



Isdefe

su mejor aliado

Aspectos de seguridad e información clasificada en propuestas colaborativas del clúster 3 de Horizonte Europa

ISDEFE EN 1 MINUTO

Ingeniería de Sistemas para la Defensa de España, **Isdefe**, somos una Sociedad Mercantil Estatal creada en el año 1985, propiedad del Ministerio de Defensa y medio propio y servicio técnico de la Administración española. Ofrecemos servicios de ingeniería y consultoría a organismos públicos e instituciones nacionales e internacionales, en áreas de interés tecnológico y estratégico.

Nuestros valores

Independencia

Visión Global


Proactividad

Compromiso

Experiencia y Conocimiento


Sectores de actividad y servicios

Proporcionamos servicios de ingeniería y consultoría en los siguientes sectores de actividad:


 **Defensa y Seguridad**

 **Espacio**

 **Transporte**

 **Administraciones Públicas**

 **TIC**

 **Energía**

FASE INICIAL

Revisando el WP

Encontrando el topic

Conociendo los aspectos de seguridad

FASE INTERMEDIA

Preparando el consorcio

Profundizando en los aspectos de seguridad

Decidiendo sobre aspectos de seguridad

FASE FINAL

Manejando los aspectos de seguridad

Finalizando la propuesta

Tomando las ultimas decisiones

Preparando el consorcio

Buscando a los socios adecuados

Expertos en seguridad

Coordinador con experiencia en manejo de aspectos de seguridad

Profundizando en los aspectos de seguridad

¿Qué implicaciones de seguridad puede tener ahora nuestra propuesta?

Evaluar el posible uso indebido

¿Es exclusivamente de aplicación civil?

Decidiendo sobre aspectos de seguridad

Revisión conjunta por parte del consorcio de los aspectos de seguridad

Decisión: ¿puede tener nuestra propuesta implicaciones de seguridad

Manejando los
aspectos de seguridad

Establecimiento del SAB

Designación del PSO

Finalizando la
propuesta

Entregables y actividades clasificados

Rellenando la tabla de seguridad de la parte A

Borrador del anexo de seguridad

Tomando las ultimas
decisiones

Propuesta de SAL

Security Classification Guide

Finalización de anexo de seguridad

Revisión final de tabla de seguridad

Manejando los
aspectos de seguridad

Establecimiento del SAB

Designación del PSO

THE PROJECT Security Section

1. Summary of the project security issues

The consortium has established a Security Advisory Board (SAB) and has appointed a Security Project Officer (PSO) (section 4), who have participated in the preparation of the proposal and has been involved in the discussion about the securities issues and the possible classification of some of the [REDACTED]'s deliverables.

As a result of the SAB's work, the consortium has identified the following security issues:

Manejando los aspectos de seguridad

4.2 - Security Advisory Board (SAB)

The SAB [redacted] is composed of 3 (uneven) members consisting of end-user representatives with a good knowledge of the security issues.

The SAB members have the appropriate national security clearance.

The role of the SAB is to review, throughout the project's life, the project deliverables, in order to assess whether they include any security sensitive information, propose their classification, declassification etc. and other timely measures for preventing the misuse of such information.

Security Advisory Board			
Member's name	Nationality	Profession	Areas of competence
[redacted]	French	Law Enforcement Agent	Artificial Intelligence Software development Analysis of Criminal Data
[redacted]	Spanish	Guardia Civil [redacted]	Management of EU projects as part of Technological Innovation Office of Guardia Civil in Madrid
[redacted]	German	Police Officer	- Security Management LEA Organizations - Security Management in EU-Projects

Manejando los aspectos de seguridad

4.2 - Security Advisory Board (SAB)

The SAB should be composed of 3 (uneven) members consisting of end-user representatives with a good knowledge of the security issues.

The SAB members have the appropriate national security clearance.

The role of the SAB is to review, throughout the project's life, the project deliverables, in order to assess whether they include any security sensitive information, propose their classification, declassification etc. and other timely measures for preventing the misuse of such information.

