आचार्य मनिष र. जोशी
सचिव

Prof. Manish R. Joshi
Secretary

सत्यमेव जयते

विश्वविद्यालय अनुदान आयोग
University Grants Commission
(शिक्षा मंत्रालय, भारत सरकार)
(Ministry of Education, Govt. of India)

F.No. 5-1/2024(MMTTPGuideline)   12th December 2024/21 अग्रहायण, 1946

आदरणीय महोदया/महोदय,

As you are aware, NEP 2020 highlights the importance of integrating technology in education, including Cyber-Security and Artificial Intelligence (AI). With the increasing reliance on digital infrastructure in education, Cyber Security (CS) has become a critical component to ensure the safety and integrity of educational systems.

In this regard, the Ministry of Education has conceptualised a Capacity-Building Programme for the faculty members of Higher Education on Cyber Security by using the services of any of the IITs, under the aegis of the Malaviya Mission Teacher Training Programme (MMTTP).

The Indian Institute of Technology Madras (IITM), Chennai, is starting the Capacity Building Programme in Cyber Security. The first program commences on 16th December 2024. The detailed concept note of the programme and programme details by IIT Madras are attached for reference.

In view of the above, Higher Education Institutions are requested to disseminate the information among the faculty members under their purview to make full use of this opportunity to enhance their knowledge and expertise in Cyber Security.

Your support in ensuring maximum participation will contribute significantly to building institutional capacity in this crucial domain.

सादर ,

भवदीय,

(मनिष जोशी)

Encl: As above

To,
The Vice-Chancellors of all Universities
The Principals of all Colleges
The Programme Directors of 116 MMTTCs

<div align="center">**Concept Note**</div>

<div align="center">**Capacity Building Programme on Cybersecurity and Artificial Intelligence**</div>

Background

With the increasing reliance on digital infrastructure in education, Cybersecurity (CS) has become a critical component to ensure the safety and integrity of educational systems. Educational institutions, including universities and colleges, are rapidly adopting online platforms, digital resources, and cloud-based services for administration, research, and teaching. This digital transformation, while enabling more accessible and innovative educational experiences, also exposes institutions to significant cybersecurity threats. Parallelly, Artificial Intelligence (AI) is emerging as a powerful tool in transforming educational paradigms, fostering an environment of innovation and preparing students for future challenges. It will not only enhance faculty expertise but also promotes interdisciplinary collaboration, ensuring that institutions remain at the forefront of educational excellence. On various occasion, Hon'ble Prime Minister has emphasized the critical importance of cybersecurity and the role of artificial intelligence (AI) in modern education.

Introduction

National Education Policy 2020 (NEP 2020) inter alia stipulates that the world is undergoing rapid changes in the knowledge landscape. With various dramatic scientific and technological advances, such as the rise of big data, machine learning, and artificial intelligence, many unskilled jobs worldwide may be taken over by machines, while the need for a skilled workforce, will be increasingly in greater demand. NEP 2020 highlights the importance of integrating technology in education, including cybersecurity and artificial intelligence (AI). Following are the relevant points concerning training for faculty:

i.   **Digital Literacy**: NEP 2020 emphasizes the need for enhancing digital literacy among educators. This includes understanding the basics of cybersecurity to protect data and privacy.

ii. **Incorporation of Technology**: The policy encourages the use of AI and other emerging technologies in education. Faculty and staff training in these areas is essential for effective implementation and integration into the curriculum and administrative processes.

iii. **Capacity Building**: NEP 2020 advocates for continuous professional development, suggesting that training programs should include components on cybersecurity protocols and the ethical use of AI in educational settings.

iv. **Collaboration with Institutions**: The policy mentions collaboration with relevant institutions and organizations to provide training and resources, ensuring faculty and staff are well-versed in current technologies and practices.

v. **Research and Development**: Encouraging research in the fields of AI and cybersecurity is also a focal point, implying that faculty should be trained not only in application but also in understanding the underlying principles and research methodologies.

