

# CALL FOR PAPERS

## General conditions of contract for participation Cybersecurity Summer BootCamp 2021

## CONTENTS

<b>1. PURPOSE.....</b>	<b>3</b>
<b>2. CANDIDATES.....</b>	<b>3</b>
<b>3. DATES OF THE PROCESS.....</b>	<b>4</b>
<b>4. PROPOSALS.....</b>	<b>5</b>
TYPES OF PROPOSALS .....	5
TOPICS OF INTEREST .....	5
<b>5. PROCEDURE FOR SUBMITTING PROPOSALS .....</b>	<b>6</b>
DEADLINE .....	6
SENDING PROPOSALS.....	6
<b>6. ASSESSMENT OF PROPOSALS .....</b>	<b>6</b>
WORKSHOPS FOR LEAs AND CSIRTs .....	6
LEGISLATION AND REGULATORY FRAMEWORK.....	7
<b>7. PROCEDURE FOR SELECTING PROPOSALS .....</b>	<b>8</b>
<b>8. CONCLUSION OF THE CONTRACTS.....</b>	<b>8</b>
LEGISLATION AND APPLICABLE JURISDICTION .....	8
CONFIDENTIALITY .....	9
PROTECTION OF INTELLECTUAL PROPERTY.....	9
ASSIGNMENT OF IMAGE RIGHTS .....	9
PROTECTION OF PERSONAL DATA.....	10
CONTACT.....	11
<b>APPENDIX I. - CYBERSECURITY SUMMER BOOTCAMP 2021 SPEAKERS' CONTRACT .....</b>	<b>12</b>

## 1. PURPOSE

---

The purpose of these rules is to regulate the participation and hiring of **speakers**, in the forthcoming edition of the Cybersecurity Summer BootCamp event, organised by Spanish National Cybersecurity Institute (INCIBE), alongside the Organization of American States (OAS), between 12 and 22 July 2021. Given the current health situation, again, this shall be the second edition that shall take place online with live broadcasting in the programme of conferences and training workshops.

## 2. CANDIDATES

---

Any natural or legal person (the candidate) may submit a proposal, though the proposed speaker must be a natural person **over 18 years old** who is not an employee of INCIBE nor undertaking an internship at INCIBE.

In order to participate, the candidate must meet the requirements set out in these general conditions of contract and send on time and in the proper manner his/her proposal for participation, following the instructions set out below.

By means of this call, a minimum of **18 proposals** shall be selected for the Cybersecurity Summer BootCamp training programme, which shall include:

- 6 workshops aimed at members of Law Enforcement Agencies who work in cybersecurity-related operational units.
- 6 workshops aimed at technical staff working in Computer Security Incident Response Teams (CSIRTs).
- 6 workshops aimed at staff of regulatory or legislative bodies working in areas related to the legal and regulatory aspects of cybersecurity (policymakers) and current court and prosecutorial staff, government solicitors, civil servants working in the Administration of Justice (Public Prosecutor's Office, judges and prosecutors).

It is possible that there may arise the need for additional speakers, workshops or talks in the event's programme. To deal with this eventuality, the following shall be prepared:

- a) **Ranking of selected proposals:** This list shall contain the best 18 proposals bearing in mind the limits imposed by the types set out above and shall be selected for being the best proposals according to the assessment criteria set out in these general conditions of contract.
- b) **Ranking of reserve proposals:** The selection shall be made according to the ranking of the proposals submitted from the most points to the fewest for each type, beginning with proposals not selected in the previous ranking.

### 3. DATES OF THE PROCESS

DATES (2021)	ACTION
12 April	Opening of the call for papers
11 May	Closure of the call for papers
12 May	Start of the assessment of the calls for papers received
31 May	End of assessment
1 June	Notification of the calls for papers accepted
2 June	Public announcement of the proposals selected on the website <a href="https://www.incibe.es/summer-bootcamp">https://www.incibe.es/summer-bootcamp</a>
From 2 to 30 June	Conclusion of the contracts
From 23 July to 30 July 2021	<p>Receipt of invoices that shall be paid, prior agreement with it, within a maximum 30 days as from the date of receipt in the inbox <a href="mailto:contabilidad@incibe.es">contabilidad@incibe.es</a></p> <p>Natural persons who, according to applicable legislation and jurisdiction, are not obliged to submit invoices, are exempted from doing so.</p>

**Table 1. Dates of the process**

## 4. PROPOSALS

---

### TYPES OF PROPOSALS

All the proposed workshops must revolve around **cybersecurity**<sup>1</sup>:

- Duration: 180 minutes.
- Target audience: Technical profiles and/or professional experts in Cybersecurity.
- Price: €750.00 taxes and withholdings not included
- Proposed types of formats:
  - Technical master classes.
  - Live or pre-recorded technological or technical demonstrations.

