलपति महोदया के संज्ञानार्थ।


कुलसचिव

प्रेषक,

गिरिजेश कुमार त्यागी,
विशेष सचिव,
उत्तर प्रदेश शासन।

सेवा में,

1. निदेशक,

उच्च शिक्षा, उ०प्र०,
प्रयागराज।

2. कुलसचिव

समस्त राज्य/निजी विश्वविद्यालय
उ०प्र०।

दिसम्बर

उच्च शिक्षा अनुभाग-3

लखनऊ : दिनांक ०७ नवम्बर, 2022

विषय:- प्रदेश स्थित विश्वविद्यालयों एवं महाविद्यालयों में स्नातक एवं परास्नातक स्तर पर साइबर सिक्योरिटी कोर्स लागू किये जाने के सम्बन्ध में।

महोदय,

उपर्युक्त विषयक गृह (गोपन) अनुभाग-2 के पत्र संख्या-बी०एस०-64/2022-सी०एक्स०-2, दिनांक 18.11.2022 (छायाप्रति संलग्न) के साथ संलग्न गृह मंत्रालय भारत सरकार के पत्र संख्या-22003/53/2019-I4C दिनांक 03.11.2022 एवं विश्वविद्यालय अनुदान आयोग के पत्र संख्या-1-42/2022 (e.gov) दिनांक 17.10.2022 का कृपया सन्दर्भ ग्रहण करने का कष्ट करें, जिसके द्वारा यह अवगत कराया गया है कि साइबर क्राइम रोके जाने के प्रति जागरूकता बढ़ाये के उद्देश्य से यू०जी०सी० द्वारा दिनांक 06.10.2022 को स्नातक एवं स्नातकोत्तर स्तर पर साइबर सिक्योरिटी कोर्स प्रारम्भ किया गया है एवं उक्त कोर्स को राज्य के विश्वविद्यालयों एवं महाविद्यालयों के एकेडमिक प्रोग्राम में शामिल किये जाने की अपेक्षा की गयी है।

2- इस सम्बन्ध में मुझे यह कहने का निदेश हुआ है कि गृह (गोपन) अनुभाग-2 के पत्र दिनांक 18.11.2022 द्वारा की गयी अपेक्षा के क्रम में विश्वविद्यालय अनुदान आयोग द्वारा प्रारम्भ किये गये साइबर सिक्योरिटी कोर्स को स्नातक एवं परास्नातक स्तर के प्रत्येक संकाय में लागू कराये जाने हेतु नियमानुसार आवश्यक कार्यवाही सुनिश्चित कराने का कष्ट करें। उल्लेखनीय है कि उक्त कोर्स का विवरण <https://www.ugc.ac.in/e-book/Cyber Security/mobile/index.html> लिंक पर उपलब्ध है।

संलग्नक-यथोक्त

भवदीय,

(गिरिजेश कुमार त्यागी)
विशेष सचिव।

संख्या- 4056 (1) /सत्तर-3-2022-तददिनांक:

प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित:-

- 1- कुलपति, समस्त राज्य/निजी विश्वविद्यालय, उ०प्र०।
- 2- समस्त क्षेत्रीय उच्च शिक्षा अधिकारी, उ०प्र०।
- 3- अपर सचिव, उ०प्र० राज्य उच्च शिक्षा परिषद।

आज्ञा से,

(सर्वश कुमार सिंह)
संयुक्त सचिव।

संख्या 1572/NP/2022

संख्या 4056 / सत

प्रमुख सचिव कार्यालय में
प्राप्त दिनांक 22/11/22

उत्तर प्रदेश शासन

गृह (गोपन) अनुभाग-2

संख्या:- बी0एस0- 64 / 2022-सी0एक्स0-2

लखनऊ: दिनांक 18 नवम्बर, 2022

JS (SKS)

