"Institut Cybersécurité Occitanie"

Key Challenge Project

2024 CALL : "Support to scientific and outreach cybersecurity events "

Context and objectives

The "Institut Cybersécurité Occitanie" (ICO) Project was launched in January 2022. ICO is a multidisciplinary initiative that aims to gather and federate key players in cybersecurity, from academia and industry, in order to position the Occitanie region among the top leaders in this field in France as well as at the international level. The Institute aims to stimulate upstream research, develop training and promote collaboration and innovation with industry.

The ambition of this project is to privilege the application sectors that are historical markers for the Occitanie region: in particular, aeronautics, automotive, space and healthcare. Another strong differentiator of the Occitanie ecosystem concerns the interdisciplinarity of the research conducted, which covers computer science, mathematics as well as legal, social and business-related aspects of cybersecurity.

The Institute is funded by the Occitanie Region for 5 years. The funding includes the support of research actions through open calls for PhD and postdocs scholarships, funding for engineers to implement research demonstrators and prototypes scientific projects and travel grants mobility cofinancing, as well as the support for organization of scientific and outreach events and education initiatives that contribute to enhancing the visibility and attractiveness of the cybersecurity ecosystem in the Occitanie region. Proposals involving different labs or multidisciplinary topics are highly encouraged.

Scope of the call

One of the goals of the ICO is to increase the visibility and attractiveness of the cybersecurity ecosystem in the Occitanie region at the regional, national and international levels. Accordingly, this call is aimed at sponsoring and offering financial support to the organization of regional, national or international scientific events (conferences, workshops, summer schools, …) as well as education related initiatives and events aimed at dissemination of cybersecurity culture and increasing awareness about related threats and protection techniques.

Eligibility rules

- The supported events must take place in the Occitanie region. Applications should be submitted by a member of a research lab in the Occitanie region involved in research activities in cybersecurity. The list includes: ENAC, CEA, Équipe de droit pénal et sciences forensiques de Montpellier (UR 212 UM), IES (UMR 5214 CNRS/UM), IDETCOM (EA 785 UT CAPITOLE), Institut de droit privé (EA 1920 UT CAPITOLE), IMAG (UMR 5149 CNRS/UM), IMT (UMR 5219 CNRS/INSA/INUC/UT CAPITOLE/UT2/UT3), IRIT (UMR 5505 CNRS/INP/UT3/UT CAPITOLE/UT2), ISAE-SUPAERO, LAAS-CNRS (UPR 8001), Laboratoire de Droit Privé (UR 207 UM), LERASS (EA 827 UT3), LIRMM (UMR 5506 CNRS/UM), TSE-R (UMR 1415UT CAPITOLE/CNRS/INRAE/EHESS). Other labs that are not listed can also apply.
- For scientific events, priority will be given to events with international and national scope and aimed at enhancing collaboration between several partners at the regional level. The applicants requesting ICO support must be members of the organizing committee or the scientific committee of the event.
- Events related to the dissemination of scientific culture can be local. They can target one of the following audiences: school children, students, young people, teachers, general public / citizens.
- The following criteria will be considered for the assessment of applications:

  - The scientific reputation of the event or for scientific outreach events, its expected impact;
  - The contribution of the event to strengthening the visibility and attractiveness of the cybersecurity ecosystem in the Occitanie region
  - The encouragement of the participation of young researchers and students
  - The collaborative dimension with other ICO partners.

Obligations of the event organizer

- The event organizer shall ensure that the ICO logo appears on all communication materials related to the event (printed and electronic documents).

- Every publication related to the supported event shall include the following acknowledgement:

  "This work was supported by ICO, Institut Cybersécurité Occitanie,
  funded by Région Occitanie, France"

Financial support

The ICO Executive Committee will decide on the amount of financial support granted to the event based on the requested budget, taking into account the nature of the event, the number of participants, the expected impact of the event and the financing plan.

Application

Deadline and selection

- ICO will organize 3 calls per year, with **deadlines of September 30th, January 31st and May 31st** of each year.

- Applications will be assessed by the ICO Executive Committee and the applicants will be notified within 2 to 3 weeks after the deadline of each call for participation.

How to apply

Formal applications should include:

- Title of the event, date and location, target audience and estimated number of attendees
- Description of the objectives and scope of the event
- Provisional program including the names of confirmed and prospective speakers, themes/disciplines addressed and link with ICO topics of interest
- Estimated budget and use of ICO support if granted
- Other financial support obtained/ requested.

Applications should be submitted as a single file with a maximum size of 10 Mo. The file name should be the following:

ICO_Events_Acronym_ApplicantName.pdf

Send the pdf file by email to: bureau@ico-occitanie.fr

Contact

For more information about the call, please send an email to: bureau@ico-occitanie.fr