4.2.1 Short CV

[REDACTED] is a researcher at the Central Service of Criminal Intelligence of the French National Gendarmerie where, among others, he applies network theories on the analysis and forecasting of criminality patterns. [REDACTED]

[REDACTED]

Manejando los aspectos de seguridad

Establecimiento del SAB

Designación del PSO

4.1 - Project Security Officer (PSO)

The role of the PSO is to guarantee that the rules on the handling of EU classified information and applicable security procedures are respected. The PSO together with the SAB's members will monitor possible security issues and decide on the classification of the deliverables and their level.

The tables below collect the information about [REDACTED]'s PSO, [REDACTED] from the Bavarian police who has National Security clearance

Project Security Officer		
Name	Nationality	Profession
[REDACTED]	German	Police Officer

Manejando los aspectos de seguridad

Short Concise CV

Date	Position
since 1999	Bavarian State Police
2007 – 2009	Studies at University of Applied Sciences for Administration and Affairs Bavaria (Department of Police Management and Policing) (HfoeD)
2009 – 2013	Bavarian State Police Middle Management
2013 – 2016	Bavarian State Police Middle Management Personnel Development

2016 – 2018	Studies at German Police University (DHPol)	Focused on Cybercrime, Radicalization and Extremism (Master Course)
2018 - 2019	Bavarian State Police Officer Lecturer University of Applied Sciences for Legal Administration and Legal Affairs Bavaria (Department Police Management and Policing)	Department of Criminology (responsible for Cybercrime, IT, Data Protection, Data Security)
2019 – today	Bavarian State Police Officer Chief-Superintendent	
2018 – today	Scientific Researcher University of Applied Sciences for Legal Administration and Legal Affairs Bavaria (Department Police Management and Policing)	In side-line scientific researcher in the research institute for security research. Participation and coordination of different H2020/H20230 EU projects – focused on Cybercrime, AI driven policing approaches, Radicalization and Counterterrorism.
2020 – today	PhD Candidate German Police University (DHPol)	Research focus on Radicalization and Counterterrorism.

Manejando los
aspectos de seguridad

Establecimiento del SAB

Designación del PSO

Manejando los aspectos de seguridad

Establecimiento del SAB

Designación del PSO

Finalizando la propuesta**Entregables y actividades clasificados**

Rellenando la tabla de seguridad de la parte A

Borrador del anexo de seguridad

Tomando las ultimas decisiones

Propuesta de SAL

Security Classification Guide

Finalización de anexo de seguridad

Revisión final de tabla de seguridad

Security issues table

1. EU Classified Information (EUCI)²

Does this activity involve information and/or materials requiring protection against unauthorised disclosure (EUCI)? Yes No

Does this activity involve non-EU countries? Yes No

Do participants from non-EU countries need to have access to EUCI? Yes No

Do the non-EU countries concerned have a security of information agreement with the EU? Yes No

2. Misuse

Does this activity have the potential for misuse of results? Yes No

3. Other Security Issues

Does this activity involve information and/or materials subject to national security restrictions?
If yes, please specify: (Maximum number of characters allowed: 1000) Yes No

Are there any other security issues that should be taken into consideration?
If yes, please specify: (Maximum number of characters allowed: 1000) Yes No

Manejando los
aspectos de seguridad

Establecimiento del SAB

Designación del PSO

Call: [insert call identifier] – [insert call name]

EU Grants: Application form (Part B Security)

Horizon Europe Programme Proposal Template (Part B)

Security Section

1. Summary of the project security issues
2. Sensitive information with security recommendation
3. Classified information
 - 3.1 – Security Aspects Letter (SAL)
 - 3.2 - The Security Classification Guide (SCG) (appendix of the SAL)
4. Security Staff
 - 4.1 - Project Security Officer (PSO)
 - 4.2 - Security Advisory Board (SAB)
5. Other project-specific security measures

Summary of the project security issues

██████████ project will involve:

- Activities or results raising security issues: YES
- ‘EU-classified information’ as background or results: YES

██████████ project involves activities or results raising security issue or “EU-classified information” as background of results.

