Cybersecurity for ALL (CS4ALL) Project

Terms of Reference for External Evaluator

Project Information

Project Title	Cybersecurity for all
Project acronym	CS4ALL
Coordinator	Prof. Aman Mittal, LPU
Project Start Date	July,2023
Project Duration	36 months
Work Package	WorkPackage7: External Evaluation
Work package leader (Institution)	LPU

Project Partners

Sr. No	Partner Name	Country
1	LOVELY PROFESSIONAL UNIVERSITY	India
2	EDULAB EDUCATIONAL EXCHANGE PRIVATE LIMITED	India
3	LOKMANYA TILAK JANKALYAN SHIKSHAN SANSTHA NAGPUR	India
4	GUJARAT UNIVERSITY	India
5	EDEX - EDUCATIONAL EXCELLENCE CORPORATION LIMITED	Cyprus
6	UNIVERSITAT POLITECNICA DE VALENCIA	Spain
7	VISOKO UCILISTE ALGEBRA	Croatia
8	POKHARA UNIVERSITY	Nepal
9	FAR-WESTERN UNIVERSITY	Nepal
10	Dirghayu Nepal	Nepal
11	ACTIONAID NEPAL	Nepal
12	INSTITUT PERTANIAN BOGOR	Indonesia
13	YAYASAN PENDIDIKAN JAYA	Indonesia
14	Chikitsak Samuha's Sir Sitaram and Lady Shantabai Patkar College of Arts & Science and V. P. Varde College of Commerce & Economics	India

CS4ALL Project Description

The EU's Cybersecurity Strategy in the Digital Decade adopted on 16 December 2020 has among its main aims to strengthening collective capabilities to respond to major cyberattacks. In order to enhance cybersecurity resilience for SMEs, upskill EU workforce and reach the 2030 targets of the Digital Decade, the main goals are:

1. Putting people and their rights at the centre of the digital transformation

2. Supporting solidarity and inclusion

3. Ensuring freedom of choice online

4. Fostering participation in the digital public space

5. Increasing safety, security and empowerment of individuals

6. Promoting the sustainability of the digital future

Cybersecurity is everyone's problem. Everyone has a role to play in ensuring our collective cybersecurity. It is also essential to prepare the public to protect themselves against cyberthreats, for instance through national campaigns to raise cybersecurity awareness across the general population. There are four primary groups such a campaign ought to target: First, cybersecurity should feature in the educational curriculum for students – digital natives – so they can practice vigilance from a young age. For that, teachers with adequate competences and skills are necessary. Second, the general public must also be made aware of cyberthreats and how to mitigate them. This can be done through engagement with the community, events at the sub-district or provincial level. Third, with comprehensive lifelong learning programs, the private sector could then be encouraged to improve their baseline cybersecurity standards in their respective scopes of business. Lastly, policymakers who have the authority to pass laws and regulations and to allocate the state's budget should be aware of the impact of cyberattacks and the need to act sooner rather than later, so NGOs in the project responsible for dissemination can be a step closer to proposing pro-cybersecurity policies through local authorities. Mandates could be established by law, either through bills or the National Education System Law to integrated cybersecurity programs in these countries at least at basic level. However, changes in regulations would be out of the scope of this project.

HEIs may serve as beacons of information for society. Many universities now offer courses on cybersecurity as a minor and, more and more, as a major. With the increase digitalisation of society, transaction, communication, exchange the number of crimes taking place or using cyber tools (malware) of also increased as mentioned previously. Thus, it is only natural that universities playing their role of learning, research and innovation beacon have already developed tools, processes to help both the civil society, governments and private companies with their challenges in cybersecurity. Not only HEIs do provide formal education within the aspect of cyber security but they should also playing a pivotal role to educate and train the society we are living in.

AIMS:

There are several key aims of the project

- Provide excellent and frontier knowledge to students majoring in Informatics-related study program within the area of cyber security. This will be achieved through curriculum revision which entails modification of existing courses and creating new ones to cater for the rapid development of the fields;

- Provide education and training for SMEs to manage their digital platform safely;

- Create public awareness campaign on the issue of cybercrime and threats;

- Establish a cyber information portal (within the website) in which society can gain information and connect to experts for advice in cyber safety-related issues.

The aim of the project is thus to give an answer to the lack of sensibilization to current risks, updated content on cyber security courses to two important target groups: academic staff and students and workers. Both populations are frequent and big users of connected devices for personal, educational and professional reasons. The project will give academic staff and students and workers the content on cybersecurity in order to increase the awareness in the fields, impart knowledge of basic principles on cybersecurity, create mindsets and attitude for safe online presence. To achieve this, the project will identify key data points and create and update modular courses for graduate students and Lifelong learning micro-credentials for adult learners and professionals. The expected shift from the current situation is to have more cyber security ready higher education institutions, more students and individuals with basic and advanced knowledge in cybersecurity. Dissemination events by NGOs will also create events and activities towards a younger population which tends to be preferred targets of both cybercrime but also predatory practices from apps (loot boxes, micro transactions, abusive privacy policies, etc). Side effects that could arise from the programme are more robust cyber security policies in universities, private and public sector as well as legal frameworks.

