# No. 56490*

# Spain
# and
# Viet Nam

**Agreement between the Kingdom of Spain and the Socialist Republic of Viet Nam on the mutual protection and exchange of classified information. Madrid, 27 March 2019**

**Entry into force:** *21 January 2021 by notification, in accordance with article 12(1)*

**Authentic texts:** *English, Spanish and Vietnamese*

**Registration with the Secretariat of the United Nations:** *Spain, 12 February 2021*

**No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.*

# Espagne
# et
# Viet Nam

**Accord entre le Royaume d'Espagne et la République socialiste du Viet Nam concernant l'échange et la protection réciproque d'informations classifiées. Madrid, 27 mars 2019**

**Entrée en vigueur :** *21 janvier 2021 par notification, conformément au paragraphe 1 de l'article 12*

**Textes authentiques :** *anglais, espagnol et vietnamien*

**Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies :** *Espagne, 12 février 2021*

**Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.*

[ TEXT IN ENGLISH – TEXTE EN ANGLAIS ]

# AGREEMENT

# BETWEEN

# THE KINGDOM OF SPAIN

# AND

# THE SOCIALIST REPUBLIC OF VIET NAM

# ON

# THE MUTUAL PROTECTION AND EXCHANGE

# OF CLASSIFIED INFORMATION

The Kingdom of Spain and the Socialist Republic of Viet Nam (hereinafter referred to as the "Parties"),

Having agreed to broaden their political, military and economic co-operation, and to hold talks on political and security-related issues,

Being aware of the changes in the political situation in the world and recognizing the important role of their mutual co-operation for peace, stability, national and international security,

Realising that good co-operation may require exchange of Classified Information between the Parties,

Desiring to create a set of rules regulating the mutual protection of Classified Information applicable to any future co-operation agreements and classified contracts, which will be implemented between the Parties, containing or involving Classified Information,

Have agreed as follows:

## ARTICLE 1
## DEFINITIONS

In this Agreement, the following concepts are understood:

1. **"Classified Information"** means information of whatever form, nature or method of transmission either manufactured or in the process of manufacture to which a security classification level has been attributed and which, in the interests of national security and in accordance with the national laws and regulations requires protection against unauthorized access or destruction.

2. **"Unauthorized access to Classified Information"** means access by any individual or legal entity to Classified Information without approval of the Competent Authority, in accordance with the national laws and regulations of each Party and the provisions of this Agreement.

3. **"Security Classification Level"** means a category assigned to Classified Information which indicates its sensitivity, the degree of damage that might arise in the event of its unauthorized disclosure or loss and the level of protection to be applied to it by the Parties.

4. **"Classification marking"** means a mark which shows the Security Classification Level of the Classified Information.

5. **"Security clearance"** means a positive determination stemming from a vetting procedure that shall ascertain loyalty and trustworthiness of an individual or legal entity as well as other security aspects in accordance with national laws and regulations. Such a determination enables granting the individual or the legal entity access, and allows them to handle Classified Information up to a certain level.

6. **"Transferring Party"** means the Party sending Classified Information.

7. **"Receiving Party"** means the Party to which Classified Information is transmitted.

8. **"User"** means an individual or a legal entity that takes part in relevant cooperation activities or in the implementation of Classified Contracts to which this Agreement shall be applied.

9. **"Competent Authority"** means the authority, which in compliance with the national laws and regulations of the respective Party has ultimate responsibility for the protection of Classified Information, exercises overall control in this sphere as well as conducts and oversees the implementation of this Agreement. Such authorities are listed in Article 4 of this Agreement.

10. **"Contractor"** means an individual or a legal entity possessing the legal capacity to conclude contracts under the provisions of this Agreement.

11. **"Classified Contract"** means an agreement between users of the Parties which contains Classified Information, or the performance of which generates or requires access to Classified Information of either Party.

12. **"Need to know"** principle means the necessity to have access to Classified Information in connection with official duties and for the performance of a concrete official task.

13. **"Third Party"** means a state or an international organization or a user, which is not a Party to this Agreement.

14. **"Declassification of Information"** means the removal of the security classification level.

15. **"Security Incident"** means an action or inaction contrary to national laws and regulations, which results or may result in the unauthorized access, disclosure, loss, destruction or compromise of Classified Information, generated and/or exchanged under this Agreement.

## ARTICLE 2
## OBJECTIVE

The objective of this Agreement is to ensure the protection of Classified Information exchanged between the Parties. It sets out the security procedures and arrangements for such protection.

## ARTICLE 3
## SECURITY CLASSIFICATION LEVELS

1. The Parties agree that the following Security Classification Levels are equivalent and correspond to the Security Classification Levels specified in the national laws and regulations of the respective Party.

| For the Kingdom of Spain | For the Socialist Republic of Viet Nam |
|---|---|
| SECRETO | TUYỆT MẬT |
| RESERVADO | TỐI MẬT |
| CONFIDENCIAL | MẬT |

2. Information received from the Kingdom of Spain classified as DIFUSIÓN LIMITADA shall be protected as MẬT in the Socialist Republic of Viet Nam.

## ARTICLE 4
## COMPETENT AUTHORITIES

1. The Competent Authorities of the Parties are:

   **For the Kingdom of Spain:**
   National Intelligence Centre.

   **For the Socialist Republic of Viet Nam:**
   Ministry of Public Security.

2. The Parties shall notify each other through diplomatic channels of any subsequent changes of their Competent Authorities.

3. The Competent Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information.

4. In order to ensure close co-operation in the implementation of the present Agreement, the Competent Authorities may hold consultations at the request made by one of them.

5. In order to achieve and maintain comparable standards of security, the respective Competent Authorities shall, on request, provide each other with information about the security standards, procedures and practices for protection of Classified Information applied by the respective Party.

6. The Competent Authorities of the Parties may conclude Implementing Arrangements in relation with this Agreement.

7. The Security Services of the Parties may exchange and return operative and/or intelligence information directly with each other in accordance with national laws and regulations.

## ARTICLE 5
## TRANSMISSION OF CLASSIFIED INFORMATION

1. Classified Information marked CONFIDENCIAL / MẬT and above shall normally be transferred by means of diplomatic couriers. However, other channels may be used if mutually agreed by the Competent Authorities and in accordance with the national laws and regulations of the Parties. The Receiving Party shall confirm in writing receipt of Classified Information marked CONFIDENCIAL / MẬT and above.

2. Electronically transmitted Classified Information shall be protected by cryptographic means mutually approved by the Competent Authorities and holding a duly issued certificate pursuant to the national laws and regulations of the Parties.

3. In case of transferring a large consignment containing Classified Information, the Competent Authorities shall mutually agree on and approve a transportation plan, which will include the means of transport, escort requirements, the route and the other security measures.

## ARTICLE 6
## MEASURES FOR PROTECTION OF CLASSIFIED INFORMATION

1. In compliance with their national laws and regulations, the Parties shall implement all appropriate measures for protection of Classified Information which is generated or exchanged under this Agreement. Such Classified Information shall be protected as national Classified Information with the corresponding Security Classification Level.

2. The Parties shall inform each other about any changes in their respective national laws and regulations affecting the protection of Classified Information. In such cases, the Parties shall inform each other in compliance with Paragraphs 4 and 5 of Article 4 in order to discuss possible amendments to this Agreement. Meanwhile, the Classified Information shall be protected according to the provisions of the Agreement, unless otherwise agreed in writing.

3. No individual shall be entitled to access Classified Information solely by virtue of his or her rank, official position or previous Security Clearance. Access to Classified Information shall be granted only to those individuals who have been issued a Security Clearance and in accordance with the "Need to know" principle.

4. The Receiving Party is obligated:

   a) Not to disclose Classified Information to a Third Party without the prior written consent of the Competent Authority of the Transferring Party;

   b) To grant Classified Information a Security Classification Level equivalent to that provided by the Transferring Party;

c) Not to use Classified Information for other purposes than those for which it was provided;

d) To ensure the protection of Classified Information according to the terms of protection as provided in their respective national laws and regulations, unless otherwise requested in writing by the Transferring Party.

## ARTICLE 7
## TRANSLATION, REPRODUCTION AND DESTRUCTION OF CLASSIFIED INFORMATION

1. Classified Documents marked with a security classification level SECRETO / TUYỆT MẬT shall only be reproduced with the written permission of the Competent Authority of the Transferring Party.

2. All translations and reproductions of Classified Information shall be limited to the minimum number required for an official purpose and shall be made only by individuals with a "Need to know" and who are in possession of the appropriate Security Clearance. Such translations and reproductions shall bear an equivalent security classification marking of the Receiving Party and shall be placed under the same protection as the original information.

3. Translations shall contain a suitable annotation, in the language into which they have been translated, indicating that they contain Classified Information of the other Party.