प्रमुख सचिव,
उच्च शिक्षा विभाग,

(डा० सुधीर सिंह बोबडे) उत्तर प्रदेश शासन।

प्रमुख सचिव,
उच्च शिक्षा विभाग
उत्तर प्रदेश शासन

कृपया गृह मंत्रालय, भारत सरकार के अर्द्ध0शा0 पत्र संख्या-22003/53/2019-I4C, दिनांक 03.11.2022 (प्रतिलिपि संलग्न) का कृपया सन्दर्भ ग्रहण करने का कष्ट करें, जिसमें अवगत कराया गया है कि साइबर क्राइम को रोके जाने के लिये Law Enforcement Agencies (LEAs) की कार्य क्षमता बढ़ाये जाने के दृष्टिगत इण्डियन साइबर क्राइम कोऑर्डिनेशन सेन्टर (I4C) तथा नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल (NCRP) की स्थापना की गयी है। इसी क्रम में साइबर क्राइम रोके जाने के प्रति जागरूकता बढ़ाये जाने के उद्देश्य से यू0जी0सी0 द्वारा दिनांक 06.10.2022 को स्नातक एवं स्नातकोत्तर स्तर पर साइबर सिक्योरिटी कोर्स प्रारम्भ किया गया है और इस कोर्स को राज्य के विश्वविद्यालयों एवं कॉलेजों के एकेडेमिक प्रोग्राम में शामिल किये जाने की अपेक्षा की गयी है।

2. इस सम्बन्ध में गृह मंत्रालय, भारत सरकार का उपरोक्त पत्र दिनांक 03.11.2022 इस अनुरोध के साथ संलग्न कर प्रेषित है कि कृपया उपरोक्त से सम्बन्धितों को अवगत कराते हुये पत्र में की गयी अपेक्षानुसार आवश्यक कार्यवाही सुनिश्चित कराने का कष्ट करें।

संलग्नक: उपरोक्तानुसार।

(वी0 के0 सिंह)

विशेष सचिव।

संख्या व दिनांक तदैव।

प्रतिलिपि पुलिस महानिदेशक, उत्तर प्रदेश को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

आज्ञा से,

(वी0 के0 सिंह)

विशेष सचिव।

22003/53/2019-I4C
Government of India
Ministry of Home Affairs
Indian Cyber Crime Coordination Centre
(CIS Division)

5th Floor, NDCC-II Building,
Jai Singh Road, New Delhi - 110001,
Dated the 3rd November, 2022.

No. 37341/MS/GI/2022

To,

1. Chief Secretaries / Administrators of all States/UTs.
2. DGPs/CPs of all States/UTs.

Sub: - Syllabus of Cyber Security course for Under Graduate and Post Graduate released by UGC on 06.10.2022 - reg.

Sir/Madam,

It is informed that the Ministry of Home Affairs has launched the Indian Cyber Crime Coordination Centre (I4C) to strengthen the capabilities of Law Enforcement Agencies (LEAs) and to improve coordination among the LEAs and other agencies to fight cyber crime. The MHA has also launched the National Cyber Crime Reporting Portal (NCRP) to facilitate online reporting of incidents of cyber crime.

One of the key steps for preventing cyber crime is to generate sustained awareness among public, especially among the vulnerable sections and groups on 'Cyber Hygiene'. In this regard, it is informed that the matter was taken up with UGC and UGC has released a **Syllabus of Cyber Security course** for Under Graduate and Post Graduate levels on 06.10.2022. The letter dated 17.10.2022 of Secretary, UGC is enclosed herewith for kind reference.

3. States/UTs may kindly like to request the Universities and Colleges for introducing this 'Course Curriculum' in their academic program.

Encl: - As mentioned above.

Yours sincerely,

(Rajesh Kumar)
Chief Executive Officer

16-11-22
(तरुण गाबा)
सचिव,
गृह विभाग
उत्तर प्रदेश शासन।

16-11-22
(वी० के० सिंह)
विशेष सचिव
गृह विभाग
उ० प्र० शासन



प्रो. रजनीश जैन
सचिव

Prof. Rajnish Jain
Secretary



विश्वविद्यालय अनुदान आयोग
University Grants Commission

(शिक्षा मंत्रालय, भारत सरकार)
(Ministry of Education, Govt. of India)

बहादुरशाह जफर मार्ग, नई दिल्ली-110002
Bahadur Shah Zafar Marg, New Delhi-110002

Ph.: 011-23236288/23239337

Fax : 011-2323 8858

E-mail : secy.ugc@nic.in

D.O.No.F.1-42/2022(e.Gov)

17th October, 2022

Subject: Regarding the implementation of Syllabus of Cyber Security Course at Undergraduate and Post Graduate level.

Respected Madam/Sir,

On the occasion of Cyber Jaagrookta Diwas, 06th October, 2022, the University Grants Commission (UGC) launched the Syllabus of Cyber Security Course at Undergraduate and Post Graduate levels (https://www.ugc.ac.in/e-book/Cyber_Security/mobile/index.html).

The syllabus aims to create more aware, responsive and responsible digital citizens, thereby contributing effectively to an overall healthy cyber security posture and ecosystem.