### TOPICS OF INTEREST

Below is a list, merely by way of example, of topics of interests for the programme of the Cybersecurity Summer BootCamp.

- Police investigation (LEA):
  - Forensic analysis
  - Open-source intelligence (OSINT)
  - Intelligence in police investigations
  - Criminal investigation in the cloud
  - Digital Forensics and Incident Response (DFIR)
  - Cryptocurrencies and bank fraud
  - Blockchain
- CSIRTs operations:
  - Security notices and vulnerability identification
  - Cyber threat intelligence
  - Forensic analysis
  - Incident management
  - Intelligence Research
  - Open-source intelligence (OSINT)
  - Digital Forensics and Incident Response (DFIR)
  - CounterOps
  - Blockchain
- Legislation and regulatory framework:
  - Cryptocurrencies in cybercrime
  - Chain of custody and electronic evidence
  - Governance of cybersecurity
  - Technological research and case law
  - Practical foundations of technological research.
  - International law applicable to cyberspace
  - Regulation of privacy, data protection and the right to honour.
  - Development of cybersecurity strategies and/or frameworks
  - Risk management in adopting emerging technologies

---

<sup>1</sup> Set of activities aimed at protecting cyberspace from improper use of it, defending its technological infrastructure, the services they provide and the information they handle [M.O. 10/2013, of 19 February, creating the Joint Cyber Defence Command of the Armed Forces]

## 5. PROCEDURE FOR SUBMITTING PROPOSALS

---

### DEADLINE

The deadline for receiving proposals to participate in the Cybersecurity Summer BootCamp 2021 is **23.59 (CET) on 11 May 2021**.

### SENDING PROPOSALS

To send the proposal, the form available in the [call for papers](#) section of the Cybersecurity Summer BootCamp web portal must be submitted and the required fields filled out properly.

Once the form has been filled out, it must be sent to [contacto\\_SummerBC@incibe.es](mailto:contacto_SummerBC@incibe.es) by the aforementioned deadline, giving, in the subject field, the reference: **"CFP Cybersecurity Summer BootCamp 2021"**.

If the candidate deems it necessary, complementary additional information about the proposal may be attached.

## 6. ASSESSMENT OF PROPOSALS

---

Each proposal shall be assessed with a score from 0 to 100, based on the following criteria:

### WORKSHOPS FOR LEAs AND CSIRTs

- **Innovation and differentiation.** From 0 to 15 points.  
The differentiating approach in the field of cybersecurity for the specific target audience shall be assessed.
- **Treatment.** From 0 to 10 points.  
An assessment shall be made as to whether the proposed topic is within the list of subjects assumed to be of interest for the target audience, offering a thorough treatment of any of the aspects identified with an innovative approach to them.
- **Clarity of exposition.** From 0 to 10 points.  
The suitability of the presentation's structure and outline and its suitability for the target audience and the subject presented shall be assessed.
- **Practical approach.** From 0 to 10 points.  
A practical approach such that the target audience acquires practical knowledge in their own fields of action and which are simple to implement within the attendee's field of action shall be looked upon favourably.
- **Practical aspects.** From 0 to 15 points.  
The degree of appropriateness and suitability of the practical aspects set out in the proposal, such as:
  - Techniques for recognising and defending against threats.
  - Setting out and/or discovering new cybersecurity vulnerabilities, whether own or those of third parties.
  - Presentation of new tools or systems developed in cybersecurity, be they own or third-party developments.
  - Public distribution of the tools set out.
  - New cybersecurity defence systems.

- New lines of cybersecurity research.

- **Demonstration.** From 0 to 15 points.