According to the “*Guidelines for the classification of research results*” provided by the European Commission, ██████████ being a security project in the field of Terrorism and Organized Crime, is candidate to be security classified as RESTREINT EU since the project is susceptible to generate information whose unauthorized disclosure could be disadvantageous to the interest of the EU or one or more of its Member States. Especially, according to this Guide, this project could provide detailed information about scenarios of potential attack strategies due to its strategic and foresight approach, in which wild cards and black swans will be imagined and detailed. Because of its strategic vision it will produce contents related to prediction, detection, understanding and response, the four measures that according to the guide should be classified. On this regard, the Security Classification Guide (SCG) (see section 6.2.2 below) provides information of the deliverables that potentially can have classified parts.

On the other hand, given its potential sensitivity, special attention will be paid for limited dissemination of foreground outside the consortium for security reasons and “any foreground, generated in the course of the project shall not be disseminated to any legal entity outside the existing consortium, unless agreed otherwise by the beneficiaries and the Commission”.

So, all information gained through ██████████ will not be automatically released; dissemination of potentially sensitive material will be in accordance with applicable EU rules and national legislation.

Summary of the projectsecurity issues

In general, information generated or handed by [REDACTED] will be split into two categories:

- Unclassified information, which can be either: Public (PU) enabling the start of dissemination towards non [REDACTED] partners, or Confidential, restricted under conditions set out in Model Grant Agreement (CO) or specified.
- Classified information (CI), as referred to in Commission Decision 2015/444 of 13 March 2015.

Applying these strict rules, information will be disseminated in specific ways users group, or in specific closed workshops with restricted deliverables to allow management of these confidentiality aspects. Furthermore, the necessary provisions for the exchange of classified information are described in the Security Aspect Letter (SAL) included hereafter.

Sensitive information

An overview of all deliverables and their dissemination level is in section 1.3.2. WT2 list of deliverables, of the Annex I, Description of Action (part A) of this ██████████ Grant Agreement. For clarity and completeness, the list of those deliverables that are subject to limited dissemination (not including the classified deliverables that are collected in the Security Classification Guide in section 6.2.2. below) is included hereafter:

Num.	Name	WP	Lead	Type	Dissem. Level	Deliv. Date
D1.1	Six-monthly Progress Reports	WP1	██████████	R	CO	M40
D1.2	First Periodic Activity and Management Report	WP1	██████████	R	CO	M18
D1.3	Second Periodic Activity and Management Report	WP1	██████████	R	CO	M40
D1.4	Data and Knowledge Management Plan	WP1	██████████	R	CO	M40
D2.4	Legal, ethical and societal requirements for intelligence-led technologies	WP2	██████████	R	CO	M12
D3.2	Prototype HMI for analysts for	WP3	██████████	SW	CO	M9

Manejando los aspectos de seguridad

Establecimiento del SAB

Designación del PSO

Finalizando la propuesta

Entregables y actividades clasificados

Rellenando la tabla de seguridad de la parte A

Borrador del anexo de seguridad

Tomando las ultimas decisiones**Propuesta de SAL**

Security Classification Guide

Finalización de anexo de seguridad

Revisión final de tabla de seguridad

Security Aspect Letter

6.2.1 Security aspect letter

The Commission's provisions on security and the rules on security as laid down in Commission Decision 2015/444 of 13 March 2015 on the security rules for protecting EU classified information²⁶ are an integral part of this grant agreement.

This implies that beneficiaries shall make sure to take all appropriate measures to comply with the Commission's provisions on security when handling European Union Classified Information (EUCI).