In view of the importance of cyber security and for propagating cyber hygiene amongst HEIs, you are requested to take necessary steps for implementation of the Syllabus of Cyber Security Course at Undergraduate and Post Graduate level in all the streams of your esteemed University and also in the affiliated/constituent Colleges.

With kind regards.

Yours sincerely,

(Rajnish Jain)

To

- The Vice-Chancellors of all Universities
- The Principals of all Colleges

Syllabus of Cyber Security Course at Undergraduate and Post Graduate level



सत्यमेव जयते



ज्ञान-विज्ञान विमुक्तये

The University Grants Commission
Bahadur Shah Zafar Marg
New Delhi – 110002
www.ugc.ac.in

Contents

S. No.	Particulars	Page No.
1.	Introduction	5
2.	Terms of Reference	5
3.	Essential Components of Cyber security	5
4.	Program Educational Objectives (PEOs)	6
5.	Program Specific Outcomes (PSOs)	6
6.	Syllabus of Cyber Security Program at Undergraduate Level	7
7.	Syllabus of Cyber Security Program at Post Graduate Level	10
8.	Practical Work	12
9.	Teaching Scheme	13

Syllabus of Cyber Security Course at Undergraduate and Post Graduate level

Introduction

The evolution of Information Communication Technology (ICT) and growing security concerns demands flexible and generally comprehensive approach to the issue of cyber security. The rapid growth of ICT has raised various complex questions which need to be addressed. A need has been felt to address cyber security broadly, as also in sufficient depth so that even students from non-technical streams will develop a more complete picture of the cyber security issues. The syllabus has been prepared with an aim to create more aware, responsive and responsible digital citizens, thereby contributing effectively to an overall healthy cyber security posture and ecosystem.

Terms of Reference

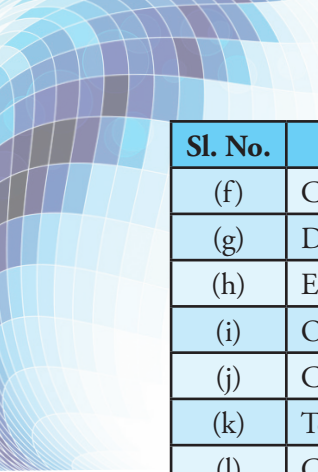
2. Terms of Reference (TOR) for drafting the proposed syllabus.

- (a) Cyber security as a subject needs to be incorporated at Graduation and Post-Graduation level in all the streams.
- (b) A separate syllabus for Graduation and Post-Graduation program to be prepared.
- (c) The syllabus should incorporate all the essential elements of cyber security so that the students at the Graduation and Post-Graduation level understand the essence and concept of cyber security as a whole.
- (d) The syllabus of cyber security at the Undergraduate level to be pitched at basic and mid-level wherein the syllabus at Post Graduate level should cover mid and advanced level concepts, duly considering the fact that Post Graduation students would have exposure to the basic concepts of cyber security in the preceding degree.
- (e) The syllabus should have sufficient depth so that even students from the non-technical streams can develop a complete picture of cyber security.

Essential Components of Cyber security

3. People, Process and Technology are the important pillars of the Cyber security, as to how, effectively the aspects related to these components fit into the curriculum considering the cyber threat landscape forms part of the content structuring and syllabus formation. With this backdrop, the following aspects, as tabulated below, have been taken into consideration in the syllabus formation: -

Sl. No.	Content	Level
(a)	Essential components of cyber security	Basic
(b)	Cyber security threat landscape	Basic
(c)	Cyber crime and its types	Basic – Medium
(d)	Remedial and mitigation measures	Basic
(e)	Reporting of Cyber crime	Basic



Sl. No.	Content	Level
(f)	Cyber Law	Basic
(g)	Data privacy and security	Basic
(h)	E-Commerce, Digital payments and its security	Medium
(i)	Overview of Social media and its security	Medium
(j)	Cyber security of digital devices	Medium
(k)	Tools and technology for cyber security	Medium
(l)	Cyber security plan and crisis management	Advanced
(m)	Security controls	Advanced
(n)	Risk based assessment, audit and compliance	Advanced
(o)	Cyber security best practices and do's and don'ts	Medium
(p)	Platforms to report and combat cyber crime	Basic
(q)	Practical hands-on	Basic-Medium and Advanced

Program Educational Objectives (PEOs)