4. Classified Information shall be destroyed or modified insofar as to prevent its reconstruction in whole or in part.

5. The Transferring Party may expressly prohibit reproduction, alteration or destruction of Classified Information by marking the relevant carrier of Classified Information or sending subsequent written notice. If destruction of the Classified Information is prohibited, it shall be returned to the Competent Authority of the Transferring Party.

6. Classified Information of SECRETO / TUYỆT MẬT Security Classification Level shall not be destroyed and shall be returned to the Competent Authority of the Transferring Party.

7. In case of a force majeure situation, which makes it impossible to protect

and return Classified Information generated or transferred according to this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent Authority of the Transferring Party in writing about the destruction of the Classified Information as soon as possible.

## ARTICLE 8
## CLASSIFIED CONTRACTS

1. Classified Contracts shall be concluded and implemented in accordance with the national laws and regulations of each Party. Upon request, the Competent Authority of each Party shall furnish information whether a proposed contractor has been issued a national Security Clearance, corresponding to the required Security Classification Level. If the proposed contractor does not hold a Security Clearance, the Competent Authority of each Party may request for that contractor to be security cleared.

2. A security annex will be an integral part of each Classified Contract or subcontract. In this annex, the contractor of the Party possessing Classified Information will specify which Classified Information will be released to the other Party, and which corresponding Security Classification Level has been assigned to this information.

3. The contractors' obligation to protect the Classified Information shall, in all cases, refer, at least, to the following:

   a) Disclosure of the Classified Information only to a person who has been previously security cleared for access with regard to the relevant contract activities, who has a "Need to know" and who is employed or engaged in the carrying out of the contract;

   b) The means to be used for the transfer of the Classified Information;

   c) The procedures and mechanisms for communicating the changes that may arise in respect of Classified Information either because of changes in its Security Classification Level or because protection is no longer necessary;

   d) The procedure for the approval of visits, access or inspection by personnel of one Party to facilities of the other Party which are covered by the contract;

e) To notify in due time the contractor's Competent Authority of any actual, attempted or suspected unauthorized access to Classified Information of the contract;

f) Usage of the Classified Information under the contract only for the purposes related to the subject matter of the contract;

g) Strict adherence to the procedures for destruction of Classified Information;

h) Provision of Classified Information under the contract to any Third Party only with the written consent of the Competent Authority of the Transferring Party.

## ARTICLE 9
## SECURITY INCIDENT

1. Any actual or suspected Security Incident concerning Classified Information of the other Party shall be investigated by the Party where the incident occurs. The other Party shall, if required, cooperate in the investigation.

2. If a Security Incident occurs in a third country, the Competent Authority of the Transferring Party shall take the actions under paragraph 1, when possible.

3. In all cases, the Competent Authority of the Party where the Security Incident has occurred shall inform the other Party of the results of the investigation, the extent of damage caused, solutions for recovery and any actions taken to prevent a recurrence.

## ARTICLE 10
## VISITS

1. Visits requiring access to Classified Information shall be subject to the prior written consent of the Competent Authority of the host Party.

2. Visit procedures shall be agreed between the Competent Authorities.

3. The request for visit shall contain at least the following information:

a) Name, date and place of birth, nationality, passport (ID card) number of the visitor;

b) Position, title of the visitor and name of the organization he/she represents if applicable, a description of the Classified Contract in which they are participating and the subject of the visit;

c) Confirmation and date of expiry of the visitor's Security Clearance;

d) Purpose, proposed working programme and planned date of the visit. In the case of recurring visits the total period covered by the visits shall be stated;

e) Names of organizations and facilities to be visited;

f) Name, address, phone number, fax number (if applicable), and e-mail address of the point of contact of the organization or facility to be visited.

g) The anticipated level of Classified Information to be discussed or accessed;

4. The Competent Authorities of the Parties may agree to establish lists of authorized persons to make recurring visits. These lists are valid for an initial period of twelve months. Once these lists have been approved by the Competent Authorities of the Parties, the terms of the specific visits shall be arranged directly with the appropriate authorities of the organization or facility to be visited, in accordance with the terms and conditions agreed upon.

5. Each Party shall guarantee protection of personal data of the visitors, according to the respective national laws and regulations.

6. Each Party shall have the right to exclude from the list of visitors certain individual(s).

## ARTICLE 11
## EXPENSES

In the case of any cost, each Party shall bear the expenses incurred in the course of implementing its obligations under this Agreement.

## ARTICLE 12
## FINAL PROVISIONS

1. This Agreement is concluded for an indefinite period of time and shall enter into force on the date of receipt of the last written notification whereby the Parties inform each other of the fulfillment of all internal legal procedures necessary for its entry into force.

2. This Agreement may be amended on the basis of mutual written consent by both Parties. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

3. Each Party may terminate this Agreement by written notice forwarded to the other Party. The termination shall enter into force six months after the date of receipt of the notification. Notwithstanding the termination of this Agreement, all Classified Information generated or transferred pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein, until the Transferring Party dispenses the Receiving Party from this obligation.

4. Any dispute regarding the interpretation or application of this Agreement shall be resolved amicably by consultation between the Parties without recourse to outside jurisdiction.

Done at Madrid, on the 27th day of March 2019, in two original copies, each in the Spanish, Vietnamese and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English language text shall prevail.

**For the Kingdom of Spain**

FÉLIX SANZ ROLDÁN
Secretary of State
Director of the
National Intelligence Centre

**For the Socialist Republic of Viet Nam**

BÙI VĂN NAM
Deputy Minister of Public Security

[ TEXT IN SPANISH – TEXTE EN ESPAGNOL ]

# ACUERDO

# ENTRE

# EL REINO DE ESPAÑA

# Y

# LA REPÚBLICA SOCIALISTA DE VIETNAM

# SOBRE

# INTERCAMBIO Y PROTECCIÓN MUTUA

# DE INFORMACIÓN CLASIFICADA

El Reino de España y la República Socialista de Vietnam (denominados en lo sucesivo "las Partes"),

Habiendo acordado ampliar su cooperación política, militar y económica y mantener conversaciones sobre asuntos políticos y de seguridad,

Conscientes de los cambios en la situación política mundial y reconociendo la importancia de su cooperación mutua para la consecución de la paz, la estabilidad y la seguridad nacional e internacional,

Conscientes de que una buena cooperación puede exigir el intercambio de Información Clasificada entre las Partes,

Deseando constituir un conjunto de normas que regule la protección recíproca de la Información Clasificada y que resulte aplicable a futuros acuerdos de cooperación y contratos clasificados entre las Partes que contengan o supongan el intercambio de Información Clasificada.

Han convenido en lo siguiente:

## ARTÍCULO 1
## DEFINICIONES

En el presente Acuerdo, los términos empleados se entenderán conforme a las siguientes definiciones:

1. Por **"Información Clasificada"** se entenderá información, cualquiera que sea su forma, naturaleza o método de transmisión, generada o en proceso de ser generada, a la que se la haya asignado un grado de clasificación de seguridad y que, en interés de la seguridad nacional y conforme a las leyes y reglamentos nacionales, requiera protección frente a la destrucción o el acceso no autorizados.

2. Por **"Acceso no autorizado a Información Clasificada"** se entenderá el acceso de cualquier persona física o jurídica a Información Clasificada sin la aprobación de la Autoridad Competente, de conformidad con las leyes y los reglamentos nacionales de las Partes y las disposiciones del presente Acuerdo.

3. Por **"Grado de Clasificación de Seguridad"** se entenderá la categoría asignada a la Información Clasificada con indicación del grado de sensibilidad, grado de perjuicio que puede producirse en caso de divulgación no autorizada o pérdida, y el grado de protección que deben aplicar las Partes.

4. Por **"Marca de clasificación"** se entenderá una marca que indique el Grado de Clasificación de Seguridad de la Información Clasificada.

5. Por **"Habilitación de Seguridad"** se entenderá la determinación efectiva, derivada de un procedimiento de habilitación, de la lealtad y fiabilidad de una persona física o jurídica, así como de otros aspectos relativos a la seguridad, de conformidad con las leyes y reglamentos nacionales. Dicha determinación permite conceder la autorización de acceso a la Información Clasificada a las personas físicas y jurídicas, que podrán manejarla hasta un grado específico.

6. Por **"Parte Transmitente"** se entenderá la Parte que remita Información Clasificada.

7. Por **"Parte Receptora"** se entenderá la Parte a la que se transmita la Información Clasificada.

8. Por **"Usuario"** se entenderá una persona física o jurídica que participe en actividades de cooperación pertinentes o en la ejecución de Contratos Clasificados a los que resulte aplicable el presente Acuerdo.

