

**Memorandum of Understanding on Cyber Security Cooperation**  
**between the Information System Authority of the Republic of Estonia and**  
**RedCLARA - Cooperación Latino Americana de Redes Avanzadas**

RedCLARA - Cooperación Latino Americana de Redes Avanzadas - and the Information System Authority of the Republic of Estonia (RIA) - (hereinafter referred to collectively as "Participants" and individually as "Participant");

Desiring to further develop co-operation and consolidate existing friendly relations between their two institutions;

Noting their continuing shared vision in fostering the Latin America and the Caribbean region's digital transformation, strengthening of cybersecurity, promoting the increasing academic, research, economic and social benefits accruing from the growth in use of an open, peaceful and secure cyberspace where the same rights people enjoy offline are also protected online;

Recognising the threats posed to the nations and specifically academic institutions and networks by malicious cyber activity and the importance of raising awareness of these threats;

Recognising the indivisibility of cyberspace and the shared interest in the protection of critical infrastructure and ensuring a safe and reliable academic Internet that supports science, research, innovation and economic and social development;

Given the fact that Information Security is of great value to the academic networks that are members of RedCLARA and to the institutions that form part of these networks;

Recognising that the collaboration between the Participants would be channelled through the EU CyberNet project (EU Service Contract No. IFS/2019/405-538), implemented by RIA. Noting that EU CyberNet was launched with the purpose to strengthen the global delivery, coordination and coherence of EU's external cyber capacity building projects, and to reinforce EU's own capacity to provide technical assistance to partner countries in the field of cybersecurity and cybercrime, including through the EU CyberNet-managed Latin America and the Caribbean Cyber Competence Centre (LAC4) inaugurated in May 2022 in Santo Domingo, the Dominican Republic.

Recognizing that the EU CyberNet is tasked to provide enduring lead support to the establishment and operationalisation of the LAC4 that serves as a focal point for sharing EU's collective expertise in the region, building up local capacity, facilitating collaboration on joint projects and actions, and promoting the benefits of an open, free and inclusive cyberspace.

Acknowledging the Participants' common interest in addressing these international challenges and collaborating to strengthen cyber security;





Recognising the benefits of close cooperation between government, academia and the private sector in sharing expertise, research and working to secure the future of cyberspace internationally;

Building on the existing collaboration between RedCLARA and the EU through the BELLA Programme and previous initiatives;

The Participants have reached the following understanding:

## 1. Introduction and Purpose

This Memorandum of Understanding (hereinafter referred to as “MoU”) has its purpose in promoting cooperation in the field of cyber security between the Participants based on the principle of equal benefit and mutual interest.

## 2. Scope of Collaboration

The Participants will cooperate on the following areas:

**Cyber security skills:** Work together to improve cyber security professional development and build a cyber security skills base; encourage experts from RedCLARA member institutions to join the EU CyberNet Experts Pool with the possibility to engage in EU CyberNet cyber capacity building missions in partner countries, as appropriate.

**Sharing of best practices:** Share good practices on the approach to cyber and digital technology, including (but not limited to) information on cyber governance and processes and information related to the cyber security of emerging critical technologies; consider ways to address the cyber security risk associated with Digital Service Providers (such as managed service providers, cloud service providers and critical software vendors) and their customers in the LAC Research and Education Networks environment;

**Capacity building:** Work together to design and deliver cyber security training; RedCLARA will contribute with its infrastructure and facilities to host and promote LAC4 skills training and identify additional complementarities in topics related to cybersecurity;

**Operational delivery:** Coordinating and facilitating cooperation with national institutions, industry, academia, civil society and the private sector to support involvement of these organisations in the activities organised or facilitated by the Participants.

Promoting the LAC4 and the EU CyberNet project mission in international events and forums.

Contributing to the identification of cyber capacity building needs and the development of the LAC4 training curricula and other activities to support cybersecurity endeavours of the LAC region.;

**EU CyberNet** [www.eucybernet.eu](http://www.eucybernet.eu) [eucybernet@ria.ee](mailto:eucybernet@ria.ee)



Any other cooperative activities jointly decided by the Participants.

### **3. Confidentiality and intellectual property**

Without prejudice to the existing legal provisions on free access to public information, all information exchanged shall be treated with the utmost confidence and neither party shall disclose any confidential information obtained as a result of their cooperation.

The title to, and intellectual property rights in, or in relation to, any document or material supplied by one Party to the other Party under this MoU will remain with the Party supplying the document or material.

In the event the Parties will engage in joint activities that may result, intentionally or unintentionally, in the creation of items of intellectual property the Parties will enter into a separate agreement governing such joint intellectual property rights.

### **4. Use of Logo and Name**

Neither Party shall use the name, logo(s), trademarks, or other representation(s) of any kind of the other Party without the prior written approval of the other Party. In any such statement, the relationship of the Parties shall be accurately and appropriately described, as previously agreed by the Parties in writing.

### **5. Entry into Effect, Duration and Termination**

This MoU will come into effect on the date of signature indicated herein and will remain in effect until the date of completion of the EU CyberNet project, currently scheduled for August 2025, unless terminated by either Participant giving at least one (1) month's prior notice in writing to the other Participant.

### **6. Non-Legally Binding**

This MoU does not constitute or create and is not intended to constitute or create any legally binding obligations. Nothing in this MoU will alter or affect any existing agreements between the Participants.

Without prejudice to the generality of the immediately preceding paragraph, the Participants acknowledge that this MoU will not be deemed as an international agreement and will not constitute or create legal obligations governed by international law.





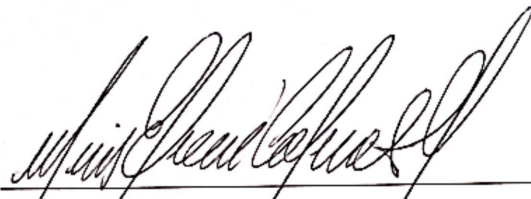
This MoU is not intended to conflict with national or international law; In case of conflict, national or international law will take precedence over the terms of the MoU.

## 7. Amendments

Either Participant may propose an amendment to this MoU by means of written notice to the other Participant. An amendment will be effected only upon the mutual written consent of the Participants.

SIGNED in duplicate in the English language.

For RedCLARA:



Luis Eliécer Cadenas Marín  
Executive Director

Date: 5-10-2022

For the Estonian Information System  
Authority:



Gert Auväart  
Director of Cyber Security  
on the authority of the Director General

Date: 20.09.2022