NEP 2020 underscores the necessity for a skilled workforce in education that is proficient inter-alia in cybersecurity and AI to enhance teaching, learning, and administrative efficiency. This ToT program on **Cyber Security and Artificial Intelligence for Teachers through Prompting** is an innovative step towards integrating CS & AI into educational practices. By empowering teachers with CS & AI skills, we can foster a more effective, engaging, and personalized learning environment in higher education, aligning with the broader goals of NEP 2020 and the Malaviya Mission.

Accordingly, following capacity building programs for faculty, administrators and policy makers of HEIs have been conceptualised under the aegis of Malaviya Mission Teacher Training Programme (MMTTP) to address the key elements of NEP 2020 with a specific focus on: -

(i) Capacity Building Program on Cybersecurity

(ii) Capacity Building Program on Artificial Intelligence

(i) Capacity Building Program on Cybersecurity

As India advances in its digital transformation, it is equally necessary to stress upon the cybersecurity and empowering faculty and administrators with the tools for digital safety. To protect the nation's digital assets and ensure a secure educational environment, the program envisages a comprehensive training to equip faculty with essential cybersecurity knowledge and best practices for safeguarding sensitive information. Accordingly, the program shall endeavour for the following: -

i. **Cybersecurity Training Programs**: providing comprehensive training for educators on cybersecurity best practices to protect sensitive information and digital assets.

ii. **Curriculum Development**: Incorporating cybersecurity awareness and skills into teacher training programs, ensuring faculty are equipped to educate students on this critical topic.

iii. **Collaboration with Experts**: Partnering with cybersecurity experts and institutions to develop resources and training materials tailored for educators.

iv. **Promoting Safe Digital Practices**: Encouraging faculty to adopt and promote safe online practices within their institutions, fostering a culture of cybersecurity awareness among students.

Objectives of Capacity Building Program on Cybersecurity:

- Increase awareness of cybersecurity threats and vulnerabilities specific to educational institutions.
- Equip faculty with best practices for online safety, including password management, secure communications, and data protection.
- Educate faculty on safe online behaviours and practices to ensure a secure learning environment.
- Train faculty on how to respond effectively to cybersecurity incidents, including reporting protocols and mitigation strategies.
- Protect academic resources and sensitive student information from cyber threats, ensuring the integrity of academic programs.
- Encourage a culture of cybersecurity awareness across the institution, promoting shared responsibility among faculty and staff.
- Equip institutions with trained faculty who can advocate for cybersecurity measures and policies.

Expected Outputs & Outcomes of Capacity Building Program on Cybersecurity:

- **Increased Awareness:** Faculty members will have a heightened awareness of cybersecurity threats and vulnerabilities specific to the educational sector.
- **Improved Cyber Hygiene:** Faculty will adopt best practices for online safety, leading to enhanced password management, secure communications, and data protection measures.
- **Enhanced Teaching Capabilities:** Educators will be equipped to teach students about cybersecurity, integrating it into their lessons and promoting a culture of digital safety.
- **Effective Incident Management:** Faculty will be able to respond effectively to cybersecurity incidents, minimizing potential damage and ensuring prompt reporting.
- **Protection of Academic Resources:** Increased protection of academic resources and sensitive student information, contributing to the integrity and reliability of educational programs.
- **Institutional Culture Shift:** A shift towards a culture of cybersecurity awareness within educational institutions, promoting shared responsibility among faculty, staff, and students.
- **Advocacy for Cybersecurity Policies:** Trained faculty will advocate for stronger cybersecurity measures and policies at their institutions, influencing overall governance.
- **Long-Term Resilience:** Educational institutions will build long-term resilience against cyber threats, fostering a secure learning environment that supports digital transformation.