The project builds up on the work done by the European Commission on Digital Security and update/create modular courses in computer sciences programs based on competences and skills for future security analysts. Likewise, one of the innovations is to develop a European approach in Asia to micro-credentials applied to cybersecurity skills as announced in the Council Resolution on a strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030), the European Skills Agenda and the Digital Education Action Plan (2021-2027). Likewise, the partners will follow the recommendations from the MICROBOL project for the European Commission's proposal for a Council recommendation on micro-credentials for lifelong learning and employability the EU Public consultation on "Micro-credentials – broadening learning opportunities for lifelong learning and employability". The project goes further using the framework to prepare a roadmap that leads to formal recognition of LLL courses by software companies, SMEs and startups as direct and tangible result of the project. The project enhances a collaborative environment between EU and Asian partners using a train-the trainer methodology with coaching approach where UPV, ALG and UNIC will supervised the design and development of modular courses by their counterparts in Nepal, Indonesia and India respectively. Employability will be enhanced both in the classroom (through adequate teaching/learning methods) and outside the classroom (through complementary work placements either in software companies, SMEs or startups). The project will develop LLL courses for adult learners and workers at beginner and advanced level. Thus, CS4ALL will build capacity in Nepalese, Indian and Indonesian HEIs within the above-mentioned priorities by developing/modernizing innovative curricula in computer sciences following ADDIE methodology; training their academic staff in the new/updated courses with appropriate pedagogic methods and modern software and security analysis techniques; developing an online learning environment to support students, academic staff and Lifelong learners during and after the project. Additionally, the added value of CS4ALL is its contribution to society thanks to the cooperation with 4 NGOs for raising awareness of cyber threats and how to combat it among civil society and vulnerable groups (e.g. digital illiterate population and young population) through a specific communication and dissemination campaign as explained in the corresponding section (3.2). The proposal is not based on any previous or ongoing projects by any of the partners but is the result of the need analysis elaborated by the Asian partners.

Specific Objectives

. The wider goal of the project will be achieved through completion of the set of specific objectives concerned with the areas where the measures should be applied:

- at national level, providing better understanding of cybersecurity threats and risks that poses for organizations and society at large

- at institutional level, establishing and improving integrated modular courses in cybersecurity while fostering university-enterprise cooperation focusing particularly on security analysis and data protection skills set and employability schemes.

-at faculty level/staff, retraining specialists and forming future teachers through the engagement of faculty, staff and students with local, national and EU experts. Herein, CS4ALL will be used as a tool for continuous professional development. The project will address the process of recognition and validation of those new/updated courses as well as the period of practices. The consortium during the preparation of the proposal acknowledges the different stages of development across the partners.

Objectives of the External Evaluator

The Primary task of the External Evaluator for the CS4ALL project is to supervise the Quality Plan of the project in terms of implementation of the project activities by all the partner institution and to offer assessment on various project aspects referring to the following responsibilities and tasks:

General responsibilities of the External Evaluator (EE):

1. Be the Chair of the Quality and Ethics Board and lead the Quality and Ethics Board (QEB).

2. Attend all the Quality and Ethics Board meetings.

3. Along with the QEB members, the EE, will evaluate the quality and progress of the project activities and outputs, to ensure these are executed as per the standards promised in the Logical Framework Matrix and work plan specified in the project document.

4. Provide necessary feedback on the project progress, project implementation and project documents.
5. Support the Work Package Leader/ Risk Owners in the process of Risk Management Plan and Managing Risks. The support is in terms of identification of potential risks and design alternatives scenarios “Plan Bs”/ contingency plan. Details of additional responsibilities are laid out in the CS4ALL Risk Management Document.

6. Raise issues related to the Risk Management Process as one of the main agenda during the regular QEB meeting.

7. Escalate items of major risks which have an impact on overall project execution needs to be the Project Management Board through the Project coordinator.

8. Resolve and manage any ethical issues during the project for all the project partners.

9. Ensure all the issues raised by the project partners are freely discussed & are adequately managed.

10. Support the project coordinator in Quality & Ethics Control to develop the quality plan and the feedback mechanisms/processes to ensure that a good basis for quality assurance is available for the CS4ALL project.

11. Write & submit three reports (one after each year). Each report should evaluate the following items: timeliness of delivery of outputs, each output & product produced according to completeness, usefulness for target groups, impact they can achieve, communication & work ethics among the partners.

12. The EE should be updated with the project progress and understand the project requirements.

13. Report to the CS4ALL Project Coordinator on any issues related to the work assigned.

The External Evaluator can schedule independent meetings with all partners as and when required for the project related tasks. The project management board is responsible to provide all project documents and deliverables to the external evaluator on request.

Expertise needed:

1. Experience in working as an External Evaluator for any of the Erasmus projects.

2. Knowledge and understanding of Erasmus projects.

3. Research experience in the field of higher education.

4. Knowledge and understanding of project monitoring and evaluation.

5. Experience in writing project-based evaluation reports.

Duration of the project: 36 Months (2023-2026).

Expert's fee: Defined by the CS4ALL project and the fees shall be paid annually after the submission and final assessment by the coordinator.

Document submission:

1. CV (Euro pass format)

2. Motivation letter

Deadline: 10/11/2023

Procedure: Documents should be sent to the Work Package leader (External Evaluation) at eucs4all@lpu.co.in