



ಕರ್ನಾಟಕ ಸರ್ಕಾರ

ಕರ್ನಾಟಕ ರಾಜ್ಯ ಉನ್ನತ ಶಿಕ್ಷಣ ಪರಿಷತ್ತು

ಸಂಖ್ಯೆ: ಕರಾಉಶಿಪ/160/1ರಿಂದ 6ನೇ ಸೆಮಿಸ್ಟರ್/2022-23 /794 ದಿನಾಂಕ: 16-11-2023

ಇವರಿಗೆ,

ಕುಲಸಚಿವರು

ರಾಜ್ಯದ ಎಲ್ಲಾ ಸಾರ್ವಜನಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯಗಳು

ಮಾನ್ಯರೆ,

ವಿಷಯ: **Skill Enhancement Courses (SEC) - Employability Skills or Cyber Security** ವಿಷಯಗಳ ಪಠ್ಯಕ್ರಮ ಮತ್ತು ವ್ಯಾಸಂಗ ಕ್ರಮದ ಬಗ್ಗೆ ಸ್ಪಷ್ಟೀಕರಣ.

ಉಲ್ಲೇಖ: ಉನ್ನತ ಶಿಕ್ಷಣ ಪರಿಷತ್ತಿನ ಪತ್ರ ಸಂಖ್ಯೆ: ಕರಾಉಶಿಪ/160/1ರಿಂದ 6ನೇ ಸೆಮಿಸ್ಟರ್/2022-23/655, ದಿನಾಂಕ: 21/09/2023.

ಮೇಲ್ಕಂಡ ವಿಷಯಕ್ಕೆ ಸಂಬಂಧಿಸಿದಂತೆ ಉಲ್ಲೇಖಿತ ಪತ್ರದಲ್ಲಿ ವಿಷಯ ತಜ್ಞರ ಸಮಿತಿಗಳು ಅಂತಿಮಗೊಳಿಸಿದ 1ರಿಂದ 6ನೇ ಸೆಮಿಸ್ಟರ್ ಗಳ ಮಾದರಿ ಪಠ್ಯಕ್ರಮಗಳನ್ನು ಮತ್ತು 5ನೇ ಸೆಮಿಸ್ಟರ್ ನಲ್ಲಿ Skill Enhancement Courses (SEC) ನಲ್ಲಿ Employability Skills or Cyber Security ಒಳಗೊಂಡ ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಕರ್ನಾಟಕ ರಾಜ್ಯ ಉನ್ನತ ಶಿಕ್ಷಣ ಪರಿಷತ್ತಿನ ವೆಬ್‌ಸೈಟ್ ನಲ್ಲಿ ಪ್ರಕಟಿಸಿರುವಂತೆ ವಿಶ್ವವಿದ್ಯಾಲಯಗಳ ಅಧ್ಯಯನ ಮಂಡಳಿಗಳು ಸೂಕ್ತವಾಗಿ ಅಳವಡಿಸಿಕೊಂಡು ಸ್ನಾತಕ ಪದವಿಯ ತರಗತಿಗಳಿಗೆ ಅನುಮೋದಿಸಲು ತಿಳಿಸಲಾಗಿತ್ತು.

ಈ ಸಂಬಂಧ **Employability Skills or Cyber Security** ವಿಷಯಗಳಿಗೆ ಸಂಬಂಧಪಟ್ಟಂತೆ ಪಠ್ಯಕ್ರಮ, ಕ್ರೆಡಿಟ್ ಮತ್ತು ವ್ಯಾಸಂಗ ಕ್ರಮದ ಬಗ್ಗೆ ಕೆಲವು ಗೊಂದಲಗಳಿರುವ ಬಗ್ಗೆ ಕೆಲವು ವಿಶ್ವವಿದ್ಯಾಲಯಗಳು ಸ್ಪಷ್ಟೀಕರಣ ಕೋರಿರುವ ಹಿನ್ನೆಲೆಯಲ್ಲಿ 5ನೇ ಸೆಮಿಸ್ಟರ್ ನಲ್ಲಿ ಈ ಎರಡೂ ವಿಷಯಗಳಿಗೆ ತಲಾ 03 ಕ್ರೆಡಿಟ್ ಗಳು, ವಾರಕ್ಕೆ 03 ಗಂಟೆಗಳಂತೆ ಒಟ್ಟು ಬೋಧನಾ ಅವಧಿ 45 ಗಂಟೆಗಳು, ಪರೀಕ್ಷಾ ಅವಧಿ 03 ಗಂಟೆಗಳು ಹಾಗೂ ಒಟ್ಟು 100 ಅಂಕಗಳನ್ನು ನಿಗದಿಪಡಿಸಿರುವುದಾಗಿ ಈ ಮೂಲಕ ಸ್ಪಷ್ಟೀಕರಿಸಲಾಗಿದೆ. ಅದರಂತೆ ಎರಡೂ ವಿಷಯಗಳ ಪಠ್ಯಕ್ರಮ ಮತ್ತು ವ್ಯಾಸಂಗ ಕ್ರಮಗಳನ್ನು ಪರಿಷ್ಕರಿಸಿ ಕರ್ನಾಟಕ ರಾಜ್ಯ ಉನ್ನತ ಶಿಕ್ಷಣ ಪರಿಷತ್ತಿನ ವೆಬ್ ಸೈಟ್ ನಲ್ಲಿ upload ಮಾಡಲಾಗಿದೆ. ಪರಿಷ್ಕೃತ ಪಠ್ಯಕ್ರಮಗಳನ್ನು ವಿಶ್ವವಿದ್ಯಾಲಯಗಳ ಅಧ್ಯಯನ ಮಂಡಳಿಗಳು ಸೂಕ್ತವಾಗಿ ಅಳವಡಿಸಿಕೊಳ್ಳಲು ಮತ್ತು ಮುಂದಿನ ಅಗತ್ಯಕ್ರಮ ತೆಗೆದುಕೊಳ್ಳುವಂತೆ ಕೋರಲಾಗಿದೆ.