4. The exposure of the students to Cyber Security program at Graduate and Post Graduate level should lead to the following: -
- Learn the foundations of Cyber security and threat landscape.
 - To equip students with the technical knowledge and skills needed to protect and defend against cyber threats.
 - To develop skills in students that can help them plan, implement, and monitor cyber security mechanisms to ensure the protection of information technology assets.
 - To expose students to governance, regulatory, legal, economic, environmental, social and ethical contexts of cyber security.
 - To expose students to responsible use of online social media networks.
 - To systematically educate the necessity to understand the impact of cyber crimes and threats with solutions in a global and societal context.
 - To select suitable ethical principles and commit to professional responsibilities and human values and contribute value and wealth for the benefit of the society.

Program Specific Outcomes (PSOs)

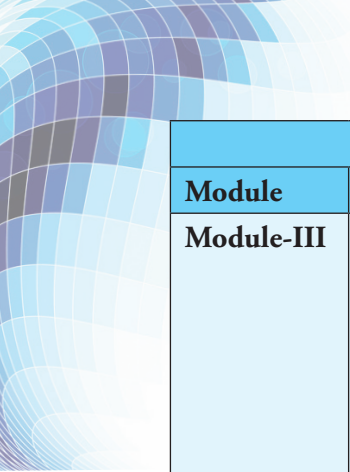
5. Upon completion of the degree program, students will be able to:-
- Understand the cyber security threat landscape.
 - Develop a deeper understanding and familiarity with various types of cyberattacks, cyber crimes, vulnerabilities and remedies thereto.
 - Analyse and evaluate existing legal framework and laws on cyber security.
 - Analyse and evaluate the digital payment system security and remedial measures against digital payment frauds.

- (e) Analyse and evaluate the importance of personal data its privacy and security.
- (f) Analyse and evaluate the security aspects of social media platforms and ethical aspects associated with use of social media.
- (g) Analyse and evaluate the cyber security risks.
- (h) Based on the Risk assessment, plan suitable security controls , audit and compliance.
- (i) Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities and training.
- (j) Increase awareness about cyber-attack vectors and safety against cyber-frauds.
- (k) Take measures for self-cyber-protection as well as societal cyber-protection.

Syllabus of Cyber Security Program at Undergraduate Level

6. The proposed syllabus at Undergraduate level academic program is as under: -

Cyber security Program at Undergraduate Level			
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 cyber security, Issues and challenges of cyber security.	After completion of this module, students would be able to understand the concept of Cyber security and issues and challenges associated with it.
Module-II	Cyber crime and Cyber law	Classification of cyber crimes, Common cyber crimes- cyber crime targeting computers and mobiles, cyber crime against women and children, financial frauds, social engineering attacks, malware and ransomware attacks, zero day and zero click attacks, Cybercriminals modus-operandi , Reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Cyber crime and offences, Organisations dealing with Cyber crime and Cyber security in India, Case studies.	Students, at the end of this module, should be able to understand the cyber crimes, their nature, legal remedies and as to how report the crimes through available platforms and procedures.
Practical	1. Checklist for reporting cyber crime at Cyber crime Police Station. 2. Checklist for reporting cyber crime online. 3. Reporting phishing emails. 4. Demonstration of email phishing attack and preventive measures.		



Cyber security Program at Undergraduate Level			
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 the reporting 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 IV	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 payments and customer protection in unauthorised 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.		

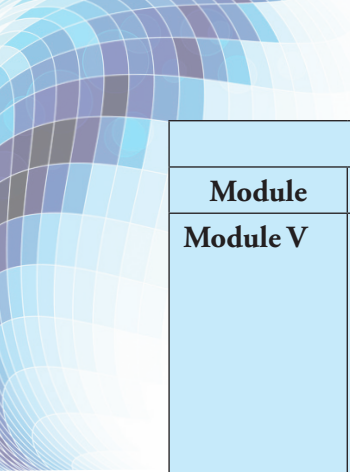
Cyber security Program at Undergraduate Level			
Module	Module Name	Module Content	Learning Outcomes
Module V	Digital Devices Security, Tools and Technologies for Cyber Security	End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management 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	<ol style="list-style-type: none"> 1. Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User). 2. Setting and configuring two factor authentication in the Mobile phone. 3. Security patch management and updates in Computer and Mobiles. 4. Managing Application permissions in Mobile phone. 5. Installation and configuration of computer Anti-virus. 6. Installation and configuration of Computer Host Firewall. 7. Wi-Fi security management in computer and mobile. 		
References	<ol style="list-style-type: none"> 1. Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010. 2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011) 3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. 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. 		