9. Por **"Autoridad Competente"** se entenderá la autoridad que, de conformidad con las leyes y reglamentos nacionales de las Partes, ostente la responsabilidad última de proteger la Información Clasificada, ejerza el control general en este ámbito y dirija y supervise la aplicación del presente Acuerdo. Dichas autoridades se enumeran en el artículo 4.

10. Por **"Contratista"** se entenderá toda persona física o jurídica con capacidad jurídica para celebrar contratos al amparo de lo dispuesto en el presente Acuerdo.

11. Por **"Contrato Clasificado"** se entenderá un acuerdo entre los usuarios de las Partes que contenga Información Clasificada o cuya ejecución requiera acceder a Información Clasificada de cualquiera de las Partes o la genere.

12. Por **«Principio de "Necesidad de conocer"»** se entenderá la necesidad de tener acceso a Información Clasificada a efectos del desempeño de funciones oficiales y para la ejecución de un cometido oficial específico.

13. Por **"Tercero"** se entenderá todo Estado, organización internacional o usuario que no sea Parte en el presente Acuerdo.

14. Por **"Desclasificación de Información"** se entenderá la retirada del grado de clasificación de seguridad.

15. Por **"Incidente de Seguridad"** se entenderá toda acción u omisión contraria a las leyes y los reglamentos nacionales que puedan resultar o resulten en el acceso o la divulgación no autorizados, la pérdida, la destrucción o comprometimiento de la Información Clasificada que haya sido generada y/o intercambiada en virtud del presente Acuerdo.

## ARTÍCULO 2
## OBJETO

El objeto del presente Acuerdo es asegurar la protección de la Información Clasificada intercambiada entre las Partes. Establece los procedimientos y acuerdos de seguridad para dicha protección.

## ARTÍCULO 3
## GRADOS DE CLASIFICACIÓN DE SEGURIDAD

1. Las Partes acuerdan que los siguientes Grados de Clasificación de Seguridad son equivalentes y se corresponden con los Grados de Clasificación de Seguridad previstos en la legislación de cada Parte respectiva.

| Para el Reino de España | Para la República Socialista de Vietnam |
|---|---|
| SECRETO | TUYỆT MẬT |
| RESERVADO | TỐI MẬT |
| CONFIDENCIAL | MẬT |

2. La información recibida del Reino de España clasificada como DIFUSIÓN LIMITADA se protegerá en la República Socialista de Vietnam como el grado MẬT.

## ARTÍCULO 4
## AUTORIDADES COMPETENTES

1. Las Autoridades Competentes de cada Parte serán:

   **Por el Reino de España**:
   Centro Nacional de Inteligencia.

   **Por la República Socialista de Vietnam**:
   Ministerio de Seguridad Pública.

2. Las Partes se notificarán mutuamente por vía diplomática cualquier modificación que afecte a sus Autoridades Competentes.

3. Las Autoridades Competentes se informarán mutuamente de las leyes y los reglamentos nacionales vigentes en materia de protección de la Información Clasificada.

4. Para garantizar una cooperación estrecha en la aplicación del presente Acuerdo, las Autoridades Competentes podrán celebrar consultas a solicitud de cualquiera de ellas.

5. Con objeto de establecer y mantener normas de seguridad comparables, las Autoridades Competentes de cada Parte se facilitarán mutuamente, previa petición, información sobre las normas, procedimientos y prácticas que apliquen en materia de seguridad para la protección de la Información Clasificada.

6. Las Autoridades Competentes de las Partes podrán celebrar Acuerdos de Aplicación de conformidad con el presente Acuerdo.

7. Los Servicios de Seguridad de las Partes podrán intercambiar y facilitarse directamente entre sí información operativa y/o de inteligencia, de conformidad con las leyes y reglamentos nacionales.

## ARTÍCULO 5
## TRANSMISIÓN DE INFORMACIÓN CLASIFICADA

1. La Información Clasificada marcada como CONFIDENCIAL / MẬT o superior se transmitirá en general por conducto diplomático. Sin embargo, podrán emplearse otros conductos, de conformidad con las leyes y reglamentos nacionales, si así lo acuerdan las Autoridades Competentes. La Parte Receptora confirmará por escrito la recepción de

la Información Clasificada marcada como CONFIDENCIAL / MẠT o superior.

2. La Información Clasificada que se transmita por vía electrónica se protegerá por medios criptográficos aprobados de mutuo acuerdo por las Autoridades Competentes y dotados de un certificado debidamente expedido conforme a las leyes y reglamentos nacionales de las Partes.

3. Si es preciso transmitir un gran volumen de Información Clasificada, las Autoridades Competentes aprobarán de mutuo acuerdo un plan de transporte, que incluirá los medios de transporte, las necesidades de escolta, la ruta y otras medidas de seguridad.

## ARTÍCULO 6
## MEDIDAS DE PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

1. Las Partes, con arreglo a sus leyes y reglamentos nacionales, adoptarán todas las medidas que resulten adecuadas para la protección de la Información Clasificada que se genere o intercambie en virtud del presente Acuerdo, que se protegerá como Información Clasificada nacional con el Grado de Clasificación de Seguridad correspondiente.

2. Las Partes se informarán mutuamente de cualquier modificación de sus leyes y reglamentos nacionales que afecte a la protección de la Información Clasificada. En tales casos, las Partes se informarán mutuamente conforme a lo previsto en los apartados 4 y 5 del artículo 4, a fin de debatir posibles modificaciones del presente Acuerdo. Entretanto, la Información Clasificada se protegerá con arreglo a las disposiciones del Acuerdo, salvo pacto escrito en contrario.

3. No se autorizará a ninguna persona el acceso a Información Clasificada únicamente por razón de su rango, cargo oficial o Habilitación de Seguridad. Dicho acceso sólo se concederá a aquellas personas a las que se le haya expedido una Habilitación de Seguridad previa y con arreglo al principio de "Necesidad de conocer".

4. La Parte Receptora estará obligada a:

   a) No divulgar Información Clasificada a Terceros sin el consentimiento previo por escrito de la Autoridad Competente de la Parte Transmitente;

b) Asignarle a la Información Clasificada un Grado de Clasificación de Seguridad equivalente al atribuido por la Parte Transmitente;

c) No usar la Información Clasificada para fines distintos de aquellos para los que se ha facilitado;

d) Velar por la protección de la Información Clasificada conforme a las condiciones establecidas en sus leyes y reglamentos nacionales, salvo que la Parte Transmitente solicite otra cosa por escrito.

## ARTÍCULO 7
## TRADUCCIÓN, REPRODUCCIÓN Y DESTRUCCIÓN DE INFORMACIÓN CLASIFICADA

1. Los Documentos Clasificados marcados con el grado de clasificación de seguridad SECRETO / TUYỆT MẬT solo se podrán reproducir con la autorización por escrito de la Autoridad Competente de la Parte Transmitente.

2. Las traducciones y reproducciones de Información Clasificada se limitarán a las mínimas requeridas para fines oficiales y serán realizadas exclusivamente por personas con "Necesidad de conocer" y que sean titulares de la Habilitación de Seguridad correspondiente. En estas traducciones y reproducciones deberá figurar la marca de clasificación de seguridad equivalente de la Parte Receptora y serán objeto de la misma protección que la información original.

3. Las traducciones incorporarán una anotación adecuada en el idioma de destino en la que se indicará que contienen Información Clasificada de la otra Parte.

4. Se destruirá o modificará la Información Clasificada en la medida en que sea necesario para evitar su reconstrucción total o parcial.

5. La Parte Transmitente podrá prohibir expresamente la reproducción, alteración o destrucción de Información Clasificada a través de una marca en el soporte de esta o notificándolo por escrito posteriormente. La Información Clasificada cuya destrucción se prohíba se devolverá a la Autoridad Competente de la Parte Transmitente.

6. La Información Clasificada con el grado de clasificación de seguridad SECRETO / TUYỆT MẬT no se destruirá y se devolverá a la Autoridad Competente de la Parte Transmitente.

7. En caso de fuerza mayor en el que resulte imposible proteger y devolver Información Clasificada que se haya generado o transmitido con arreglo al presente Acuerdo, se procederá a su destrucción inmediata. La Parte Receptora notificará por escrito la destrucción de Información Clasificada a la Autoridad Competente de la Parte Transmitente lo antes posible.

## ARTÍCULO 8
## CONTRATOS CLASIFICADOS

1. Los Contratos Clasificados se celebrarán y ejecutarán de acuerdo con las leyes y los reglamentos nacionales de las Partes. Previa solicitud, las Autoridades Competentes de las Partes comunicarán si los contratistas propuestos son titulares de la Habilitación de Seguridad nacional que se corresponda con el Grado de Clasificación de Seguridad exigido. Si el contratista propuesto no posee una Habilitación de Seguridad, las Autoridades Competentes de cada una de las Partes podrán solicitar que se le habilite.