(ii) Capacity Building Program on Artificial Intelligence for Faculty and Academic Leaders

Role of artificial intelligence (AI) in education, particularly in enhancing the capabilities of faculty and Academic leaders is very critical. Initiatives aimed at integrating AI into

teacher training programs, developing AI-driven educational tools, and promoting research in AI to improve teaching methodologies will equip Higher Education eco-system in enhancing over all quality. The program shall endeavour for the following:

(i) **Training Programs**: Launch of specialized training programs for educators to enhance their understanding and teaching capabilities in AI, fostering a skilled workforce.

(ii) **Collaboration with Institutions**: Partnerships with leading technology companies and universities to provide resources, training modules, and real-world applications of AI.

(iii) **Research and Innovation**: Promotion of AI research in academic institutions, encouraging faculty and academic leaders to engage in innovative projects and collaborations.

(iv) **Focus on Inclusivity**: Ensuring that AI training is accessible to a diverse range of academic leaders and faculty, including those from underrepresented backgrounds.

(v) **Skill Development Initiatives**: Integration of AI training within broader skill development initiatives to prepare students for future job markets.

Objectives of Capacity Building Program on Artificial Intelligence:

(i) Ensure that AI training programs support the goals of the National Education Policy (NEP) 2020, which emphasizes holistic, multidisciplinary education, critical thinking, and the integration of technology.

(ii) Equip faculty and academic leaders with advanced AI knowledge and skills to enhance their teaching methodologies and educational practices.

(iii) Establish a standardized AI curriculum across higher education institutions to improve the quality and consistency of AI education.

(iv) Promote a culture of research and innovation in AI among faculty, enabling them to engage in cutting-edge projects that contribute to the field.

(v) Foster a mindset of continuous/lifelong learning among educators, encouraging them to stay updated with AI advancements and educational technologies.

(vi) Ensure that AI training programs are accessible to a diverse range of faculty and academic leaders, promoting equity in educational opportunities.

(vii) Integrate AI training within broader skill development initiatives to prepare students for future careers in an AI-driven world.

Expected Outputs & Outcomes of Capacity Building Program on Artificial Intelligence:

(i) **Enhanced Teaching Quality:** Faculty will implement innovative teaching methodologies informed by AI, resulting in improved student engagement and learning outcomes.

(ii) **Standardized AI Literacy:** A consistent level of AI knowledge among educators will lead to a more informed and capable academic workforce.

(iii) **Increased Research Output:** Greater faculty engagement in AI-related research will result in innovative projects, publications, and collaborations, positioning institutions as leaders in AI research.

(iv) **Collaborative Partnerships:** Stronger ties with technology companies and research institutions will provide resources, expertise, and real-world applications for faculty and students.

(v) **Diverse Academic Environment:** A more inclusive training framework will ensure diverse perspectives in AI education, enriching the learning experience for all students.

(vi) **Skilled Graduates:** Students will graduate with the competencies needed to thrive in AI-related fields, aligning their skills with market demands.

(vii) **Contribution to National Goals:** By integrating AI into teacher training program, HEIs will contribute in fulfilling the vision of Viksit Bharat.

Host Institutions/ Implementing agency for Capacity Building Programs on Cybersecurity and Artificial Intelligence:

Initially, IIT Madras and IIT Ropar have been identified for conducting **Capacity Building Program on Cybersecurity and Capacity Building Program on Artificial Intelligence** respectively based on their proposals and institutional core strength.

Other eminent Institutions may also be identified for conducting these Capacity Building Programs, if required, subject to approval of PAB.

Implementation Framework for Capacity Building Programs on Cybersecurity and Artificial Intelligence:

All host institutes can exercise autonomy in assigning facilitators, setting syllabi, and developing pedagogical approaches in accordance with the following standardised programme modalities:

a. **Participants –** Faculty from centrally-funded institutes and State Universities for Capacity Building Programme on Cyber Security; Faculty and Academic Leaders for Capacity Building Programme on Artificial Intelligence.

b. **Eligibility for Nomination / Selection –**Regular faculty OR faculty performing non-academic work such as Registrar, Dean, Controller of Exam etc.

