**Grants to Build a Culture of Security in Maker, DIY and Innovation Communities in Argentina and Brazil**

|  |  |
| --- | --- |
| Competition Opens: | **29 December 2022** |
| Application Deadline: | **19 January 2023** |
| Eligibility: | Nationals of Argentina or Brazil who attended CRDF Global and iGEM’s December 2022 workshop on Creating a Security Culture: Managing Dual-Use of DIY Bio and 3D Printing |
| How to Apply: | By email to techtrainings@crdfglobal.org |
| General Area: | Security Studies |
| Award Amounts: | Up to $10,000 USD |
| Award Duration: | Up to 6 months |
| Announcement and Application: | On CRDF Global’s website:<https://www.crdfglobal.org/grants/funding-opportunities> |

**Overview**

* CRDF will award grants to support trainings and other capacity building activities which promote international best practices to improve safety and security within maker/DIY spaces and the innovation community in Argentina and Brazil.
* Grants are a one-time, six-month award up to $10,000 USD.
* Grantees will be expected to conduct activities for stakeholders from maker and DIY spaces in Argentina and/or Brazil to sensitize the innovation community to dual-use risks of emerging technologies to improve the culture of security within these institutions.
* The grant application should clearly convey how the activities will impact security practices by improving physical and data security related to emerging technologies, accessing personnel reliability, and promoting responsible research practices.

**Scope**

CRDF Global seeks applications for grants to fund trainings and other capacity building activities which promote international best practices to improve safety and security within maker/DIY spaces and the innovation community in Argentina and Brazil. Possible topics include:

* Creating a new laboratory inventory system and running trainings on how to use it.
* Developing a new records-keeping system for 3D printers and ensuring it is functional through several months of assessment and stress-testing.
* Designing a Standard Operating Procedure for project dual-use risk assessment and designating a responsible person for ensuring the SOP is enacted.
* Convening focus groups among members of multiple spaces to determine appropriate access controls and incident reporting, then publishing the chosen systems to allow adoption by others.
* Bringing all computer and networked systems in the space up to cybersecurity best practices, then ensuring all staff are trained.
* Draft a Code of Conduct for your maker/DIY space and host workshops to teach members about the Code of Conduct and solicit ideas about how to implement it.
* One-day security conference to bring together leaders of local makerspaces to hear from experts on security best practices.
* Run a monthly workshop series in your space, bringing in experts for interactive trainings on different aspects of security.

The activities should use recent case studies and specific examples to raise awareness of:

* How emerging technologies can be misused and weaponized.
* How intentional and inadvertent transfers of data, technology, or related components occurs to malign actors, proliferator states, or non-state actors.
* How emerging technologies can be used to secure sensitive data, locations, research to prevent misuse.

Throughout the six-month grant period, grantees will participate in three virtual check-ins with experts from CRDF Global and iGEM to facilitate project implementation.

**Eligibility**

* All applicants must be nationals of Brazil or Argentina.
* Applicants may apply individually or as a team.
* Applications must be past participants of CRDF Global and iGEM’s Workshop in Argentina or Brazil in December 2022.
* Local SMEs and speakers are only eligible to apply as part of a team that also includes participants.
* Applicants who will conduct activities on behalf of an institution must obtain pre-approval from the institution and its leadership to be considered for this competition.

**Application Materials**

Application materials and research products may be submitted in English, Spanish or Portuguese. Complete applications will include:

* Grant application form with project description and proposed action plan.
* Proposed detailed budget up to $10,000 USD.
* The resume or curriculum vitae (CV) of each individual on the team.
* The passport or national ID card for each individual on the team.
* At least two references.

**Proposal Evaluation Criteria**

A panel of subject matter experts will evaluate applications based on the following criteria.

1. Project relevance and impact:

* Does the proposed project address a pressing security concern and what is the potential impact?

2. Sustainability and commitment

* Ability to sustain the project and support research outcome dissemination after the grant ending period

3. Clarity, feasibility, and detail

* Is the project clearly outlined and possible to successfully accomplish? Can the project feasibly be completed during the grant period?

4. Past performance

* Do applicants have previous experience conducting trainings, managing projects, organizing events?
* Do applicants have past experience working with “do it yourself” biology and 3D printing maker spaces, biotechnology incubators and university students?
* Do applicants have knowledge related to the dual-use nature of emerging technologies and the importance of protecting knowledge, data, and technologies through increased cybersecurity, physical security of technologies, personnel reliability, and best practices related to DIY biology and 3D printing?

**Budget Instructions**

Applicants should use the Training tab of the budget template for training projects. For all other types of projects, applicants should use the Primary tab. The costshare tab should be used to the contributions of the organization to the project.

**Additional Information**

* For detailed information regarding general CRDF Global grant policies please visit:<https://www.crdfglobal.org/funding-opportunities/#information-applicants>
* For additional questions regarding the grant competition please email techtrainings@crdfglobal.org