In particular but not exclusively, the following security requirements shall be complied with for handling and storage of the elements and parts of the grant agreement that are mentioned in the Security Classification Guide at Appendix to this SAL for the grant agreement for performing [REDACTED]

General

- The performance of the grant agreement will involve information classified EU RESTRICTED/RESTREINT UE.
- A Facility Security Clearance is not required.
- Persons who need to access EU classified information must be briefed as to their responsibility for security²⁷.
- The beneficiaries concerned shall take all measures prescribed by the National Security Authority/Designated Security Authority (NSA/DSA) for safeguarding EUCI.
- The beneficiaries concerned shall appoint a Project Security Officer (PSO)
- The beneficiaries concerned, through the PSO, shall maintain a continuing relationship with his NSA/DSA.
- The beneficiaries concerned shall maintain a record of his employees taking part in the project and who have been cleared for access to EUCI. (N.B. Personal Security Clearances are only required for projects in which the maximum classification is CONFIDENTIEL UE/EU CONFIDENTIAL or above).

- EU classified information for the purpose of these instructions is to be understood as information classified and marked [relevant classification level] or its equivalent national classification.
- Information generated by the beneficiaries concerned will require EU classification and marking.
- The beneficiaries concerned must obtain the approval of the Contracting Authority before beginning negotiations with a view to subcontract.
- The Commission Security Directorate may - in co-ordination with the responsible NSA/DSA - conduct inspections at beneficiaries' facilities concerned to verify the implementation of the security requirements for the handling of EUCI.
- The beneficiaries concerned shall report all cases of unauthorised disclosure or loss of EUCI to the responsible NSA/DSA, the Commission Security Directorate and the Contracting Authority.
- All EUCI provided or generated under this grant agreement shall continue to be protected in the event of termination of the grant agreement.
- The beneficiaries concerned shall undertake not to utilise the EUCI provided or generated, other than for the specific purpose of the grant agreement [REDACTED]
- Without prejudice to the Commission decision 2015/444²⁸, the instructions in the Guide for handling classified information in the context of framework programme research projects have to be followed.²⁹

6.2.2 Security classification guide

M
aspecto

Production of classified Foreground information					
Subject	Classification level	Name	Resp.	Date of production	Comments
D2.1 Use cases: understanding Technological Factors driving OCT	RES-EU	[Redacted]	PSO	M8	
			Main contributor		
			Contributor		
			Contributor		
			Contributor		
			Contributor		
			Contributor		
			Contributor		
			Contributor		
			Contributor		
			Contributor		
			Contributor		
			Contributor		
			Contributor		
			Read		
Read					
Read					
Read					
Read					
Read					
Read					
			PSO		

datos
I de la parte A

Other Project-Specific Security Measures

5. Other project-specific security measures

ISDEFE, [REDACTED] coordinator, as a state owned company whose goal is to provide Technical and Strategic Consultancy for the Defense and Civil sectors, is cleared as NATO control point and has a Security Department in its organization with highly experienced personnel on these matters, and will be part of the SAB. The Project Coordinator, Raquel Pastor, and the ISDEFE personnel working on [REDACTED] are cleared up to EU SECRET level, and have also national and NATO security clearances.

The fact that the consortium and its partners are already aware of these concerns (some of them have national/EU/NATO security clearances) is a guarantee of good practices.