c. **Batch size –** Upto 100 participants per batch

d. **No. of programs –** Minimum 9 in a year (6 Basic/Foundation Level + 3 Intermediate/Advanced)

e. **Mode of delivery & duration – 5 + 5 days (online)**
   i. Basic/Foundation Level -5 days (35 hours total)
   ii. Intermediate/Advanced Level - 5 days (35 hours total)

Note: Successful completion of the Basic/Foundation course is mandatory for enrolment in the Intermediate/Advanced course.

f. **Modules –** Host institutions will have full autonomy to design curriculum and pedagogy of the programme relevance to theme (Cyber Security/ Artificial Intelligence)

g. **Engagement -** Pre-training micro-learning via WhatsApp/mail to familiarize participants with course objectives.

h. **Assessment and certificate of participation –** The host institution shall assess the learning outcomes of the participants. Upon successful completion of the programme, Host Institution shall award a certificate of completion under the aegis of Malaviya Mission Teacher Training Programme (MMTTP). Assessment is primarily to see effectiveness of the delivery and feedback to the participants.

Feedback Mechanism - Participants are required to fill in the feedback form after each programme.

Financial Norms

S. No.	Component	Unit Cost*	Physical (2 years)		Financial (2 years)	Number of Institutions	Host Institution
			No. of training program	No. of beneficiaries/ faculty to be trained	(Amount in Rs.)		
1	**Capacity Building Program on Artificial Intelligence for Faculty Members**						
(i)	Artificial Intelligence Essential (Foundation Course)	3,60,000	12	1200	43,20,000	1	**IIT Ropar**
(ii)	AI Prompting - tricks in the trade: (Advanced Course)	4,05,000	6	600	24,30,000	1	
2	**Capacity Building Program on Artificial Intelligence for Academic Leaders**						
(i)	Artificial Intelligence Essential (Foundation Course)	3,60,000	12	1200	43,20,000	1	**IIT Ropar**
(ii)	AI Prompting - tricks in the trade: (Advanced Course)	4,05,000	6	600	24,30,000	1	
3	**Capacity Building Program on Cyber Security for Faculty**						

(i)	Cyber security Essentials – (Basic Course)	3,60,000	12	2400	43,20,000	1	**IIT Madras**
(ii)	Cyber Security Essentials – (Intermediate Course)	4,05,000	6	1200	24,30,000	1	

* cost includes all expenses and taxes, if any

Impact

Cybersecurity training for faculty in higher education is crucial in an increasingly digital landscape, as it equips educators with the skills needed to protect sensitive data and maintain the integrity of academic systems. This training not only enhances faculty awareness of potential cyber threats but also fosters a culture of security within the institution.

Furthermore, incorporating Artificial Intelligence into training programs can personalize learning experiences, adapt to individual knowledge levels, and provide real-time feedback, thereby improving the effectiveness of the training.

Together, these initiatives are expected to empower faculty to safeguard educational environments while promoting a proactive approach to cybersecurity, ultimately enhancing the overall resilience of higher education institutions against cyber threats. Faculty trained under this initiative will serve as ambassadors, cascading knowledge within their institutions and across the education sector, reinforcing the HEI's preparedness.

***

Capacity Building Programme on Cybersecurity

The growing reliance on digital platforms across sectors has amplified the need for robust cybersecurity awareness and measures. Empowering teachers and trainers with essential cybersecurity skills will address the gap and enable them to foster a culture of digital safety and preparedness among students and institutions.

Given this background and context, two special training programs on Cybersecurity for teachers/faculty members (ToT) under the Malaviya Mission Teacher Training Program are conceptualized:

1. Capacity Building Programme on Cybersecurity - Basic level
2. Capacity Building Programme on Cybersecurity - Intermediate level

The first batch of basic level is ready to commence on **16th December 2024**. Detailed schedule of the training programme is in Appendix B of this document.

Proposed Program Overview:

1. **Objective:** To equip educators and professionals with the necessary knowledge and skills to address cybersecurity challenges effectively, thereby promoting a secure and resilient digital environment.