Syllabus of Cyber Security Program at Post Graduate Level

7. The syllabus for Cyber Security Program at Post Graduate Level is as under: -

Cyber Security Program at Post Graduate Level			
Module	Module Name	Module Contents	Learning Outcome
Module-I	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, Cyber terrorism, Protection of end user machine, Critical IT and National Critical Infrastructure, Cyberwarfare, Case Studies.	Students after completing this module will be able to understand the basic terminologies related to cyber security and current cyber security 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-II	Cyber crimes	Cyber crimes 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, Cyber-squatting, Pharming, Cyber espionage, Cryptojacking, Darknet- illegal trades, drug trafficking, human trafficking., Social Media Scams & Frauds- impersonation, identity theft, job scams, misinformation, fake news cyber crime against persons - cyber grooming, child pornography, cyber stalking., 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 cyber crimes and as to how report these crimes through the prescribed legal and Government channels.

Cyber Security Program at Post Graduate Level			
Module	Module Name	Module Contents	Learning Outcome
Practical	1. Platforms for reporting cyber crimes. 2. Checklist for reporting cyber crimes online.		
Module-III	Cyber Law	Cyber crime and legal landscape around the world, IT Act,2000 and its amendments. Limitations of IT Act, 2000. Cyber crime 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.	Students after completing this module will be able to understand the legal framework that exist in India for cyber crimes 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 IV	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.		



Cyber Security Program at Post Graduate Level			
Module	Module Name	Module Contents	Learning Outcome
Module V	Cyber security Management, Compliance and Governance	Cyber security Plan- cyber security policy, cyber crises management plan., Business continuity, Risk assessment, Types of security controls and their goals, Cyber security audit and compliance, National cyber security policy and strategy.	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	<ol style="list-style-type: none">1. Prepare password policy for computer and mobile device.2. List out security controls for computer and implement technical security controls in the personal computer.3. List out security controls for mobile phone and implement technical security controls in the personal mobile phone.4. Log into computer system as an administrator and check the security policies in the system.		
References	<ol style="list-style-type: none">1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.2. Information Warfare and Security by Dorothy F. Denning, Addison Wesley.3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform.4. Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram, CRC Press.5. Information Security Governance, Guidance for Information Security Managers by W. KragBrothy, 1st Edition, Wiley Publication.6. Auditing IT Infrastructures for Compliance By Martin Weiss, Michael G. Solomon, 2nd Edition, Jones Bartlett Learning.		

Practical Work

8. The practical list has been suggested for the applicable modules; however, the faculty may expand the list as per the syllabus content duly taking into consideration the emerging nature of cyber threats and incumbent protective measures to guard against such threats.

TEACHING SCHEME

Cyber security Program at Undergraduate Level and Postgraduate Level

Sl. No	Course Title	Teaching Scheme at UG and PG Level		
		L/T	P	C
1	Cyber Security	3	1	4

Legend:

L: Lectures T: Tutorials P: Practical/Projects C: Credits

Notes:

1 Credit: 1 Hour for Lecture/Tutorial

1 Credit: 2 Hour for Practical/Projects

Terms of Reference for Credit Scheme (3+1)

- There are total of 90-96 working days (15 -16 Weeks) in a semester.
- 1 Credit = 15 Hours, therefore 3 Credits = 45 hours ($3 \times 15 = 45$)
- In a week, (3 lectures of theory, each period of one hour duration every week-.45 hours in a semester) and 1 practical session of two hours (30 hours in a semester)

Notes:

1 C: 1 Hour for Lecture/Tutorial

C: 2 Hour for Practical/Projects

Terms of Reference for Credit Scheme (3+1)

- There are total of 90-96 working days (15 -16 Weeks) in a semester.
- 1 Credit = 15 Hours, therefore 3 Credits = 45 hours ($3 \times 15 = 45$)
- In a week, 3 lectures of theory, each period of one hour duration every week, (45 hours in a semester) and 1 practical session of two hours. (30 hours in a semester)

NOTE : As far as transaction of these courses at UG and PG level in HEIs is concerned, HEIs may invite Cyber Security/Computer/IT qualified faculty or else Experts from Industry/Subject Matter Experts to take the lectures, practicals and tutorials. The proposed syllabus gives broad guidelines and teachers who would teach the subject will have enough flexibility to strike the balance between time vis-a-vis depth of coverage.