An assessment shall be made as to whether it includes demonstrations and the estimated number of minutes this practical part will entail.

$$\text{Score} = (15 * \text{minute demonstration}) / 120$$

The maximum number of minutes proposed for the demonstration is 120

- **Resources.** Points assigned: from 0 to 15 points.

A favourable view shall be taken of the inclusion and appropriateness of means and material resources such as virtual machines, repository of tools, or any other downloadable resources that makes it possible to reproduce the workshop on the part of the attendee offline.

- **Being unpublished.** From 0 to 10 points.

The award shall be made to proposals that have not been disseminated in events and training events open to the public.

$$\text{Score} = 10 - \text{no. of conferences or training events in which the proposal was distributed publicly.}$$

## LEGISLATION AND REGULATORY FRAMEWORK

- **Suitability to the topic of the event.** From 0 to 20 points.

The inclusion and appropriateness of the messages and clear, actionable proposals for actions shall be looked upon favourably.

- **Specificity and depth of the treatment.** From 0 to 20 points.

An assessment shall be made as to whether the proposed topic is within the list of subjects assumed to be of interest for the target audience, offering a thorough treatment of any of the aspects identified with an innovative approach to them.

- **Experience of prior implementation.** From 0 to 20 points.

The speaker's having personal experience of the topic or evidence of examples of success shall be looked on favourably.

- **Practical approach.** From 0 to 15 points.

A practical approach such that the target audience acquires practical knowledge in their own fields of action and which are simple to implement within the attendee's field of action shall be looked upon favourably.

- **Didactic value.** From 0 to 10 points.

It shall be looked upon favourably if the workshop's approach and didactic focus guarantees its success and the knowledge to be conveyed is useful and instructive.

- **Clarity of exposition.** From 0 to 10 points.

The suitability of the presentation's structure and outline and its suitability for the target audience and the subject presented shall be assessed.

- **Differentiation and innovation.** From 0 to 5 points.

It shall be looked upon favourably if the proposed topic offers a differentiating approach in the field of cybersecurity for the specific target audience.

## 7. PROCEDURE FOR SELECTING PROPOSALS

---

The selection of the proposals submitted in response to this call for papers shall be made by a jury made up of INCIBE and OAS staff. The decision of this jury shall not be subject to appeal.

The assessment procedure shall be as follows:

- It shall be verified whether the topic concerns **cybersecurity** and is among the **topics of interest** described in this call. Proposals that do not meet this requirement shall be excluded.
- **Proposals that apply** the criteria set out in the previous section shall be looked upon favourably. A list shall be prepared for each type of proposal. The proposals shall be ranked from highest to lowest ratings.

The ranking of selected and reserve proposals shall be prepared as long as those proposals exceed **60 points**.

In the case of a draw:

- In both categories, the jury shall give priority in the rating to the proposal with the highest score in the practical approach criterion.
- **Publication of the results**
  - The notification of the selection of the papers submitted in response to the Call for Papers shall be made through the same email address as set out in the application form.
  - A list shall be published for each type of proposal that have been selected.
  - A list shall be published with the proposals held in reserve for each mode, as long as the proposal exceeds the threshold of **60 points**.

## 8. CONCLUSION OF THE CONTRACTS

---

These conditions shall be used for the purposes of publicity, competition, transparency and equal treatment of the minor contract that may later be processed.

According to the terms of these general conditions of contract, if the candidate (the person who presents a paper) is:

- A legal person: minor contracts shall be concluded according to art. 118 of Law 9/2017, on Public Sector Contract.
- Natural person, article 310 of Law 9/2017, on Public Sector Contracts shall be applicable in relation to the contracting system, which means that the provisions of this Law shall not be applicable to the preparation and awarding of the contract.

At all events, in order to standardise the processing and the conclusion of the contracts with the candidates selected, both if it is a natural person and if it is a legal person, the contract form **appendix I** shall be signed.

## LEGISLATION AND APPLICABLE JURISDICTION

These general conditions of contract are governed by Spanish law. Any dispute arising from the application or construction of these Conditions shall be submitted to the courts and tribunals of the city of Leon, and the parties expressly waive their right to proceed in their own jurisdiction if different. The decisions made by the Juries regarding the activities are



final as from when they are published and shall not be subject to appeal and shall be decided at the sole discretion of the Organisers of the event, which must be in accordance with the general and specific conditions of contract.

