



## Défi clé

# « Institut Cybersécurité Occitanie »

## Appel 2024 : « Allocations Post-Doctorales »

---

### Contexte et objectifs

Le défi clé « Institut Cybersécurité Occitanie » (ICO) a été lancé en janvier 2022. L'ICO est une initiative pluridisciplinaire qui vise à rassembler et fédérer les acteurs de la cybersécurité, du monde académique et de l'industrie, afin de positionner la région Occitanie parmi les leaders dans ce domaine en France ainsi qu'au niveau international. L'Institut a pour objectif de stimuler la recherche amont, de développer la formation et de favoriser la collaboration et l'innovation avec les industriels.

L'ambition de ce projet est de privilégier les secteurs applicatifs qui sont des marqueurs historiques pour la région Occitanie : notamment l'aéronautique, l'automobile, le spatial et la santé. Un autre différenciateur fort de l'écosystème Occitanie concerne l'interdisciplinarité des recherches menées, qui couvrent l'informatique, les mathématiques ainsi que les aspects juridiques, sociologiques, géopolitiques et économiques de la cybersécurité.

L'Institut est financé par la Région Occitanie pour 5 ans. Le financement comprend le soutien d'actions de recherche par le biais d'appels ouverts pour des bourses de doctorat (50%) et de post-docs, des projets scientifiques et des cofinancements de mobilité, ainsi que le soutien à l'organisation d'événements scientifiques, de sensibilisation et d'actions de formation qui contribuent à renforcer la visibilité et l'attractivité de l'écosystème de la cybersécurité dans la région Occitanie. Les propositions impliquant différents laboratoires ou des sujets interdisciplinaires sont fortement encouragées.

---

### Bénéficiaires

Le projet de post-doc doit être réalisé dans un laboratoire de recherche de la région Occitanie, avec la possibilité d'être également cofinancé par un partenaire industriel. Les projets collaboratifs, impliquant plus d'un partenaire au niveau de la région, sont encouragés.

---

### Règles d'éligibilité

Le projet doit satisfaire les conditions suivantes :

- Il doit se dérouler dans un laboratoire de recherche de la région Occitanie en cybersécurité. La liste inclut : 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 1415 UT CAPITOLE/CNRS/INRAE/EHESS). D'autres laboratoires sont également invités à répondre à cet appel.

- Les contributions peuvent couvrir différentes disciplines incluant l'informatique, les mathématiques ainsi que des aspects juridiques, sociaux, géopolitiques et économiques de la cybersécurité.
- Le sujet de recherche devra cibler, à court, moyen ou long terme, des défis répondant à un ou plusieurs des objectifs de recherche suivants :
  1. Renforcer la sécurité des matériels, des logiciels et des systèmes.
  2. Assurer la sécurité des futurs réseaux et environnements connectés/technologies émergentes.
  3. Mieux protéger les données et la vie privée, et améliorer la confiance dans les réseaux sociaux.
  4. Améliorer la conception par des approches formelles et étudier l'impact/contribution de l'intelligence artificielle.

Les critères suivants seront également pris en compte (la liste n'est pas exhaustive):

- L'originalité des sujets de recherche et leur évolution par rapport aux travaux de thèse.
  - La qualité du parcours académique des candidats et de leurs publications.
  - Le changement d'environnement de travail des candidats favorisant la mobilité dans les laboratoires en Occitanie (a minima) pour travailler sur de nouveaux projets.
  - La promotion de la collaboration Occitanie Est-Ouest.
  - La qualité des dossiers dans une perspective d'un recrutement CNRS ou MCF à l'avenir.
  - Les candidatures internationales ou candidats ayant effectué leurs travaux de thèse en dehors de l'Occitanie répondant aux critères d'éligibilité pertinents.
- 
- Les publications issues des projets retenus devront inclure le texte de remerciement suivant :

*« Ce travail a bénéficié du soutien de l'ICO, Institut Cybersécurité Occitanie, financé par la Région Occitanie, France »*

---

## **Financement**

- Les dépenses éligibles concernent le salaire brut du post-doctorant ou de la post-doctorante sur la base des salaires CNRS selon l'expérience.
- Un complément de 5 k€ sera attribué pour les frais de fonctionnement associés.
- Le financement peut couvrir une durée maximale de 18 mois (en cas d'interruption, le montant du financement non utilisé sera restitué à l'ICO).