ತಮ್ಮ ನಂಬುಗೆಯು,

K. G. [Signature] 16/11/23
ಕಾರ್ಯನಿರ್ವಾಹಕ ನಿರ್ದೇಶಕರು

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.</p> <p>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.

<p align="center">Name of the Program: Bachelor of Arts/ Science/ Commerce/ Business Administration/ Social Works; Bachelor of Arts/ Science/ Commerce/ Business Administration/ Social Works (Hons. With or without Research), and Bachelor of Performing Arts, Bachelor of Visual Arts, and Bachelor of Hotel/Hospitality Management</p> <p align="center">Course Code: 5.6</p> <p align="center">Name of the Course: Employability Skills</p>			
Course Credits	No. of Hours per Week	Total No. of Teaching Hours	
3 Credits	3 Hrs	45 Hrs	
Formative Assessment Marks	50	Summative Assessment Marks MCQ	50
Pedagogy: Classroom lectures, Activities based learning, Practice Questions, Tutorial Classes, Group discussions, Mock Tests, etc,			
<p>Course Outcomes: On successful completion of the course, the students will be able to</p> <ol style="list-style-type: none"> Develop systematic problem-solving abilities. Enhance verbal and non-verbal reasoning skills. Improve numerical and analytical abilities. Enhance English language and communication skills. 			
Syllabus:			Hours
Module No. 1: General Orientation on all Competitive Exams			5
Overview of Competitive Exams for Government Recruitment in India - Introduction, Eligibility Criteria, Exam Pattern, Syllabus, and Resources.			
Module No. 2: Quantitative Aptitude			20
Number system, HCF & LCM, Ratio and Proportion, Averages, Ages, Percentages, Partnerships, Time, Speed and Distance, Profit and Loss, Data Interpretation, Problems based on Simple interest, Compound interest, Clocks, and Calendars.			
Module No. 3: Verbal and Nonverbal Reasoning			10
<p>Verbal Reasoning: Data analysis, Data sufficiency, Decision making, coding & decoding, Blood relations, Puzzle tests, Direction sense test, Problems based on Venn Diagram/Syllogisms, Alphabet test, Arithmetical reasoning, Input/Output, Series and Seating arrangements.</p> <p>Non-Verbal Reasoning: Analogy, Water images, mirror images, embedded figures, Completion of Pattern, Paper folding, Cubes & dice, Figure Formation & Analysis.</p>			
Module No. 4: English Language and Comprehension Solving			10
Vocabulary, English Grammar, Verbal Ability, Sentence Structure, Spot the Error, Fill in the Blanks, Idioms & Phrases, Cloze Passages, and Comprehension Passages.			
Skill Development Activities:			
Various activity-based learning methods such as problem-solving exercises, case studies, role-playing, debates, group discussions, mock tests, and assessments can be conducted, in addition to any other relevant activities for the course to ensure effective learning.			

Materials:

1. <https://free.aicte-india.org/Quantitative-Aptitude-Basics.php>
2. https://onlinecourses.nptel.ac.in/noc20_hs19/preview
3. <https://www.udemy.com/course/reasoning-verbal-non-verbal/>

Note: Latest editions of books such as Quantitative Aptitude for Competitive Examinations, Modern Approach to Verbal and Non-Verbal Reasoning, Quick Learning Objective General English by R.S.Agarwal or Arihant Publications, and other renowned titles can be referred to enhance exam preparation.