2. **Target Audience:**

   o Teachers and educators in higher education institutions.
   o Trainers under skilling initiatives.

3. **Program Highlights:**

   o Modules on basic cybersecurity awareness, secure digital practices, and protection.
   o Modules at Intermediate topics, include, Mobil security, Cloud security, OSINT tools for intelligence gathering, Introduction to IAM with data security, privacy and data protection & Introduction to Cryptocurrencies, with CVE database use for fixing security flaws.
   o Hands-on demos with real-world scenarios using latest tools & virtual labs and attack simulations.
   Please refer Appendix A – Course Structure for Basic & Intermediate trainings

4. **Delivery Model:** Online learning with demos, to maximize reach and engagement.

5. **Proposed Timeline:**

   o Launch Date: **December 2024**.

      o Basic Level – 16th Dec 2024 (5 days) & 23rd Dec 2024 (5 days)

o   Intermediate Level – 30th Dec 2024 (5 days)

Please refer Appendix B Proposed Schedule of Training Programs

6. **Expected Outcomes:**

    o   Enhanced cybersecurity awareness and preparedness among educators.
    o   Creation of a teachers pool to address cybersecurity awareness to society
    o   Strengthened digital resilience within educational institutions.

7. **Registration**

    o   Trainees may complete their nominations using the webpage provided below
        https://digitalskills.iitmpravartak.org.in/adduser.php

Course structure – Basic

Day	Basic Course Topics	Duration
Day 1	A. Introduction and overview of cyber security • Important terminologies • Threat landscape • CIA Triad • Defense in-depth for Information security • password management and password best practices with hands on tools • Authentication and authorisation • Live Demos - related to common web threats - commonly identifiable threats to data safety on websites B. Introduction to physical security – • Definition, design, best practices to protect critical assets, requirements • Case Studies with videos Short quiz at the end of day 1	7 hours
Day 2	A. Overview of threat landscape on Information Security layers How to assess and mitigate threats especially in education sector B. Hands on practical • Testing data breach of email ids and personal information • Password strength • USB killer demo • Live phishing • Mail spoofing identification C. Practical to help identify and mitigate web threats • Cross site scripting (XSS) • Spoofing • Sqlmap demo • Mitigating Xss	7 hours

	• Sql injection • Broken auth and session management Short quiz at the end of day 2	
Day 3	A. Introduction to cryptography and digital signatures Hands on tools – • Hashcalc, • Quick stego, • Basics of encryption, • Symmetric asymmetric key, • Public and private key • Digital Certificates • Digital Signature B. Introduction to Cyber Threats , Cyber laws • Important IT laws • Civil wrongs • Crimes and related punishments • RBI zero liability policy Case Studies and Discussions Short quiz – Day 3	7 hours
Day 4	A. Latest cyber security threats, scams and frauds • Case studies - UPI frauds, remote access frauds, online gaming frauds, Sim Swap, Romance/matrimony frauds, education scholarship frauds. • Ways to mitigate B. Threats - to physical security and information security specifically faced by educational institutions and ways to mitigate TTP for: • End point protection, • WiFi protection, • Devices protection, • Data and backup,	7 hours

	• Computer protection, • Perimeter protection Case studies and videos related to scams frauds and attacks Short Quiz – Day 4	
Day 5	A. Cyber Etiquette and Cyber Hygiene • Various aspects of securing the Assets with People as major force to prevent attacks • Proactive defence • Incentives and Penalties for following the cyber policy of the organisation B. Recommended best practices for • Cyber security - data security, data backup and recovery, social media best practices • Specific focus on how to help identify instances of cyber bullying and harassment students face • Helpline and redressal - how to report via helpline 1930 and cybercrime.gov Recap + Short Quiz Day 5	7 hours

Course structure – Intermediate

	Intermediate Course Topics	
Day 1	A. Recap of Basics B. Introduction to Mobile security - • mobile security basics, • mobile vulnerability assessments, mobile security best practices - wifi security, application managements, location and privacy management, password management, • OWASP top 10 security risks, • types of malicious threat vectors • Short Quiz 1	7 hours

