

AGREEMENT
BETWEEN
THE CZECH REPUBLIC
AND
THE KINGDOM OF SPAIN
ON THE EXCHANGE
AND MUTUAL PROTECTION
OF CLASSIFIED INFORMATION

The Czech Republic and the Kingdom of Spain (hereafter referred to as "the Parties"), wishing to ensure the protection of Classified Information exchanged between them, have agreed in the interests of their national security on the following:

ARTICLE 1 DEFINITIONS

For the purpose of this Agreement the following terms are defined:

- a) **"Classified Information"** means any information or material that, under national laws and regulations of either Party, requires protection against unauthorised disclosure, misappropriation or loss, and has been designated as such and appropriately marked, regardless of its form.
- b) **"Classified Contract"** means an agreement that contains or involves access to Classified Information.
- c) **"Originating Party"** means the Party, which releases Classified Information to the other Party.
- d) **"Recipient Party"** means the Party, which receives Classified Information from the Originating Party.
- e) **"Third Party"** means any state or international organisation that is not a party to this Agreement.

ARTICLE 2 SECURITY CLASSIFICATIONS AND EQUIVALENCE

The security classifications markings and their equivalents are as follows:

In the Czech Republic	In the Kingdom of Spain
PŘÍSNĚ TAJNÉ	SECRETO
TAJNÉ	RESERVADO
DŮVĚRNÉ	CONFIDENCIAL
VYHRAZENÉ	DIFUSIÓN LIMITADA

**ARTICLE 3
SECURITY AUTHORITIES**

1. The Security Authorities responsible for the implementation of this Agreement are:

In the Czech Republic:

Národní bezpečnostní úřad

In the Kingdom of Spain:

**Secretario de Estado Director del Centro Nacional de Inteligencia
(CNI)**

Oficina Nacional de Seguridad

2. The Security Authorities shall provide each other with their official contact details.

**ARTICLE 4
ACCESS TO CLASSIFIED INFORMATION**

Access to Classified Information released under this Agreement shall be limited only to individuals duly authorised in accordance with the national laws and regulations of the respective Party.

**ARTICLE 5
RESTRICTIONS ON USE OF CLASSIFIED INFORMATION**

1. The Recipient Party shall not release or disclose the received Classified Information to a Third Party without the prior written authorisation of the Security Authority of the Originating Party.
2. The Recipient Party shall use received Classified Information only for the purpose it has been released for and within the limitations stated by the Originating Party.

**ARTICLE 6
PROTECTION OF CLASSIFIED INFORMATION**

1. The Originating Party shall:
 - a) ensure that Classified Information is marked with an appropriate security classification markings in accordance with national laws and regulations;
 - b) inform the Recipient Party that information or material released is Classified Information and requires protection under this Agreement;
 - c) inform the Recipient Party of any conditions of release and limitations on its use;

d) inform the Recipient Party of any subsequent changes in classifications.

2. The Recipient Party shall:

- a) in accordance with its national laws and regulations afford the equivalent level of protection to Classified Information as afforded by the Originating Party;
- b) ensure that received Classified Information is marked with equivalent security classification markings in accordance with Article 2 of this Agreement;
- c) ensure that classifications are not altered, except if authorised in writing by the Originating Party.

ARTICLE 7 SECURITY CO-OPERATION

- 1. The Security Authorities may conduct reciprocal visits in order to check security arrangements applied for the protection of released Classified Information and shall, on request, inform each other about their security standards, procedures and practices for the protection of Classified Information.
- 2. Subject to procedural requirements laid down in national laws and regulations, the Parties shall mutually recognise their respective Personnel and Facility Security Clearances. The Article 2 of this Agreement shall apply accordingly.
- 3. The Security Authorities shall promptly notify each other about any changes in mutually recognised Personnel and Facility Security Clearances.
- 4. On request, the Security Authorities shall notify each other about the security status of facilities residing in the territory of the other Party and individuals participating in pre-contractual negotiations or Classified Contracts.
- 5. On request, the Security Authorities shall, within the scope of their respective national laws and regulations, assist each other during the Personnel and Facility Security Clearance procedures.
- 6. The Security Authorities shall inform each other about current security risks that may endanger released Classified Information.
- 7. The co-operation under this Agreement shall be effected in English language.

**ARTICLE 8
CLASSIFIED CONTRACTS**

1. The Party wishing to place a Classified Contract with a contractor of the other Party shall obtain upon request a prior written assurance from the Security Authority of the other Party that the proposed contractor holds a Facility Security Clearance of an appropriate level.
2. Every Classified Contract concluded between the Parties, under the provisions of this Agreement, shall include an appropriate security section identifying the following aspects:
 - a) Classification guide and list of Classified Information;
 - b) Procedure for the communication of changes in the security classifications;
 - c) Communication channels and means for electromagnetic transmission;
 - d) Procedure for the transmission of Classified Information;
 - e) Relevant authorities responsible for the co-ordination of the protection of Classified Information related to the Classified Contract;
 - f) An obligation to notify any actual or suspected unauthorised disclosure, misappropriation or loss of Classified Information.
3. Any subcontractor shall fulfil the same security obligations as the contractor.
4. A copy of the security section of Classified Contract shall be forwarded to the Security Authority of the Party where the Classified Contract is to be performed to allow adequate security control.