2. Los Contratos o Subcontratos Clasificados incluirán un anexo sobre seguridad, en el que el contratista de la Parte titular de la Información Clasificada especificará cuál se cederá a la otra Parte y qué Grado de Clasificación de Seguridad correspondiente se le ha asignado.

3. La obligación de los contratistas de proteger la Información Clasificada se extenderá, sin excepción, al menos, a:

   a) La divulgación de Información Clasificada exclusivamente a quienes hayan obtenido previamente una habilitación de seguridad de acceso relativa a las actividades del contrato en cuestión, tengan "Necesidad de conocer" y a quienes se haya asignado como trabajo o labor la ejecución de dicho contrato.

   b) Los medios empleados para la transmisión de la Información Clasificada.

   c) Los procedimientos y mecanismos para comunicar cualquier cambio que pueda afectar a la Información Clasificada, sea porque se haya modificado su Grado de Clasificación de Seguridad, sea porque la protección haya dejado de ser necesaria.

   d) Los procedimientos para la autorización de visitas, del acceso o de inspecciones por parte del personal de una de las Partes a los establecimientos de la otra que estén comprendidos en el contrato.

e) La notificación oportuna a la Autoridad Competente del contratista de cualquier acceso real, frustrado o presunto no autorizado a la Información Clasificada a la que se refiere el contrato.

f) El uso de la Información Clasificada prevista en el contrato únicamente para los fines vinculados al objeto de este.

g) La observancia estricta de los procedimientos de destrucción de Información Clasificada;

h) La puesta a disposición de Terceros de la Información Clasificada a la que se refiere el contrato exclusivamente con el consentimiento por escrito de la Autoridad Competente de la Parte Transmitente.

## ARTÍCULO 9
## INCIDENTE DE SEGURIDAD

1. La Parte en la que suceda cualquier Incidente de Seguridad real o presunto que afecte a Información Clasificada de la otra se ocupará de investigarlo, si es necesario, con la cooperación de esta última.

2. Si ocurre un Incidente de Seguridad en un tercer país, la Autoridad Competente de la Parte Transmitente emprenderá las acciones establecidas en el apartado 1 en la medida de lo posible.

3. Sin excepción, la Autoridad Competente de la Parte en la que suceda un Incidente de Seguridad informará a la otra de las conclusiones de la investigación, el alcance de los daños ocasionados, las medidas de recuperación y las acciones emprendidas para evitar que se repita la situación.

## ARTÍCULO 10
## VISITAS

1. Las visitas que impliquen el acceso a Información Clasificada exigirán la previa autorización por escrito de la Autoridad Competente de la Parte anfitriona.

2. Las Autoridades Competentes convendrán en los procedimientos de visita.

3. Las solicitudes de visita contendrán, al menos, la siguiente información:

a) Nombre, fecha y lugar de nacimiento, nacionalidad y número de pasaporte (tarjeta de identidad) del visitante.

b) Cargo del visitante, nombre de la entidad a la que representa y, cuando proceda, la descripción del Contrato Clasificado en el que participan y el objeto de la visita.

c) Confirmación y fecha de expiración de la Habilitación de Seguridad del visitante.

d) Finalidad, programa de trabajo propuesto y fecha prevista de la visita. Si se trata de visitas recurrentes deberá indicarse el periodo total en el que se producirán.

e) Nombres de las entidades y de los establecimientos que se visitarán.

f) Nombre, dirección, número de teléfono y de fax (si procede) y dirección de correo electrónico del punto de contacto de la entidad o el establecimiento que se visitará.

g) El grado previsto de la Información Clasificada que se analizará o a la que se accederá;

4. Las Autoridades Competentes de las Partes podrán preparar listas con las personas autorizadas para realizar visitas recurrentes. Estas listas tendrán una validez inicial de doce meses. Una vez las Autoridades Competentes de las Partes las hayan aprobado, las condiciones de cada visita concreta se acordarán administrativamente con las autoridades de la entidad o el establecimiento que se vaya a visitar directamente y a tenor de las condiciones generales que se hayan pactado.

5. Las Partes garantizarán la protección de los datos personales de los visitantes, de conformidad con las respectivas leyes y reglamentos nacionales.

6. Las Partes tendrán derecho a excluir de la lista de visitantes a ciertas personas físicas.

## ARTÍCULO 11
## GASTOS

Si se produce algún coste, cada Parte se hará cargo de los gastos en que haya incurrido al ejecutar sus obligaciones con arreglo al presente Acuerdo.

## ARTÍCULO 12
## DISPOSICIONES FINALES

1. El presente Acuerdo se concluye por un periodo indefinido y surtirá efecto desde la fecha de recepción de la última notificación por escrito en la que las Partes se informen mutuamente de que se han cumplido todos los trámites jurídicos nacionales necesarios para la entrada en vigor.

2. El presente Acuerdo podrá modificarse con el consentimiento por escrito de ambas Partes. Las modificaciones entrarán en vigor de conformidad con el apartado 1 del presente artículo.

3. Las Partes podrán terminar el presente Acuerdo notificándoselo a la otra por escrito. La terminación surtirá efectos transcurridos seis meses desde la fecha de recepción de la notificación al respecto. Sin perjuicio de la terminación del presente Acuerdo, toda la Información Clasificada generada o transmitida en virtud del mismo seguirá protegiéndose según lo dispuesto en él hasta que la Parte Transmitente exima a la Parte Receptora de esta obligación.

4. Las controversias relativas a la interpretación o aplicación del presente Acuerdo se resolverán de manera amistosa mediante consultas entre las Partes, sin que deban someterse a un tercero ajeno al mismo.

Hecho en Madrid, el 27 de marzo de 2019 en dos ejemplares originales, ambos en español, vietnamita e inglés, siendo todos los textos igualmente auténticos. En caso de discrepancias en la interpretación, prevalecerá el texto en inglés.

**Por el Reino de España**

FÉLIX SANZ ROLDÁN
Secretario de Estado
Director del Centro Nacional de Inteligencia

**Por la República Socialista de Vietnam**

BÙI VĂN NAM
Viceministro de Seguridad Pública

[ TEXT IN VIETNAMESE – TEXTE EN VIETNAMIEN ]

# HIỆP ĐỊNH

# GIỮA VƯƠNG QUỐC TÂY BAN NHA VÀ

# NƯỚC CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

# VỀ CÙNG BẢO VỆ VÀ TRAO ĐỔI TIN MẬT

Vương quốc Tây Ban Nha và nước Cộng hòa xã hội chủ nghĩa Việt Nam (sau đây gọi là "các Bên"),

Đã nhất trí mở rộng hợp tác chính trị, quân sự và kinh tế và tổ chức đối thoại về các vấn đề liên quan đến chính trị và an ninh,

Nhận thức về những thay đổi về tình hình chính trị thế giới và nhận thấy vai trò quan trọng của hợp tác song phương vì hoà bình, ổn định, an ninh quốc gia, và an ninh quốc tế,

Nhận thấy rằng hợp tác tốt có thể đặt ra yêu cầu trao đổi tin mật giữa các Bên,

Mong muốn tạo ra các quy tắc về việc cùng bảo vệ tin mật được áp dụng cho bất kỳ thỏa thuận hợp tác và các hợp đồng mật nào trong tương lai sẽ được thực hiện giữa các Bên có chứa đựng hoặc liên quan đến tin mật,

Đã thoả thuận như sau:

## Điều 1
## Định nghĩa

Trong Hiệp định này, các khái niệm sau đây được hiểu như sau:

1. "Tin mật" là thông tin thuộc bất kỳ hình thức, loại hoặc phương pháp truyền tin nào đã được tạo ra hoặc đang trong quá trình tạo ra mà đã được xác định độ mật, vì lợi ích của an ninh quốc gia và phù hợp với pháp luật của quốc gia đòi hỏi được bảo vệ chống sự tiếp cận hoặc phá hủy trái phép.
2. "Tiếp cận tin mật trái phép" là việc các cá nhân hay pháp nhân tiếp cận tin mật mà không được cơ quan có thẩm quyền cho phép theo quy định của pháp luật quốc gia của các Bên và quy định tại Hiệp định này.
3. "Độ mật" là cấp độ xác định cho tin mật để chỉ rõ mức độ mật, mức độ thiệt hại có thể xảy ra trong trường hợp bị mất hoặc tiết lộ và mức độ bảo vệ được áp dụng bởi các bên.
4. "Dấu mật" là dấu được đóng trên tin mật cho thấy cấp độ mật.

5. "Giấy phép an ninh" là một sự xác định tích cực bắt nguồn từ quy trình xác minh đảm bảo sự trung thành và đáng tin cậy của một cá nhân hoặc pháp nhân cũng như các khía cạnh an ninh khác phù hợp với luật pháp quốc gia. Sự xác định ấy cho phép cá nhân hoặc pháp nhân tiếp cận và cho phép họ xử lý tin mật ở một mức độ nào đó.