## **CONFIDENTIALITY**

INCIBE guarantees the confidentiality and secrecy of any datum of which it may become aware due to the call, especially personal and technical data, which it may not copy or use for any purpose other than that set out in the call.

Confidential information shall be deemed to be any information, especially that concerning subjects related to the technology, products, procedures, processes or know-how of the participants in the call.

The category of confidential information excludes all information disclosed by the applicants, that which must be disclosed according to these general conditions of contract, the contracts, laws or a court judgment or act carried out by a public authority or which must be published according to this call.

The duration of the confidentiality shall be indefinite while it is such, and shall remain in force subsequent to the end of the event, notwithstanding INCIBE's obligation to guarantee adequate publicity of the grants.

## **PROTECTION OF INTELLECTUAL PROPERTY**

The candidate and/or speaker know and accept that the workshop subject to the contract may not be disseminated in whole or in part by INCIBE both in written means of communication in a physical format, and on the Internet through the portal <https://www.incibe.es/summer-bootcamp> as well as the event's social networks.

The speaker shall retain the ownership and copyright that legally pertain to him/her on the content presented or developed during his/her participation in the Cybersecurity Summer BootCamp.

The speaker(s) authorise(s) INCIBE to use, communicate and disseminate for free and without time or territorial restrictions, any image, sound or any other content presented, for the sole purpose of including them in activities to disseminate, advertise and publicise the INCIBE activity and/or event or future events.

The speaker gives permission for his/her intervention to be recorded and broadcast with a delay to the students from the Cybersecurity Summer BootCamp. Note that the communication and dissemination, and/or reproduction of his/her presentation shall be done through any channel whether traditional or online.

## **ASSIGNMENT OF IMAGE RIGHTS**

The selected speakers expressly assign, on an exclusive basis and for free, to INCIBE, the use of their personal image, which may be captured during their participation in or attendance at the event, without limitation or restriction of any type. In particular, the speakers irrevocably and freely authorise INCIBE to use their image and/or names in any notice or communication that may be made through any written or audio-visual means, throughout the world and for the entire period allowed in law, and undertake to sign any documents or authorisations that may be necessary to use said image and/or name.

INCIBE shall act strictly in accordance with the obligations bearing upon it derived from Organic Law 1/1982, on Civil Protection of the Right to Honour, to Personal and Family Privacy, and to the Self-image.

## PROTECTION OF PERSONAL DATA

The speakers are obliged to comply with current regulations concerning protection of personal data.

Legal Basis	<p>GDPR: 6.1.a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;</p> <p>Law 1/1982, on civil protection of the right to honour, personal and family privacy and self-image.</p> <p>Law 34/2002, of 11 July, on information society and electronic commerce services.</p> <p>Organic Law 3/2018, on the Protection of personal data and guarantee of digital rights (LOPGDD).</p> <p>Article 19 LPGDD. Processing of contact details of individual entrepreneurs and independent professionals. 1. In the absence of evidence to the contrary, the processing of the contact data and, where appropriate, data concerning the function or position held by natural persons providing services at a legal person shall be assumed to be covered by article 6.1.f of Regulation (EU) 2016/679, as long as the following requirements are met: a) That the processing refers solely to the data necessary to locate them for professional purposes. b) That the purpose of the processing is solely to maintain relationships of any kind with the legal person at which the data subject provides services.</p> <p>2. The same assumption shall apply for the processing of data related to individual entrepreneurs and independent professionals, when they refer to them only in said capacity and they are not processed to initiate a relationship with them as natural persons. 3. The data controllers or data processors referred to in article 77.1 of this organic law may also process the data mentioned in the foregoing sections when such is derived from a legal obligation or it is necessary to exercise their competencies.</p>
Purposes of the Processing	<p>Recording and control of participation in the event, as well as to fulfil the rest of the obligations to which INCIBE is subject.</p> <p>Sending notices related to the event.</p> <p>Recording and broadcast of the talk</p>
Group	Participants in the CFP to opt to be a speaker at the event.
Data Categories	<ul style="list-style-type: none"> <li>Participant's details (name, surname(s), email address and contact telephone number) for the purposes of his/her participation in the call, resolving queries and managing his/her participation, if selected.</li> <li>The speaker's voice and image, if selected.</li> </ul>
Category Recipients	<p>Service contractor for the event.</p> <p>Exceptionally, communications to public authorities and bodies to comply with a legal obligation to which INCIBE is subject.</p>
International Transfer	N/A

