MEMORANDUM OF UNDERSTANDING

Between

Indian Computer Emergency Response Team (CERT-In)

And

National Institute of Electronics & Information Technology (NIELIT)

This Memorandum of Understanding (hereinafter referred to as "MoU") is made as on ____ 2023 (the "Effective date"), between Indian Computer Emergency Response Team(CERT-In), Ministry of Electronics& Information Technology (MeitY), Government of India having its office address at Electronics Niketan, 6, CGO Complex, Lodi road, New Delhi-110003, India (hereinafter referred to as 'CERT-In'); and The National Institute of Electronics & Information Technology, an Autonomous Scientific Society under the administrative control of Ministry of Electronics & Information Technology (MeitY), Government of India having its office address at NIELIT Bhawan, Plot No. 3, PSP Pocket, Sector-8, Dwarka, New Delhi-110077 (hereafter, referred to as "NIELIT"). CERT-In and NIELIT are hereinafter collectively referred to as 'Parties' and individually as 'Party'

Article 1

Preamble

Digitalization has increased the need for skilled Cyber security manpower across all countries. The demand for skilled Cyber security professionals is on the rise. To enhance the Cyber resilience of India, capacity building is highly required in the area of Cyber security. The recent Indian educational policy framework, including the National Education Policy 2020, underlines the need for building skill-based capacity in the Indian youth through leveraging the capacity and capability of different institutions. To harness the same, it is important for Academia and Industry to enter into formal collaboration and MOUs for capacity building. There is a need for a strong collaboration between the universities and industries to come up with innovative ideas to enrich the R&D ecosystem. This MoU aims to bring together the industry, institutions and academia for the development of better and skill oriented all round professionals in the area of Cyber security to contribute to national development and Cyber resilience.

Article 2

Objective

i. To increase Industry- Academia Cooperation in the area of Cyber security

ii. To generate skilled manpower in all the related domains of Cyber Security.

iii. To enhance the Infrastructure for Capacity Building and R&D in emerging areas.

iv. To develop solutions to improve Cyber resilience.

Article 3

Engagement and Scope

The scope of the Memorandum of Understanding is as under –

a) **Launch of Certification Courses:**

I. **Development and Design:** CERT-In and NIELIT will collaborate to create course curriculum that aligns with international standards, and cater to the demand in all related domains of cyber security, such as Information Security, Cyber forensics, Incident Response, Cyber Hygiene, Cyber threat Intelligence, Malware analysis, Cyber security assurance, Internet of Things (IoT) Security, Industrial Control Systems (ICS) security, Artificial Intelligence (AI) for Cyber security, Cyber Resilience, Ransomware awareness and mitigation and other emerging areas in Cyber security. This includes course content, assessment methods, practical applications, and case studies.

II. **Validation and Accreditation:** Ensure the courses meet the standard and regulations set by relevant accreditation bodies, ensuring high quality of education and industry recognition.

III. **Training and Development:** Jointly organize and conduct workshops, seminars, and training sessions for educators to ensure high-quality delivery of the course content. To design and deliver training and certification programme in the Cyber Security & related fields for students, academicians and industry professionals at the National and International level.

b) **Virtual Lab in Cyber Security:**

I. **Development of Lab Environment:** Establish a secure and realistic lab environment to simulate real-time cyber security attacks and mitigation efforts, which will act as a learning platform for students, academicians and industry professionals at the National and International level.

II. **Lab Equipment and Tools:** Identify and procure the necessary software and hardware to support the real-time simulation of cyber-attacks, and to equip students with the skills to detect, prevent, and respond to these threats in real time.

III. **Training and Simulation Exercises:** Develop a series of hands-on training exercises that simulate real-world attack scenarios. These exercises should provide students with practical experience in identifying and mitigating cyber threats.

c) **Integration of emerging technologies in Cyber Security:**

The Emerging technologies such as AI, Blockchain and Cloud computing will be utilized to develop courses, Infrastructure and solutions for Incident Response and mitigation, Cyber Forensics, Cyber Threat Intelligence, Cyber security assurance, Security Operations Centre (SOC) management, Managerial and Top Level management & Decision making.

d) **Joint Research and Development:**

I. **Innovation in Cyber Security:** Foster an environment for innovation and research, encouraging the development of novel solutions in the field of cyber security.

II. **Collaboration on Research Projects**: CERT-In and NIELIT will work on the on cutting-edge technology in the area of Cyber security to promote knowledge exchange and research outcomes.

e) **Knowledge and Resource Sharing:**

I. **Resource Sharing:** Share resources and expertise for the betterment of course delivery and practical labs, creating a rich learning environment for students.

II. **Collaboration on Events and Seminars:** Collaboratively host cyber security events, seminars, and conferences to promote awareness, share knowledge, and drive engagement within the cyber security community.

III. **Costs**: Any costs or fees that either Party may have to incur in relation to such exchange including travel & other expenses will be borne by the parties as per the organizational procedure of each party.

f) **Review and Assessment:**

I. **Quality Assurance:** Regularly review and update the course curriculum and lab exercises to ensure they remain relevant, comprehensive, and aligned with industry trends and advancements.

Article 4
Intellectual Property

All Intellectual Property, including, but not limited to, copyrights, software and database rights, patents, trade secrets, trademarks, rights in designs and all other Intellectual Property or other proprietary rights ("Intellectual Property") owned by one Party prior to the date of this MOU will continue to be owned by that party. All Intellectual Property rights made available by one Party to the other Party in connection with this MOU, or otherwise, will remain the sole property of, and vest in, the first Party or its licensors. Neither Party will gain, by virtue of this MOU, any rights in or to any Intellectual Property rights owned by the other Party. Any Intellectual Property rights created by one Party without use of or reference to the Intellectual Property rights or Confidential Information of the other Party will be and will remain the sole and exclusive property of the first Party.

Article 5

Validity/Duration of Engagement

a) This MOU will be valid for a period of three (3) years from the date of last signing.

b) After the expiry of the validity of the MoU, the MoU may be extended for another three (3) years term through mutual written consent.

c) If for any reason, any one of the party is not interested to continue the MoU, the same can be informed to the other party by giving one month (30 days) in advance by writing.

d) Any party may request making amendments to this MOU, provided that such amendments shall be mutually agreed upon between the parties hereto under a written document, to the extent that the document shall thereafter be an integral part thereof.

Article 6
Governing Law and Dispute Resolution

(a) Both the NIELIT and CERT-In agree that provisions/content in this MoU do not create any legal obligations between the parties.

(b) In the event of any misunderstanding and differences between the parties hereto, such misunderstanding/differences shall be resolved amicably by mutual discussions.

(c) It is, hereby, agreed between NIELIT & CERT-In that if any dispute arises between the parties which is not resolved with mutual consent, the mediation or conciliation will be done by an officer at the level of Additional Secretary in MeitY.

In Witness Where of, the Parties have set their hand sand seals here to on the day and date first mentioned.

NIELIT

By: _____ 04/09/2023

Name: **Dr. Madan Mohan Tripathi**

Title: Director General

Witness: (ALOK TRIPATHI)

1. Alok Tripathi
Director (Technical)
NIELIT
4.9.2023

CERT-In

By: _____ 4/9/2023

Name: **Dr. Sanjay Bahl**

Title: Director General

Witness:

1. S. S. SARMA
S.S.SARMA
Director (Operations), CERT-In
4.9.23