6. "Bên chuyển giao" là Bên gửi tin mật.

7. "Bên nhận" là Bên tin mật được chuyển đến.

8. "Người sử dụng" là một cá nhân hoặc pháp nhân tham gia vào các hoạt động hợp tác liên quan hoặc tham gia vào việc thực hiện các hợp đồng mật mà Hiệp định này sẽ được áp đụng.

9. "Cơ quan có thẩm quyền" là nhà chức trách, phù hợp với pháp luật của quốc gia của các Bên có trách nhiệm cao nhất trong việc bảo vệ tin mật, tiến hành kiểm soát tổng thể trong lĩnh vực này cũng như giám sát việc thực hiện Hiệp định, triển khai Hiệp định này. Các nhà chức trách đó được nêu tại Điều 4 Hiệp định này.

10. "Bên ký hợp đồng" là một cá nhân hoặc một pháp nhân có năng lực pháp lý ký kết các hợp đồng theo quy định của Hiệp định này.

11. "Hợp đồng mật" là một thỏa thuận giữa những người sử dụng của các Bên có chứa đựng tin mật hoặc việc thực hiện sẽ tạo ra hoặc cần thiết tiếp cận tin mật của mỗi Bên.

12. "Nguyên tắc "cần biết"" là sự cần thiết có sự tiếp cận với tin mật liên quan tới những nhiệm vụ chính thức và để thực hiện một nhiệm vụ chính thức cụ thể.

13. "Bên thứ ba" là một nhà nước hoặc tổ chức quốc tế hoặc một người sử dụng không phải là một Bên ký kết Hiệp định này.

14. "Hủy độ mật của thông tin" là việc dỡ bỏ cấp độ mật.

15. "Vi phạm an ninh" là một hành động hoặc không hành động trái với luật pháp quốc gia, dẫn đến hoặc có thể dẫn đến việc tiếp cận, tiết lộ, mất, phá hủy, hoặc gây tổn hại trái phép đối với tin mật được trao đổi và/ hoặc tạo ra trong Hiệp định này.

## Điều 2
## Mục đích

Mục đích của Hiệp định này là nhằm đảm bảo việc bảo vệ tin mật được trao đổi giữa các Bên. Hiệp định quy định các quy trình và thu xếp về an ninh cho công tác bảo vệ tin mật đó.

## Điều 3
## Các cấp độ mật

1. Các Bên đồng ý rằng các cấp độ mật sau là tương ứng và phù hợp với các cấp độ mật được quy định trong pháp luật của quốc gia của mỗi Bên:

| Đối với Vương quốc Tây Ban Nha | Đối với nước Cộng hòa xã hội chủ nghĩa Việt Nam |
|---|---|
| SECRETO | TUYỆT MẬT |
| RESERVADO | TỐI MẬT |
| CONFIDENCIAL | MẬT |

2. Thông tin nhận được từ Vương quốc Tây Ban Nha được xác định là DIFUSION LIMITADA (LƯU HÀNH NỘI BỘ) sẽ được bảo vệ như thông tin MẬT tại Cộng hòa xã hội chủ nghĩa Việt Nam.

## Điều 4
## Các cơ quan có thẩm quyền

1. Các cơ quan có thẩm quyền của các Bên là:

**Đối với Vương quốc Tây Ban Nha:**

Cơ quan Tình báo Quốc gia;

**Đối với nước Cộng hoà xã hội chủ nghĩa:**

Việt Nam: Bộ Công an.

2. Các Bên sẽ thông báo cho nhau thông qua kênh ngoại giao về những thay đổi đối với các cơ quan có thẩm quyền.

3. Các cơ quan có thẩm quyền sẽ thông báo cho nhau về pháp luật hiện hành của quốc gia quy định về bảo vệ tin mật.

4. Nhằm đảm bảo hợp tác chặt chẽ trong việc thực hiện Hiệp định này, các cơ quan có thẩm quyền có thể tổ chức tham vấn theo yêu cầu của một trong hai Bên.

5. Nhằm đạt được và duy trì các tiêu chuẩn an ninh tương đương, các cơ quan có thẩm quyền, theo yêu cầu sẽ cung cấp cho nhau thông tin về tiêu chuẩn an ninh, trình tự, thủ tục và thực tiễn trong việc bảo vệ tin mật được áp dụng của Bên đó.

6. Các cơ quan có thẩm quyền của các Bên có thể ký kết các thỏa thuận thực hiện liên quan Hiệp định này.

7. Các cơ quan An ninh của các Bên có thể trao đổi và trả lại thông tin nghiệp vụ và/hoặc tình báo trực tiếp với nhau phù hợp với luật pháp của quốc gia.

## Điều 5
## Chuyển giao tin mật

1. Tin mật được đóng dấu từ mức độ CONFIDENCIAL/MẬT trở lên thông thường được chuyển qua kênh ngoại giao. Tuy nhiên, các kênh khác cũng có thể được thống nhất bởi các cơ quan có thẩm quyền phù hợp với quy định pháp luật quốc gia của các Bên. Bên nhận sẽ khẳng định bằng văn bản khi nhận được tin mật được đánh dấu từ mức độ CONFIDENCIAL/MẬT trở lên.

2. Tin mật được chuyển qua kênh điện tử sẽ được bảo vệ bởi các biện pháp mã hóa được sự đồng ý bởi các cơ quan có thẩm quyền và được chứng nhận theo quy định của pháp luật quốc gia của mỗi Bên.

3. Trong trường hợp chuyển giao một bao kiện lớn có chứa tin mật, các cơ quan có thẩm quyền sẽ cùng thỏa thuận về kế hoạch vận chuyển, phương tiện, yêu cầu hộ tống tuyến đường và các biện pháp an ninh khác.

## Điều 6
## Các biện pháp bảo vệ tin mật

1. Phù hợp với pháp luật của quốc gia mình, các Bên sẽ triển khai mọi biện pháp phù hợp để bảo vệ tin mật được tạo ra hoặc chuyển giao theo Hiệp định này. Tin mật đó sẽ được bảo vệ như tin mật của quốc gia có cùng cấp độ mật.

2. Các Bên sẽ thông báo cho nhau về bất kỳ thay đổi nào về luật pháp của quốc gia mình ảnh hưởng đến việc bảo vệ tin mật. Trong trường hợp như vậy, các Bên sẽ thông báo cho nhau theo quy định tại Khoản 4 và Khoản 5 Điều 4 nhằm trao đổi về khả năng sửa đổi Hiệp định này. Trong thời gian đó, tin mật sẽ được bảo vệ phù hợp với quy định của Hiệp định này, trừ khi có thỏa thuận khác bằng văn bản.

3. Không có cá nhân nào được quyền tiếp cận tin mật chỉ vì cấp bậc, chức vụ hoặc giấy phép an ninh trước đó. Việc tiếp cận tin mật sẽ chỉ được dành cho những cá nhân đã được cấp giấy phép an ninh và phù hợp với nguyên tắc "cần biết".

4. Bên nhận có trách nhiệm:

   a) Không tiết lộ tin mật cho Bên thứ ba mà không có sự đồng ý trước bằng văn bản của cơ quan có thẩm quyền của Bên chuyển giao;

   b) Quy định cấp độ mật của tin mật tương đương với cấp độ mật do Bên chuyển giao quy định;

   c) Không sử dụng tin mật cho các mục đích khác với các mục đích mà tin mật đã được cung cấp;

   d) Đảm bảo việc bảo vệ tin mật với thời hạn theo quy định pháp luật của quốc gia mình, trừ khi có yêu cầu khác bằng văn bản của Bên chuyển giao.

## Điều 7
## Dịch, nhân bản và hủy tin mật

1. Phù hợp với pháp luật của mỗi Bên, tin mật được đóng dấu SECRETO/ TUYỆT MẬT chỉ được nhân bản khi có sự đồng ý bằng văn bản của cơ quan có thẩm quyền của Bên chuyển giao.

2. Mọi việc dịch thuật, nhân bản tin mật sẽ được hạn chế cho mục đích chính thống và thực hiện đối với những người có nhu cầu phải biết và có giấy phép an ninh. Bản dịch đó sẽ được đóng dấu mật tương đương của Bên nhận và được bảo vệ như bản gốc.

3. Các bản dịch sẽ có chú thích phù hợp bằng ngôn ngữ đã được dịch chỉ rõ bản dịch có chứa tin mật của bên cung cấp.

4. Tin mật sẽ được hủy hoặc sửa đổi tới mức nhằm ngăn ngừa tái tạo toàn bộ hoặc một phần.

5. Bên chuyển giao có thể nêu rõ việc cấm nhân bản, thay thế hoặc hủy tin mật bằng cách đánh dấu vật chứa tin mật phù hợp hoặc gửi văn bản thông báo sau đó. Nếu việc hủy tin mật bị cấm thì tài liệu đó sẽ được trả lại cho cơ quan có thẩm quyền của Bên chuyển giao.

