
UNIVERSITY OF MYSORE
Estd. 1916

VishwavidyanilayaKaryasoudha
Crawford Hall, Mysuru- 570 005

No.AC2(S)/151/2020-21

Dated: 08.12.2023

Notification

Sub:- Syllabus of Cyber Security with effect from the Academic year 2023-24.

Ref:- 1. This office letter No: AC6/303/2022-23 dated: 28-07-2023.

2. This office Notification No: AC2(S)/151/2020-21, dated: 06.10.2023.


3. Decision of BOS in Computer Science (CB) meeting held
On 04.12.2023.

The Board of Studies in Computer Science (CB) which met on 04.12.2023 respectively has resolved to recommended and approved the syllabus and scheme of Examinations of Cyber Security with effect from the Academic year 2023-24.

Pending approval of the Faculty of Science & Technology and Academic Council meetings the above said syllabus and scheme of examinations are hereby notified.

The syllabus and scheme of Examinations contents may be downloaded from the University website i.e., www.uni-mysore.ac.in.

Draft Approved by the Registrar


Deputy Registrar (Academic)
Deputy Registrar (Academic)
University of Mysore
Mysore- 570 005

To:-

1. All the Principal of affiliated Colleges of University of Mysore, Mysore.
2. The Registrar (Evaluation), University of Mysore, Mysuru.
3. The Chairman, BOS/DOS, in Computer Science (CB), Manasagangothri, Mysore.
4. The Director, Distance Education Programme, Moulya Bhavan, Manasagangothri, Mysuru.
5. The Director, PMEB, Manasagangothri, Mysore.
6. Director, College Development Council , Manasagangothri, Mysore.
7. The Deputy Registrar/Assistant Registrar/Superintendent, Administrative Branch and Examination Branch, University of Mysore, Mysuru.
8. The PA to Vice-Chancellor/ Registrar/ Registrar (Evaluation), University of Mysore, Mysuru.
9. Office Copy.

Program Name		Semester	V
Course Title	Cyber Security (Theory)		
Course Code:	SEC-5	No. of Credits	03
Contact hours	45Hrs	Duration of SEA/Exam	03 hrs
Formative Assessment Marks	50	Summative Assessment Marks	50

Course Outcomes (COs): After the successful completion of the course, the student will be able to:

CO1	After completion of this course, students would be able to understand the concept of Cyber security and issues and challenges associated with it.
CO2	Students, at the end of this course, should be able to understand the cyber crimes, their nature, legal remedies and as to how report the crimes through available platforms and procedures.
CO3	On completion of this course, 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.
CO4	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.
CO5	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.

Contents		45Hrs
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.		09
Module-II. Cyber-crime and Cyber law: Classification of cybercrimes, 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.		09
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.		08

<p>Module IV. Definition of E- Commerce, Main components of E-Commerce, Elements of E-Commerce security, E-Commerce threats, E-Commerce security best practices, Advantage of e-commerce, Survey of popular e-commerce sites. Introduction to digital payments, Components of digital payment and stake holders, 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 unauthorized banking transactions. Relevant provisions of Payment Settlement Act,2007.</p>	08
<p>Module V. 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.</p>	11

Course Articulation Matrix: Mapping of Course Outcomes (COs) with Program Outcomes

Course Out comes(COs) /Program Outcomes (POs)	Program Outcomes (POs)														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Quickly understand the given problem and come up with the correct answer															
Identify, construct and compute numerical situations by work with numbers															
Conceive and develop a methodology for analyzing data and solving a problem.															
Define, modify and apply critical thinking to real time situations.															

Pedagogy: Problem Solving

Formative Assessment for Theory	
Assessment Occasion/type	Marks
Internal Test1	30%
Assignment/Surprise Test	20%
Total	50 Marks
<i>Formative Assessment as per guidelines.</i>	

Text/References	
1	Cyber Crime Impact in the New Millennium, by R. C Mishra, Aauther 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 , 13 th November, 2001)
4	Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
5	Fundamentals of Network Security by E. Maiwald, McGraw Hill.
6	Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.