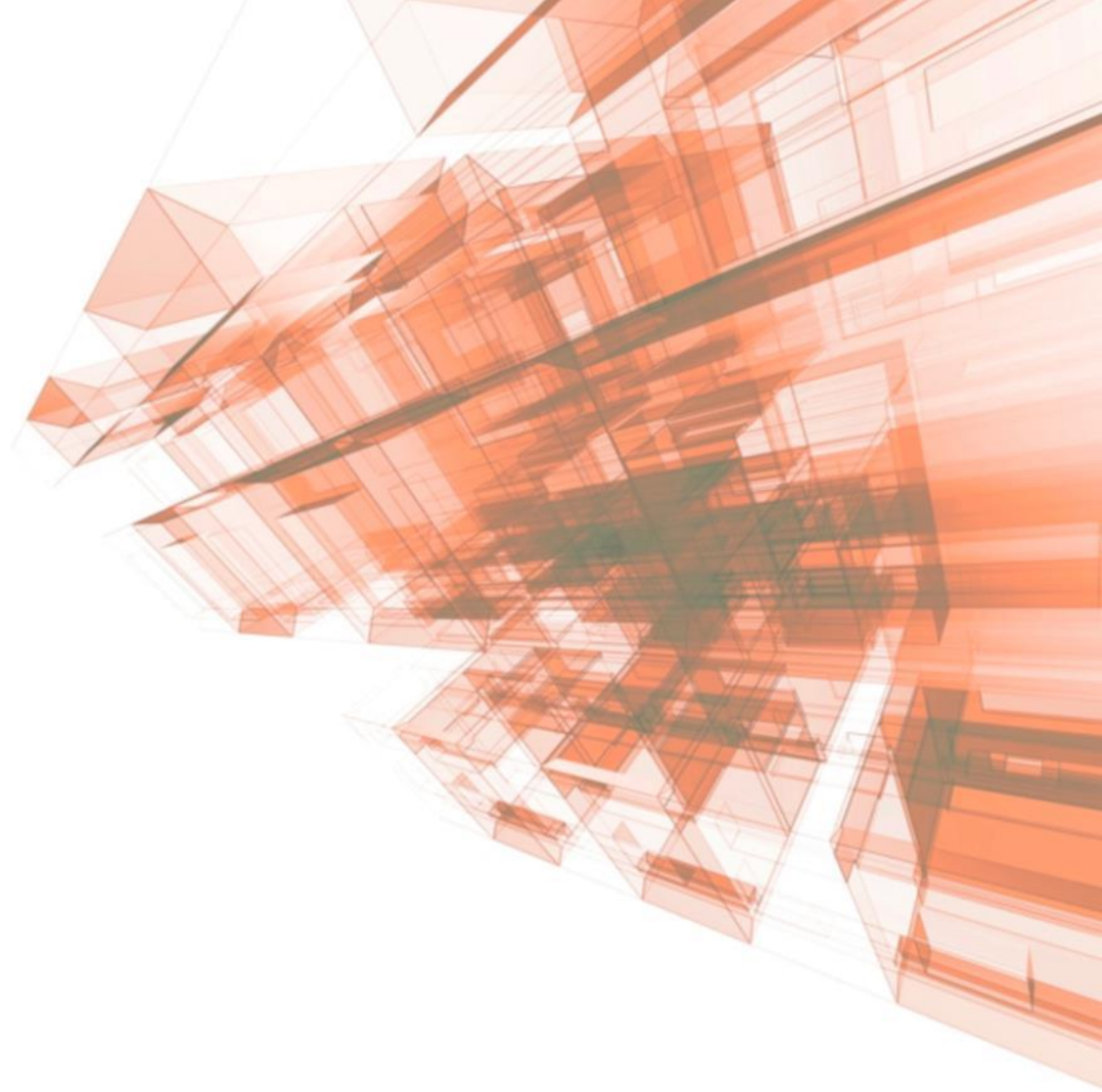
It is important to stress that personnel who need to access RESTREINT EU classified information (the classification level in case any deliverable was classified , do not need EU personal security clearance, they only required to be briefed as to their responsibility for security and know about the handling of EU classified information (EUCI). Since the SAB consist of a group of End-Users well experienced on security – sensitive issues, [REDACTED] will count also on their support on security questions.

The SAB will analyse if some of the classified deliverables, or internally restricted but not classified, could have a public version in order to contribute to the dissemination of the project, its impact, results and recommendations.



Isdefe

su mejor aliado



Isdefe
C/ Beatriz de Bobadilla, 3
28040 Madrid
Tel.: +34 91 411 50 11
Email: general@isdefe.es
www.isdefe.es