6. Tin mật độ SECRETO/ TUYỆT MẬT không được phép hủy và được trả lại cho cơ quan có thẩm quyền của Bên chuyển giao.

7. Trong trường hợp bất khả kháng không thể bảo vệ và trả lại tin mật đã được tạo ra hoặc được chuyển giao theo Hiệp định này, tin mật sẽ được hủy ngay lập tức. Bên nhận sẽ thông báo bằng văn bản cho cơ quan có thẩm quyền của Bên chuyển giao về việc hủy tin mật sớm nhất khi có thể.

## Điều 8
## Các hợp đồng mật

1. Hợp đồng mật sẽ được ký kết và triển khai phù hợp với quy định của pháp luật mỗi Bên. Theo yêu cầu, cơ quan có thẩm quyền của mỗi Bên sẽ cung cấp thông tin về việc bên được đề nghị ký kết hợp đồng đã được cấp giấy phép an ninh của quốc gia mình phù hợp với yêu cầu độ mật của

thông tin. Nếu bên được đề nghị ký kết hợp đồng không có giấy phép an ninh thì cơ quan có thẩm quyền của mỗi Bên có thể yêu cầu bên được đề nghị ký hợp đồng bảo đảm về an ninh.

2. Một phụ lục an ninh sẽ là một phần không tách rời của mỗi hợp đồng mật hoặc tiểu hợp đồng mật. Trong phụ lục này bên ký hợp đồng của Bên có tin mật sẽ quy định tin mật nào sẽ được tiết lộ cho bên kia và độ mật của thông tin đó.

3. Trong mọi trường hợp, trách nhiệm tối thiểu của các bên ký hợp đồng là:

a) Chỉ tiết lộ tin mật cho người mà trước đó đã có bảo đảm về mặt an ninh cho việc tiếp cận liên quan đến các hoạt động theo hợp đồng, đó là người "cần biết" và người được thuê hoặc tham gia vào việc triển khai thực hiện hợp đồng;

b) Phương tiện được sử dụng để chuyển giao tin mật;

c) Thủ tục và cơ chế thông báo những thay đổi có thể phát sinh liên quan đến tin mật do thay đổi về độ mật hoặc do không còn cần thiết bảo vệ;

d) Thủ tục phê duyệt các chuyến thăm, tiếp cận hoặc giám sát bởi nhân viên của một Bên đối với các cơ sở của Bên kia được nêu trong hợp đồng;

e) Thông báo kịp thời cho cơ quan có thẩm quyền của Bên ký hợp đồng về bất kỳ sự tiếp cận, âm mưu tiếp cận hoặc nghi ngờ có sự tiếp cận trái phép tin mật của hợp đồng;

f) Sử dụng tin mật theo hợp đồng chỉ vì các mục đích liên quan tới nội dung của hợp đồng;

g) Tuân thủ nghiêm ngặt quy trình hủy tin mật;

h) Cung cấp tin mật theo hợp đồng cho bất kỳ Bên thứ ba nào chỉ khi có sự đồng ý bằng văn bản của cơ quan có thẩm quyền của Bên có tin mật.

## Điều 9
## Vi phạm an ninh

1. Bất kỳ vi phạm an ninh nào đã xảy ra trên thực tế hoặc đang bị tình nghi liên quan đến tin mật của bên kia sẽ được điều tra bởi Bên nơi mà sự việc đó xảy ra. Bên kia sẽ hợp tác trong công tác điều tra, nếu được yêu cầu.

2. Nếu vi phạm an ninh xảy ra ở nước thứ ba, cơ quan có thẩm quyền của Bên gửi sẽ thực hiện các hành động theo quy định của Khoản 1 Điều này khi có thể.

3. Trong bất kỳ trường hợp nào, cơ quan có thẩm quyền của Bên mà vi phạm an ninh xảy ra phải thông báo cho Bên kia về kết quả điều tra, mức độ thiệt hại xảy ra biện pháp khắc phục, và bất kỳ hành động nào được áp dụng để ngăn ngừa tái diễn.

## Điều 10
## Các chuyến thăm

1. Các chuyến thăm yêu cầu tiếp cận thông tin mật cần có sự đồng ý trước bằng văn bản của cơ quan có thẩm quyền của Bên kia.

2. Thủ tục cho các chuyến thăm sẽ được thống nhất giữa các cơ quan có thẩm quyền.

3. Yêu cầu tổ chức chuyến thăm sẽ ít nhất bao gồm những thông tin sau:

   a) Họ tên, ngày và nơi sinh, quốc tịch, số hộ chiếu (chứng minh thư) của người đến thăm;

   b) Chức vụ của người đến thăm và tên cơ quan người đó đại diện, nếu phù hợp, miêu tả về hợp đồng mật mà trong đó họ tham gia vào chủ đề của chuyến thăm;

   c) Xác định và ngày hết hạn giấy phép an ninh của người đến thăm;

   d) Mục đích, dự kiến chương trình làm việc và thời gian của chuyến thăm, trong trường hợp có các chuyến thăm tiếp theo thì tổng thời gian của các chuyến thăm sẽ được nêu rõ;

   e) Tên cơ quan và cơ sở sẽ được đến thăm;

f) Tên, địa chỉ, số điện thoại, số fax (nếu có), và địa chỉ email của đầu mối liên lạc của tổ chức hoặc cơ sở sẽ được đến thăm;

g) Độ mật dự kiến của tin mật được trao đổi hoặc tiếp cận.

4. Các cơ quan có thẩm quyền của các Bên có thể thỏa thuận đưa ra danh sách những người được ủy quyền để thu xếp các chuyến thăm định kỳ. Các danh sách đó có giá trị trong 12 tháng. Khi các danh sách đó đã được các cơ quan có thẩm quyền của các Bên thông qua, thời hạn của các chuyến thăm cụ thể sẽ được thu xếp trực tiếp với các nhà chức trách của tổ chức hoặc cơ sở được đến thăm, phù hợp với thời hạn và điều kiện đã được thống nhất.

5. Mỗi Bên sẽ đảm bảo công tác bảo vệ dữ liệu cá nhân của người đến thăm, phù hợp với quy định của luật pháp quốc gia.

6. Mỗi Bên có quyền loại một hoặc một số cá nhân khỏi danh sách những người đến thăm.

## Điều 11
## Chi phí

Trong trường hợp có bất kỳ chi phí nào, mỗi Bên sẽ tự chịu chi phí liên quan phát sinh trong quá trình thực hiện các nghĩa vụ của mình theo Hiệp định này.

## Điều 12
## Điều khoản cuối cùng

1. Hiệp định này có hiệu lực vô thời hạn và sẽ có hiệu lực kể từ ngày nhận được thông báo cuối cùng bằng văn bản mà theo đó các Bên thông báo cho nhau về việc hoàn thành các thủ tục nội bộ cần thiết để Hiệp định có hiệu lực.

2. Hiệp định này có thể được sửa đổi trên cơ sở có sự đồng ý bằng văn bản của cả hai Bên. Việc sửa đổi như vậy sẽ có hiệu lực phù hợp với Khoản 1 của Điều này.

3. Mỗi Bên có thể chấm dứt Hiệp định bằng cách thông báo bằng văn bản cho Bên kia. Việc chấm dứt Hiệp định sẽ có hiệu lực 6 tháng sau ngày nhận được thông báo. Mặc dù chấm dứt Hiệp định này, mọi tin mật đã

được tạo ra hoặc chuyển giao theo Hiệp định này sẽ tiếp tục được bảo vệ phù hợp với quy định của các điều Khoản của Hiệp định cho đến khi Bên chuyển giao miễn trừ trách nhiệm đó cho Bên nhận.

4. Mọi bất đồng liên quan đến việc giải thích hay áp dụng Hiệp định này sẽ được giải quyết một cách thân thiện thông qua tham vấn giữa các Bên mà không nhờ đến sự phán xử của Bên ngoài.

Làm tại Madrid, ngày 27 tháng 3 năm 2019 thành hai bản gốc, mỗi bản bằng tiếng Việt, tiếng Tây Ban Nha và tiếng Anh, các văn bản đều có giá trị như nhau. Trong trường hợp có sự giải thích khác nhau, bản tiếng Anh sẽ được dùng làm cơ sở.