Erasure Period	<p>They shall be retained for the time required to achieve the purpose for which they were collected and to determine possible liabilities that may arise from the aforementioned purpose and from data processing and to send information of interest to the recipients, until they de-register.</p> <p>The obligatory minimum data collected on the registration form shall be preserved for a year following the conclusion of the event.</p>
Security Measures	The security measures implemented are those set out in the National Security Plan.
Rights	<p>Access, Rectification, Erasure, Restriction, Portability, Opposition You may exercise your rights by writing to <b>dpd@incibe.es</b></p> <p>You may file a complaint at the Spanish Data Protection Agency</p>
Responsible Body	State-Owned Enterprise Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE), holder of Tax ID Code A24530735.
Data Protection Officer	<b>dpd@incibe.es</b>
Additional information	<p>You can view additional and detailed Data Protection information on our website:</p> <p><a href="https://www.incibe.es/registro-actividad/">https://www.incibe.es/registro-actividad/</a></p> <p><a href="https://www.incibe.es/proteccion-datos-personales">https://www.incibe.es/proteccion-datos-personales</a></p> <p><a href="https://www.incibe.es/aviso-legal">https://www.incibe.es/aviso-legal</a></p> <p>In relation to the cookies, you may obtain the data on the website: <a href="https://www.incibe.es/politica-cookies">https://www.incibe.es/politica-cookies</a></p>

## CONTACT

If you have any queries about the process, you may contact the organisers of the Cybersecurity Summer BootCamp by writing to [contacto\\_SummerBC@incibe.es](mailto:contacto_SummerBC@incibe.es)

**Leon, 9 April 2021**

**Director-General**

**Rosa Díaz Moles**

## APPENDIX I. - CYBERSECURITY SUMMER BOOTCAMP 2021 SPEAKERS' CONTRACT

### AGREEMENT BETWEEN \_\_\_\_\_ AND THE STATE-OWNED ENTERPRISE INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA M.P.S.A. TO CONTRACT A COMMUNICATION SERVICE

At Leon, on ... ..... 2021

#### BY AND BETWEEN

On the one hand, MS ROSA DÍAZ MOLES, of legal age, in her capacity as the Director-General of the State-Owned Enterprise Instituto Nacional de Ciberseguridad de España, M.P.S.A. (hereinafter, "INCIBE"), whose address is at 24005-León, Edificio INCIBE, Avda. José Aguado, 41 and Tax I.D. Code A-24530735, who is entitled to act in these proceedings according to a deed with notarial record number 2233, execute on 24 May 2017 by the Notary of the Notarial College of Madrid, Ms Ana López-Monís Gallego.

On the other, \_\_\_\_\_, of legal age, whose address for these purposes is \_\_\_\_\_, on behalf of \_\_\_\_\_ in her capacity as \_\_\_\_\_, who enjoys the legal capacity to enter into a contract according to powers of attorney granted on [date] \_\_\_\_\_ before the notary of \_\_\_\_\_ Mr \_\_\_\_\_, with number \_\_\_\_\_ of his notarial records.

INCIBE and \_\_\_\_\_ (hereinafter, they may be known, individually, as "the Party" and, jointly, as "the Parties"), mutually acknowledging that they enjoy the legal capacity and to act in these proceedings to enter into this contract.

#### THEY DO STATE

**One.** - That INCIBE is a state-owned enterprise within the Ministry of Economic Affairs and Digital Transformation, and is the lead agency for developing, reinforcing and protecting the privacy, cybersecurity and digital trust of citizens and companies, especially in the information and communication technology sector, as well as for strategic sectors in general.

**Two.** - That the Cybersecurity Summer BootCamp is an event organised by the State-Owned Enterprise National institute of Ciberseguridad de España M.P., S.A. (INCIBE) along with the Organization of the American States (O.A.S.) and its next edition shall be held online between 12 and 22 July 2021.