**ARTICLE 9
TRANSMISSION OF CLASSIFIED INFORMATION**

1. Unless otherwise agreed by the Security Authorities, Classified Information shall be transmitted through diplomatic channels.
2. If required by the Originating Party, transmissions may be undertaken by couriers duly authorised in accordance with its national laws and regulations and furnished with a courier certificate issued by the respective Security Authority.
3. Delivery of large items or quantities of Classified Information arranged on case-by-case basis shall be approved by the Security Authorities.
4. The Parties may transmit Classified Information by electronic means in accordance with security procedures approved by the Security Authorities.

ARTICLE 10
TRANSLATION, REPRODUCTION AND DESTRUCTION

1. Translations and reproductions of Classified Information shall be made in accordance with the following rules:
 - a) The translations and the reproductions shall be marked and afforded the same protection as the original Classified Information;
 - b) The translations and the number of reproductions shall be limited to that required for official purposes;
 - c) The translations shall bear an appropriate note in the language of translation indicating that it contains Classified Information received from the Originating Party.
2. Classified Information marked as PŘÍSNĚ TAJNÉ/SECRETO shall be translated or reproduced only upon the written permission of the Security Authority of the Originating Party.
3. Classified Information marked as PŘÍSNĚ TAJNÉ/SECRETO shall not be destroyed and shall be returned to the Security Authority of the Originating Party.
4. Classified Information marked as TAJNÉ/RESERVADO shall be destroyed with prior written approval of the Originating Party.
5. Classified Information marked up to DŮVĚRNÉ/CONFIDENCIAL shall be destroyed in accordance with national laws and regulations of the Recipient Party.

ARTICLE 11
VISITS

1. Visits entailing access to Classified Information are subject to prior written authorisation given by the respective Security Authority.
2. Request for Visit shall be submitted through Security Authorities at least twenty (20) days before visit and shall include:
 - a) First and last name of the visitor, date and place of birth, nationality and passport/ID card number;
 - b) Official position of the visitor and specification of the facility, which the visitor represents;
 - c) Level of the Personnel Security Clearance of the visitor and date of expiry of the Personnel Security Clearance;

- d) Date and duration of the visit, in case of recurring visit the total period of time covered by the visits shall be stated;
 - e) Purpose of the visit including the highest level of Classified Information to be involved;
 - f) Name, address, phone/fax number, e-mail address and point of contact of the facility to be visited;
 - g) Date, signature and stamping of the official seal of the Security Authority.
3. In urgent cases, the Request for Visit may be submitted at least five (5) working days before the date of the visit.
 4. The Request for Visit shall be approved for a period of time not exceeding twelve (12) months. When it is expected that a particular visit shall exceed twelve (12) months, a new Request for Visit shall be submitted.
 5. Any Classified Information acquired by a visitor shall be considered as Classified Information released under this Agreement.

ARTICLE 12 BREACHES OF SECURITY

1. In the event of a breach of security resulting in loss, misappropriation or unauthorised disclosure of Classified Information released under this Agreement, or suspicion of such a breach, the Security Authority of the Recipient Party shall immediately inform the Security Authority of the Originating Party in writing. The Originating Party shall, if required, co-operate in the investigation.
2. In any case, the Recipient Party shall inform the Originating Party in writing about the circumstances of the breach of security, the extent of the damage, the measures adopted for its mitigation and the outcome of the investigation.

ARTICLE 13 EXPENSES

Each of the Parties shall bear its own expenses incurred in the course of the implementation of this Agreement.

ARTICLE 14 INTERPRETATION AND DISPUTES

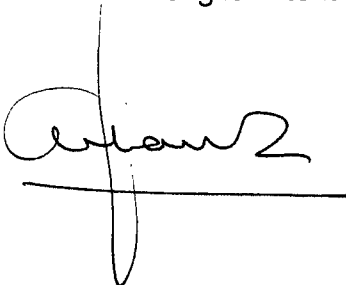
Any dispute regarding the interpretation or application of this Agreement shall be settled by negotiation between the Parties.

**ARTICLE 15
FINAL PROVISIONS**

1. This Agreement is concluded for an indefinite period of time. This Agreement shall enter into force on the first day of the second month following the date of receipt of the last of notifications between the Parties, through diplomatic channels, that the internal legal procedures for this Agreement to enter into force have been fulfilled. All Classified Information exchanged before this Agreement enters into force shall be protected in compliance with its provisions.
2. This Agreement may be amended on the basis of the mutual consent of the Parties. Such amendments shall enter into force in accordance with paragraph 1 of this Article.
3. Each of the Parties is entitled to denounce this Agreement in writing. In such case, the validity of this Agreement shall expire after six (6) months following the day on which the other Party receives the written notice of the denunciation.
4. Regardless of the denounce of this Agreement, all Classified Information released or generated pursuant to this Agreement shall be protected in accordance with the provisions set forth herein until the Originating Party dispenses the Recipient Party from this obligation.

Done in *Madrid*..... on *8 October 2009*..... in two originals, each one in the Czech, Spanish and English language, all texts being equally authentic. In case of different interpretation the English text of this Agreement shall prevail.


For the Czech Republic


For the Kingdom of Spain