Day 2	A. Intro to OSINT Framework	7 hours
	- various open-source tools that can be used for gathering intelligence reports, securing data and personal information online and offline B. Hands on • setting up of firewalls, • confirming firewalls, • anti virus software evaluation, • malware detection and • removal in mobile devices Short quiz – Day2	
Day 3	A. Identity and Access Management • IAM solutions overview • Identity management need for security • Access controls models • Access control tools B. Data Privacy, Data Security and Data Protection • Data Privacy requirements – in context of DPDPA • Data Security concepts – at rest, in motion and deletion • Data Protection – need for the same with robust and well tested systems • Data Privacy vs. Data Security – case study • Data Security vs. Data Protection – case study Short Quiz – Day 3	7 hours
Day 4	A. Introduction to cloud security • what is cloud, • how is our data stored, • Models - SaaS, IaaS, PaaS, • Risks of cloud and how to mitigate B. Incident response planning and management - specifically in the context of educational institutions Short Quiz 4	7 hours
Day 5	A. Introduction to cryptocurrencies and bitcoins -	7 hours

	- wallets, address, transactions - scams and frauds online, - how to transact safely, - how to protect bitcoins, - RBI policies and regulations, - block chains and hash functions, - bitcoin privacy model B. Cyber security design and maintaining resilience - specifically in the context of education industry along with best practices Short Quiz 5	

Pre-assessment & information prior to the training

IITM Pravartak will offer a tailored and flexible approach to teacher training, addressing several current challenges in cyber space. Teachers (Training participants in this case) often don't get time to go through handbooks. So, every day at the end of the day, a summary of learning will be provided with a heads-up of next day content. IITM Parvartak will engage with training participants 1 week prior to the program with a pre-assessment & using this method.

Proposed Schedule of Training Programs

Batch #	Name of the training program	Date	# of Participants
1.	Cyber security Essentials – (Basic Course)	16th Dec 2024 – 20th Dec 2024	200
2.	Cyber security Essentials – (Basic Course)	23rd Dec 2024 – 28th Dec 2024 No class on 25th December	200
3.	Cyber Security Essentials – (Intermediate Course)	30th Dec 2024 – 4th Dec 2024 No class on 1st January	100
4.	Cyber security Essentials – (Basic Course)	6th Jan 2025 – 10th Jan 2025	200
5.	Cyber security Essentials – (Basic Course)	20th Jan 2025 – 24th Jan 2025	200
6.	Cyber Security Essentials – (Intermediate Course)	27th Jan 2025 – 31st Jan 2025	100
7.	Cyber security Essentials – (Basic Course)	3rd Feb 2025 – 7th Feb 2025	200
8.	Cyber security Essentials – (Basic Course)	10th Feb 2025 – 14th Feb 2025	200
9.	Cyber Security Essentials – (Intermediate Course)	17th Feb 2025 – 21st Feb 2025	100
10.	Cyber security Essentials – (Basic Course)	24th Feb 2025 – 28th Feb 2025	200
11.	Cyber security Essentials – (Basic Course)	5th May 2025 - 9th May 2025	200
12.	Cyber Security Essentials – (Intermediate Course)	12th May 2025 – 16th May 2025	100
13.	Cyber security Essentials – (Basic Course)	19th May 2025 – 23rd May 2025	200
14.	Cyber security Essentials – (Basic Course)	26th May 2025 – 30th May 2025	200

15.	Cyber Security Essentials – (Intermediate Course)	2nd Jun 2025 – 6th Jun 2025	100
16.	Cyber security Essentials – (Basic Course)	9th Jun 2025 – 13th Jun 2025	200
17.	Cyber security Essentials – (Basic Course)	16th Jun 2025 – 20th Jun 2025	200
18.	Cyber Security Essentials – (Intermediate Course)	23rd Jun 2025 – 27th Jun 2025	100