**Three.** - That INCIBE made a public call to hire speakers for the event.

**Four.** - That the proposal of \_\_\_\_\_ was one of those selected after applying the assessment criteria set out in the general conditions of the Call for papers for the Cybersecurity Summer BootCamp 2021.

In accordance with the foregoing, both Parties sign this contract according to the following

## CLAUSES

### One. - Purpose.

This contract governs the conditions for delivering a workshop during the Cybersecurity Summer BootCamp 2021 event, which shall be held online from 12 to 22 July 2021.

- The candidate undertakes to carry out the technical training workshop, which is called \_\_\_\_\_ and which shall last 180 minutes on \_\_\_\_\_
- The speaker is \_\_\_\_\_.

Both the speaker and the candidate state that the speaker is of legal age and that neither of them is subject to any conflict of interest or prohibition on entering into contracts as set out in legislation.

### Two. - Duration.

The seminar or workshop shall be broadcast live through the Zoom platform and shall be recorded to be watched later by the students. Regarding the possibility of using the recording made during the event, it is unlimited per the terms regulated in this contract.

### Three. - Obligations of the parties

INCIBE undertakes to:

- Make available to the speaker Cybersecurity Summer BootCamp's official template for presentations, which shall be provided by the organisers.
- Pay the price according to the conditions of clause four.
- Make available to the speaker a contact for queries, clarifications and other procedures for his/her participation.

The candidate and/or speaker undertakes to:

- Create an innovative professional presentation, seeking to avoid presentations that have already been used in other events.
- Use Cybersecurity Summer BootCamp's official template for presentations, which shall be provided by the organisers.
- Not include advertising of any kind in the presentation (brands, companies, products, services, etc.)
- Not harm in any way against the image or prestige of any natural or legal person or brand.
- Not publicly disclose security risks of public or private entities. If such a risk exists, the content that may be necessary must be anonymised.
- Send the presentation to the organisers of the Cybersecurity Summer BootCamp at least 15 days in advance of the event, so that it can be validated (agreement with the work presented at the CFP and non-inclusion of inappropriate information).
- Seek to accommodate amendments to the presentation that the organisers may suggest, after reviewing it.
- Participate in the online technical tests prior to the event.
- Attend the event session on the date and at the time agreed by the organisers, having at your disposal everything necessary to give the presentation and ensuring that it may take place without setbacks.
- Comply with these provisions making up the general conditions of contract for the event and follow the guidelines that may be specified by the organisers.
- Respond to and respect the indications of the Organisers of the event, at all times.

- Act in good faith, and behave respectfully and with decorum towards the rest of the participants and attendees.

#### **Four. -Price**

The price of the contract is \_\_\_\_\_, taxes and withholdings not included.

#### **Five. - Payment method**

This payment shall be made after participation in the event by INCIBE upon submission and approval of the invoice or, otherwise, issuance of the certificate of execution of the service by INCIBE.

#### **Six. - Penalties**

If the speaker does not appear at the event specified in this contract, the candidate shall not receive the price of the contract, with the right to compensation for damages caused.

If the speaker's intervention lasts under 160 minutes, he/she shall be paid the amount minus in percentage terms the duration for which he/she did not speak.

If INCIBE dispensed with the services of the speaker in the 15 days prior to the event, it must pay, by way of compensation, half of the agreed fee.

If, due to force majeure, INCIBE could not hold the event, it shall be released from its obligations when the absence of fault or negligence on its part is proven.

#### **Seven. - Publication of the work and copyright, confidentiality, and privacy**

The candidate and/or speaker know and accept that the workshop subject to the contract may not be disseminated by INCIBE both in written means of communication in a physical format, and on the Internet through the portal <https://www.incibe.es/summer-bootcamp> as well as the event's social networks.

The speaker shall retain the ownership and copyright that legally pertain to him/her on the content, images, documentation of any kind presented or developed during his/her participation in the Cybersecurity Summer BootCamp. The candidates and/or speakers guarantee that they are the authors and that they hold exclusive ownership, free of any encumbrance or limitation, of all intellectual and industrial property rights over the proposals, presentations, project, contents and/or their various components, presented at the event, according to Spanish intellectual and industrial property legislation. Moreover, he/she/they authorise(s) INCIBE to use, communicate and disseminate for free and without time or territorial restrictions, any image, sound or any other content presented, for the sole purpose of including them in activities to disseminate, advertise and publicise the INCIBE activity and/or event or future events.