---

## **Modalités et dossier de candidature**

### **Calendrier et procédure de sélection**

- L'ICO organisera 3 appels par an, avec comme date limite les **31 janvier, 31 mai et 30 septembre de chaque année**, jusqu'à la consommation de l'enveloppe allouée.
- Les demandes seront évaluées par le Comité Exécutif de l'ICO dans un délai de 2 à 3 semaines à compter de la date limite de chaque appel à participation.
- Notification : quelques jours après la réunion du Comité Exécutif.

### **Dossier de candidature**

Le dossier doit inclure les éléments suivants :

- CV détaillé du candidat ou de la candidate
- Lettre de motivation
- Description du projet de post-doc
- Manuscrit de thèse et deux exemples de publications
- Deux lettres de recommandation
- Une lettre de soutien de l'équipe de recherche d'accueil expliquant en particulier comment le projet de post-doc contribuera au programme de recherche de l'équipe.

La description du projet de post-doc doit être structurée selon le plan suivant :

- Titre
- Contexte, objectifs et positionnement par rapport à l'état de l'art
- Approche proposée
- Positionnement par rapport aux objectifs de l'ICO
- Direction : Nom des encadrants, laboratoire, équipe de recherche.

Les dossiers de candidature doivent être transmis en un seul fichier pdf (taille max. 10 Mo), en nommant le fichier comme suit :

AnnéeICO\_PostDoc\_Acronyme\_NomEncadrant.pdf

Candidatures à transmettre par email à : [bureau@ico-occitanie.fr](mailto:bureau@ico-occitanie.fr)

---

## Contact

Pour toute demande d'information complémentaire, contacter par email : [bureau@ico-occitanie.fr](mailto:bureau@ico-occitanie.fr)



# “Institut Cybersécurité Occitanie”

## Key Challenge Project

### 2024 CALL – “Post-Doctoral fellowships”

---

#### 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.

---

#### Beneficiaries

The Post-doctoral research has to be carried out in research labs in the Occitanie region. Collaborative projects, involving more than one partner at the region, national or international levels are encouraged.

---

#### Eligibility rules

The project must meet the following conditions:

- The Post-Doc shall be carried in a research lab located in the Occitanie region, that is 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 1415 UT CAPITOLE/CNRS/INRAE/EHESS). Other labs that are not listed can also apply.
- Contributions can cover computer science, mathematics as well as legal, social and business-related aspects of cybersecurity.
- The research topic will have to target, in a short, mid or long run, challenges addressing one or several of the following research goals:
  1. Strengthen hardware, software and system security.
  2. Ensure the security of future networks and connected environments/emerging technologies.
  3. Better protect data and privacy, and improve trust in social networks.
  4. Improve design through formal approaches and study the impact/contribution of artificial intelligence.

The following criteria will also be taken into account (the list is not exhaustive):

- The originality of the research topics and their evolution after the doctoral research projects.
  - Candidate's academic career and publications.
  - A new work environment for post-doc candidates, favoring mobility within Occitanie laboratories to start with new projects.
  - East-West collaboration in Occitanie.
  - Quality of the applications in accordance with recruitment standards for an Assistant Professor position or a permanent researcher position at the CNRS ("chargé de recherche classe normale").
  - International applications or candidates who have carried out their thesis work outside Occitanie meeting the relevant eligibility criteria.
- Each publication by the selected Post-Doc related to the accepted project shall include the following acknowledgement:
 

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

---

## **Budget and duration**

- The eligible expenses concern the gross salary of the post-doctoral fellow for a maximum of 18 months duration on the basis of the CNRS wages depending on experience.
- A further amount of 5 k€ will be allocated to cover associated operating costs.
- In case of interruption, the non-used amount will be restituted to the Institute.

---

## **Application**

### **Deadline and selection procedure**

- ICO will organize 3 calls per year, with deadlines of **January 31st, May 31st and September 30th of each year**, until the allocated budget is exhausted.

- 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:

- Detailed CV of the candidate
- Motivation letter
- Post-Doc project description
- PhD dissertation and two samples of published work
- Two reference letters
- A support letter from the future research team hosting the Post-Doc candidate, explaining in particular how the Post-Doc project will contribute to team research agenda.

The Post-Doc proposal should be structured as follows:

- Title
- Context, objectives and positioning with respect to the state-of-the art
- Proposed approach
- Positioning with respect to ICO objectives
- Advisors: Name, research lab, research team.

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

YearICO\_PostDoc\_Acronym\_SupervisorFamilyName.pdf

Send the pdf file by email to: [bureau@ico-occitanie.fr](mailto:bureau@ico-occitanie.fr)

---

## **Contact**

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