**THAY MẶT**
**VƯƠNG QUỐC TÂY BAN NHA**

FÉLIX SANZ ROLDÁN
Quốc vụ khanh
Giám đốc Cơ quan Tình báo Quốc gia

**THAY MẶT**
**NƯỚC CỘNG HÒA XHCN VIỆT NAM**

BÙI VĂN NAM
Thứ trưởng Bộ Công an

[TRANSLATION – TRADUCTION]

# ACCORD ENTRE LE ROYAUME D'ESPAGNE ET LA RÉPUBLIQUE SOCIALISTE DU VIET NAM CONCERNANT L'ÉCHANGE ET LA PROTECTION RÉCIPROQUES D'INFORMATIONS CLASSIFIÉES LE ROYAUME D'ESPAGNE ET LA RÉPUBLIQUE SOCIALISTE DU VIET NAM (CI-APRÈS DÉNOMMÉS LES « PARTIES »),

Étant convenus d'élargir leur coopération politique, militaire et économique et de mener des discussions sur des questions de politique et de sécurité,

Conscients des évolutions de la situation politique dans le monde et reconnaissant le rôle important de leur coopération mutuelle pour la paix, la stabilité, ainsi que la sécurité nationale et internationale,

Conscients qu'une coopération de qualité peut nécessiter l'échange d'informations classifiées entre les Parties,

Désireux d'élaborer un ensemble de directives réglementant la protection mutuelle des informations classifiées, applicables à tous futurs accords de coopération et contrats classifiés qui seront mis en œuvre entre les Parties, et qui comportent ou font intervenir des informations classifiées,

Sont convenus de ce qui suit :

## *Article premier. Définitions*

Aux fins du présent Accord :

1. Le terme « informations classifiées » désigne toute information, quels qu'en soient la forme, la nature ou le mode de transmission, existante ou en cours d'élaboration, à laquelle a été attribué un niveau de classification de sécurité et qui, dans l'intérêt de la sécurité nationale et conformément aux lois et règlements nationaux des Parties, requièrent une protection contre les accès non autorisés ou la destruction ;

2. Le terme « accès non autorisé à des informations classifiées » désigne l'accès par une personne physique ou morale à des informations classifiées sans l'accord de l'autorité compétente, conformément aux lois et règlements nationaux de chaque Partie et aux dispositions du présent Accord ;

3. Le terme « niveau de classification de sécurité » désigne la catégorie attribuée à des informations classifiées, qui renseigne leur niveau de sensibilité, l'ampleur des dommages qui pourraient survenir en cas de divulgation non autorisée ou de perte et le niveau de protection que les Parties doivent leur consacrer ;

4. Le terme « marque de classification » désigne une marque qui indique le niveau de classification des informations classifiées ;

5. Le terme « habilitation de sécurité » désigne une décision favorable à la suite d'une procédure de vérification visant à vérifier la loyauté et de la fiabilité d'une personne physique ou morale ainsi que d'autres aspects de sécurité conformément aux lois et règlements nationaux. Ladite décision autorise la personne physique ou morale à avoir accès à des informations classifiées ainsi qu'à traiter ces informations jusqu'à un certain niveau ;

6. Le terme « Partie d'origine » désigne la Partie qui transmet des informations classifiées.

7. Le terme « Partie destinataire » désigne la Partie à laquelle des informations classifiées sont transmises.

8. Le terme « utilisateur » désigne toute personne physique ou morale qui prend part aux activités de coopération visées ou à la mise en œuvre de contrats classifiés pour lesquels le présent Accord s'applique ;

9. Le terme « autorité compétente » désigne l'autorité qui, conformément aux lois et règlements nationaux de la Partie concernée, est responsable en dernier ressort de la protection des informations classifiées, exerce un contrôle global dans ce domaine et assure et supervise la mise en application du présent Accord. Lesdites autorités sont énumérées à l'article 4 du présent Accord ;

10. Le terme « contractant » désigne toute personne physique ou morale possédant la capacité juridique de conclure des contrats en vertu des dispositions du présent Accord.

11. Le terme « contrat classifié » désigne un accord entre des utilisateurs des Parties, qui contient des informations classifiées, ou dont l'exécution nécessite la production d'informations classifiées ou l'accès à des informations classifiées de l'une ou l'autre des Parties ;

12. Le principe de « besoin d'en connaître » désigne la nécessité d'accéder à des informations classifiées aux fins de l'exercice de fonctions officielles ou pour l'exécution d'une mission officielle concrète ;

13. Le terme « partie tierce » désigne un État, une organisation internationale ou un utilisateur, qui n'est pas partie au présent Accord ;

14. Le terme « déclassification des informations » désigne le retrait du niveau de classification de sécurité ;

15. Le terme « incident de sécurité » désigne une action ou inaction contraire aux lois et règlements nationaux, qui entraîne ou peut entraîner l'accès non autorisé à des informations classifiées produites ou échangées au titre du présent Accord, ou encore leur divulgation, leur perte, leur destruction ou leur compromission.

*Article 2. Objectif*

Le présent Accord a pour objectif d'assurer la protection des informations classifiées échangées entre les Parties. Il définit les procédures et les dispositions de sécurité à suivre aux fins de ladite protection.

*Article 3. Niveaux de classification de sécurité*

1. Les Parties conviennent que les niveaux de classification de sécurité suivants sont équivalents et correspondent aux niveaux de classification de sécurité spécifiés dans leurs lois et règlements nationaux :

| Pour le Royaume d'Espagne | Pour la République socialiste du Viet Nam |
|---|---|
| SECRETO | TUYỆT MẬT |

| | |
|---|---|
| RESERVADO | TỐI MẬT |
| CONFIDENCIAL | MẬT |

2. Les informations transmises par le Royaume d'Espagne portant la marque de classification DIFUSIÓN LIMITADA bénéficient du même niveau de protection que celles portant la mention MẬT en République socialiste du Viet Nam.

*Article 4. Autorités compétentes*

1. Les autorités compétentes des Parties sont :

Pour le Royaume d'Espagne :

le Centre national du renseignement ;

Pour la République socialiste du Viet Nam :

le Ministère de la sécurité publique.

2. Les Parties s'informent mutuellement par la voie diplomatique de tout changement ultérieur concernant leurs autorités compétentes.

3. Les autorités compétentes s'informent mutuellement des lois et règlements nationaux en vigueur régissant la protection des informations classifiées.

4. Afin d'assurer une étroite collaboration dans la mise en œuvre du présent Accord, les autorités compétentes peuvent se concerter à la demande de l'une d'entre elles.

5. Afin d'atteindre et de maintenir des normes de sécurité comparables, les autorités compétentes de chaque Partie se communiquent mutuellement, sur demande, toute information relative aux normes, procédures et pratiques de sécurité appliquées pour protéger les informations classifiées.

6. Les autorités compétentes des Parties peuvent conclure des accords d'application concernant le présent Accord.

7. Les services de sécurité des Parties peuvent échanger et se renvoyer directement des informations opérationnelles ou des renseignements conformément aux lois et règlements nationaux.

*Article 5. Transmission d'informations classifiées*

1. Les informations classifiées portant une marque de classification de niveau égal ou supérieur à CONFIDENCIAL/MẬT sont généralement transmises par courrier diplomatique. Toutefois, d'autres canaux peuvent être utilisés s'ils sont mutuellement agréés par les autorités compétentes et conformes aux lois et règlements nationaux des Parties. La Partie destinataire confirme par écrit la réception d'informations classifiées portant une marque de classification de niveau égal ou supérieur à CONFIDENCIAL/MẬT.

2. Les informations classifiées transmises par la voie électronique sont protégées au moyen de méthodes de chiffrement mutuellement approuvées par les autorités compétentes et accompagnées d'un certificat dûment délivré conformément aux lois et règlements nationaux des Parties.

3. En cas de transmission de grandes quantités d'informations classifiées, les autorités compétentes conviennent mutuellement d'un plan de transport et l'approuvent. Ce dernier prévoit les moyens de transport, les exigences en matière d'escorte, l'itinéraire et les autres mesures de sécurité.

*Article 6. Mesures de protection des informations classifiées*

1. Conformément à leurs lois et règlements nationaux, les Parties mettent en œuvre toutes les mesures appropriées pour protéger les informations classifiées qui sont produites ou échangées dans le cadre du présent Accord. Lesdites informations classifiées sont protégées de la même manière que les informations classifiées nationales pourvues d'un niveau de classification de sécurité correspondant.

2. Les Parties s'informent mutuellement de toute modification de leurs lois et règlements nationaux respectifs régissant la protection des informations classifiées. En cas d'une telle modification, les Parties se préviennent mutuellement, conformément aux paragraphes 4 et 5 de l'article 4, afin de discuter d'éventuelles modifications à apporter au présent Accord. Entre temps, les informations classifiées sont protégées conformément aux dispositions du présent Accord, sauf accord écrit contraire.

3. Nul n'est autorisé à accéder aux informations classifiées du seul fait de son rang, de sa situation officielle ou d'une habilitation de sécurité antérieure. L'accès aux informations classifiées n'est accordé qu'aux personnes physiques ayant obtenu une habilitation de sécurité et conformément au principe du « besoin d'en connaître ».