The speaker expressly assigns, on an exclusive basis and for free, to INCIBE, the use of his/her personal image and his/her work, which may be captured during their participation in or attendance at the event, without limitation or restriction of any type. In particular, he/she irrevocably and freely authorises INCIBE to use his/her image and/or name in any notice or communication that may be made through any written or audio-visual means, throughout the world and for the entire period allowed in law in reference to the event and his/her participation in it.

The speaker gives permission for his/her intervention to be recorded and broadcast with a delay to the students from the Cybersecurity Summer BootCamp. Note that the communication and dissemination, and/or reproduction of his/her presentation shall be done through any channel whether traditional or online.

#### **Nine. - Protection of personal data**

In compliance with current regulations concerning protection of personal data, INCIBE undertakes to process them per the terms regulated in the general conditions of participation.

Specifically, the speaker authorises INCIBE to use his/her personal data to disseminate and hold the event (including the Cyber Security Summer BootCamp's website and social network and various media).

The speakers assign, on an exclusive basis and for free, to INCIBE, the use of their personal image, which may be captured during their participation in or attendance at the event, without limitation or restriction of any type. In particular, the awardees irrevocably and freely authorise INCIBE to use

their image and/or names in any notice or communication that may be made through any written or audio-visual means, throughout the world and for the entire period allowed in law, and undertake to sign any documents or authorisations that may be necessary to use said image and/or name.

INCIBE shall take appropriate measures to protect the data and files against destruction, illegal loss, alterations, assignments and unauthorised accesses.

All personal data that INCIBE, as data controller, must process to manage the processing of the invitation conditions and to conclude the contract, as well as to send notices about calls related to the event, shall be included in the INCIBE activity register "Events", which is owned by INCIBE, and whose purpose is to organise cybersecurity events to transfer, disseminate, train in knowledge and good practice in this area.

The candidate and/or the speaker authorises that the data must be communicated to INCIBE's data processor to manage the event, which shall be the company that becomes the contractor for public contracting file 016/21. The terms and conditions governing said tender set out the specific obligations in this area that are imposed upon the contractor.

#### **Ten. - Termination**

The reasons why INCIBE may agree to the termination of the Contract are:

- The death or sudden incapacity of the individual contractor or expiry of the legal personality of the awarding body. In the event of merger of companies in which the contractor company holds shares, the current contract with the absorbing company or with that resulting from the merger, which was subrogated to all the rights and obligations arising therefrom. Likewise, in the event of a spin-off, contribution or transfer of companies or branches of activity thereof, the contract shall remain with the resulting or beneficiary entity, which shall be subrogated to the rights and obligations arising therefrom, as long as it enjoys the solvency required upon agreeing the award.
- The declaration of insolvency according to any other procedure set out in the insolvency law or a declaration of insolvency in any other procedure.
- Mutual agreement of the parties.
- Failure to conclude the contract before the deadline.
- Delay in meeting the deadlines on the part of the contractor, and breach of the deadlines or the essential obligations set out in the contract. And not meeting the objectives for reasons attributable to \_\_\_\_\_. Any type of breach after the third warning.
- The sudden incapacity or want of solvency or being subject, subsequent to the award, to any of the prohibitions on entering into contracts.
- All others expressly set out in the contract.

In the event of termination of the \_\_\_\_\_ contract, at the request of INCIBE, it must immediately dismiss all contracted workers. Moreover, the work carried out to that point that is deemed useful for INCIBE shall be fully settled, and INCIBE shall pay for the work carried out according to the conditions set out in the Contract to that date. At all events, INCIBE shall deduct from the amount resulting from the settlement the amount corresponding to compensation and other applicable items.

The following is considered an essential contractual obligation:

Any of \_\_\_\_\_'s proposals that has been taken into account in the assessment.

Where appropriate, the contractor's obligations concerning subcontracting.

The termination of the contract shall be agreed by the contracting body.

In witness whereof, the Parties sign this Contract at LEON on the date set out in the header.



INCIBE

(Company)

Agreement of the paper /  
workshop

Director-General

Attorney-in-Fact