4. La Partie destinataire est tenue :

a) de ne pas divulguer d'informations classifiées à un partie tierce sans l'accord préalable écrit de l'autorité compétente de la Partie d'origine ;

b) d'attribuer aux informations classifiées un niveau de classification de sécurité équivalent à celui attribué par la Partie d'origine ;

c) de ne pas utiliser les informations classifiées à des fins autres que celles pour lesquelles elles ont été fournies ;

d) d'assurer la protection des informations classifiées conformément aux modalités de protection prévues par les lois et règlements nationaux respectifs des Parties, sauf demande écrite contraire de la Partie d'origine.

Article 7. Traduction, reproduction et destruction des informations classifiées

1. Les documents classifiés portant une marque de classification de niveau SECRETO/TUYỆT MẬT ne peuvent être reproduits qu'avec l'accord écrit de l'autorité compétente de la Partie d'origine.

2. Toute traduction et reproduction d'informations classifiées est limitée au nombre d'exemplaires minimal requis pour un usage officiel et n'est réalisée que par des personnes ayant « besoin d'en connaître » et possédant l'habilitation de sécurité appropriée. Lesdites traductions et reproductions portent une marque de classification de sécurité équivalente à celle de la Partie d'origine et sont placées sous la même protection que les informations originales.

3. Les traductions comportent une annotation appropriée, dans la langue cible, indiquant qu'elles contiennent des informations classifiées de l'autre Partie.

4. Les informations classifiées sont détruites ou modifiées de façon à empêcher leur reconstruction totale ou partielle.

5. La Partie d'origine peut interdire expressément la reproduction, l'altération ou la destruction d'informations classifiées en apposant une marque sur leur support ou en envoyant une notification écrite ultérieure. S'il est interdit de détruire des informations classifiées, celles-ci sont restituées à l'autorité compétente de la Partie d'origine.

6. Les informations classifiées portant une marque de classification de sécurité de niveau SECRETO/TUYỆT MẬT ne peuvent être détruites et doivent être restituées à l'autorité compétente de la Partie d'origine.

7. En cas de situation de force majeure rendant impossibles la protection et la restitution des informations classifiées produites ou transmises conformément au présent Accord, celles-ci sont détruites immédiatement. La Partie destinataire notifie par écrit à l'autorité compétente de la Partie d'origine la destruction des informations classifiées dans les meilleurs délais.

*Article 8. Contrats classifiés*

1. Les contrats classifiés sont conclus et exécutés conformément aux lois et règlements nationaux de chaque Partie. Sur demande, l'autorité compétente de chaque Partie indique si un contractant proposé a reçu une habilitation de sécurité nationale correspondant au niveau de classification de sécurité requis. Si le contractant proposé n'est pas titulaire d'une habilitation de sécurité, l'autorité compétente de chaque Partie peut demander à ce qu'il en reçoive une.

2. Une annexe de sécurité fera partie intégrante de chaque contrat ou sous-contrat classifié. Dans ladite annexe, le contractant de la Partie en possession d'informations classifiées précisera quelles informations classifiées seront communiquées à l'autre Partie et quel niveau de classification de sécurité correspondant leur a été attribué.

3. L'obligation qui incombe au contractant de protéger les informations classifiées concerne, dans tous les cas, au moins les éléments suivants :

a) la divulgation des informations classifiées uniquement à une personne ayant reçu au préalable une habilitation de sécurité pour accéder aux activités contractuelles concernées, ayant « besoin d'en connaître » et employée ou engagée en vue de l'exécution du contrat ;

b) les moyens à utiliser pour transmettre les informations classifiées ;

c) les procédures et mécanismes de communication des changements susceptibles de survenir relativement aux informations classifiées, soit du fait de modifications de leur niveau de classification de sécurité, soit parce que la protection n'est plus nécessaire ;

d) les procédures d'approbation des visites, de l'accès ou de l'inspection par le personnel d'une Partie des installations de l'autre Partie qui sont couvertes par le contrat ;

e) la notification en temps voulu à l'autorité compétente du contractant de tout accès non autorisé effectif ou présumé ou de toute tentative d'accès non autorisé à des informations classifiées du contrat ;

f) l'utilisation des informations classifiées dans le cadre du contrat uniquement aux fins liées à l'objet du contrat ;

g) le strict respect des procédures de destruction des informations classifiées ;

h) la divulgation d'informations classifiées relatives au contrat à toute partie tierce uniquement avec l'accord écrit de l'autorité compétente de la Partie d'origine.

*Article 9. Incident de sécurité*

1. Tout incident de sécurité réel ou présumé concernant des informations classifiées de l'autre Partie fait l'objet d'une enquête par la Partie dans laquelle l'incident se produit. Si nécessaire, l'autre Partie coopère à l'enquête.

2. Si un incident de sécurité se produit dans un pays tiers, l'autorité compétente de la Partie d'origine prend les mesures prévues au paragraphe 1, dans la mesure du possible.

3. Dans tous les cas, l'autorité compétente de la Partie dans laquelle l'incident de sécurité est survenu informe l'autre Partie des résultats de l'enquête, de l'étendue des dommages causés, des solutions de réparation et de toutes les mesures prises pour éviter qu'une telle situation se reproduise.

*Article 10. Visites*

1. Les visites nécessitant l'accès à des informations classifiées ne sont autorisées qu'avec l'accord préalable écrit de l'autorité compétente de la Partie d'accueil.

2. Les autorités compétentes conviennent des procédures de visite.

3. Toute demande de visite comporte au moins les renseignements suivants :

a) le nom, la date et le lieu de naissance, la nationalité et le numéro de passeport (carte d'identité) du visiteur ;

b) l'emploi et la fonction du visiteur, le cas échéant le nom de l'organisation qu'il ou elle représente, une description du contrat classifié auquel il ou elle est partie et l'objet de la visite ;

c) la confirmation et la date d'expiration de l'habilitation de sécurité du visiteur ;

d) l'objet, le programme de travail proposé et la date prévue de la visite.

Dans le cas de visites récurrentes, la durée totale de ces visites est indiquée ;

e) les noms des organisations et installations qui font l'objet des visites ;

f) le nom, l'adresse, les numéros de téléphone et de télécopieur (le cas échéant) et l'adresse électronique du point de contact de l'organisation ou de l'installation qui fait l'objet de la visite ;

g) le niveau de classification anticipé des informations classifiées qui seront abordées ou consultées.

4. Les autorités compétentes des Parties peuvent convenir d'établir des listes de personnes autorisées à effectuer des visites régulières. Lesdites listes sont valables pour une période initiale de douze mois. Une fois les listes approuvées par les autorités compétentes des Parties, les conditions des visites spécifiques sont fixées directement avec les autorités compétentes de

l'organisation ou de l'installation faisant l'objet des visites, conformément aux clauses et conditions convenues.

5. Chaque Partie garantit la protection des données à caractère personnel des visiteurs conformément aux lois et règlements nationaux.

6. Chaque Partie est en droit d'exclure certaines personnes de la liste des visiteurs.

*Article 11. Frais*

En cas de frais, chaque Partie prend à sa charge les dépenses engagées aux fins de la mise en œuvre de ses obligations au titre du présent Accord.

*Article 12. Dispositions finales*

1. Le présent Accord est conclu pour une durée indéterminée et entre en vigueur à la date de réception de la dernière notification écrite par laquelle les Parties s'informent mutuellement de l'accomplissement de toutes les procédures juridiques internes nécessaires à cette fin.

2. Le présent Accord peut être modifié sur la base d'un consentement mutuel écrit des deux Parties. Les modifications entrent en vigueur conformément aux modalités énoncées au paragraphe 1 du présent article.

3. Chaque Partie peut dénoncer le présent Accord par une notification écrite adressée à l'autre Partie. La dénonciation entre en vigueur six mois après la date de réception de la notification. Nonobstant la dénonciation du présent Accord, toutes les informations classifiées produites ou transmises en vertu de celui-ci continuent d'être protégées conformément à ses dispositions, et ce, jusqu'à ce que la Partie d'origine dispense la Partie destinataire de cette obligation.

4. Tout différend résultant de l'interprétation ou de l'application du présent Accord est réglé à l'amiable par voie de consultation entre les Parties sans recours à une compétence extérieure.

FAIT à Madrid le 27 mars 2019 en deux exemplaires originaux, chacun en langues espagnole, vietnamienne et anglaise, tous les textes faisant également foi. En cas de divergence d'interprétation, le texte anglais prévaut.

Pour le Royaume d'Espagne :

FÉLIX SANZ ROLDÁN

Secrétaire d'État

Directeur du Centre national du renseignement

Pour la République socialiste du Viet Nam :

BUI VAN NAM

Vice-Ministre de la sécurité publique