

**AGREEMENT**  
**BETWEEN**  
**THE GOVERNMENT OF THE CZECH REPUBLIC**  
**AND**  
**THE CABINET OF MINISTERS OF UKRAINE**  
**ON**  
**PROTECTION OF CLASSIFIED INFORMATION**

**The Government of the Czech Republic**

**and**

**the Cabinet of Ministers of Ukraine,**

Hereafter referred to as "the Parties"

With the intention of ensuring the protection of classified information exchanged between the Parties within the context of collaboration agreements concluded, or of agreements which will be concluded within the context of tendering procedures, contracts or orders of either public or private subjects of the states of the Parties,

confirming that this Agreement shall not affect the commitments of both Parties which stem from other international agreements and that it shall not be used against the interests, security and territorial integrity of other states,

Have agreed on the following:

**ARTICLE 1  
DEFINITIONS**

For the purpose of this Agreement,

(1) **Classified information** means:

Information and material, regardless of their form, nature and manner of transmission, which has been assigned a certain level of classification and marked accordingly, and which in the interest of national security and in accordance with the national legal regulations of the states of the Parties requires protection against unauthorised access.

(2) The **classified contract** means:

A legal relationship between two or more contracting entities defining mutually enforceable rights and responsibilities, which involves classified information.

(3) The **contracting entity** means:

A natural person or legal entity legally capable of concluding contracts.

(4) The **host Party** means:

A Party receiving a visit on the territory of its state.

(5) The **releasing Party** means:

A Party releasing or delivering classified information to the other Party.

(6) The **receiving Party** means:

A Party to which classified information is released or delivered by the releasing Party.

(7) The **user** means:

A natural person or legal entity that, in accordance with the national legal regulations, has been authorised to use classified information.

(8) The **third party** means:

The states, the Governments of which are not the Parties to this Agreement, their bodies, enterprises, establishments, organizations and their citizens as well as persons without citizenship or international organizations.

(9) The **Security Clearance** means:

a positive determination stemming from an investigative procedure that shall ascertain loyalty and trustworthiness of a person or entity as well as other security aspects in accordance with the national legal regulations. Such determination enables to grant the person or entity access and allow them to handle classified information on a certain level without security risk.

## ARTICLE 2 COMPETENT SECURITY AUTHORITIES

The competent Security Authorities responsible for implementation of this Agreement are:

in the Czech Republic:  
Národní bezpečnostní úřad,

in Ukraine:  
Служба безпеки України

## ARTICLE 3 PRINCIPLES OF SECURITY

- (1) The Parties shall adopt, in compliance with their respective national legal regulations, all measures necessary in order to ensure the appropriate protection of classified information received on the basis of this Agreement, and on the basis of other agreements between the Parties, or contracts or sub-contracts concluded between the Parties or between entities authorised for that purpose.
- (2) The protection and use of classified information exchanged between the Parties shall be executed in compliance with the below stated principles:
  - a) The receiving Party shall ensure that received classified information is marked with an equivalent level of classification, in accordance with Article 4;
  - b) Access to classified information shall be granted only to individuals whose functions require it, on the basis of a "need to know" principle, and who have been, in accordance with the national legal regulations, granted a security clearance certificate of the appropriate level in advance;

- c) The Parties shall mutually recognise Security Clearance Certificates issued to users;
- d) The competent Security Authorities of the states of the Parties shall inform each other without unnecessary delay of changes in the users' Security Clearance Certificates, especially in cases when the Certificate was withdrawn or downgraded;
- e) The receiving Party shall not hand over classified information to a third party without the prior written consent of the releasing Party;
- f) Released classified information shall not be used for purposes other than those that are presumed in the agreements concluded between the Parties, in the contracts or subcontracts concluded between the Parties or by entities authorised to this aim, without the prior written consent of the releasing Party;
- g) The receiving Party shall not decrease or cancel the level of classification of received classified information without the prior written consent of the releasing Party.

**ARTICLE 4  
DEGREES OF CLASSIFICATION AND THEIR EQUIVALENCY**

- (1) The Parties shall, with regard to their national legal regulations, adopt the following equivalency for the national degrees of classification:

<b>Czech Republic:</b>	<b>Ukraine:</b>	<b>English equivalent:</b>
PRÍSNE TAJNÉ	ОСОБЛИВОЇ ВАЖЛИВОСТІ	TOP SECRET
TAJNÉ	ЦІЛКОМ ТАЄМНО	SECRET
DŮVĚRNÉ	ТАЄМНО	CONFIDENTIAL
VYHRAZENÉ	ДЛЯ СЛУЖБОВОГО КОРИСТУВАННЯ	RESTRICTED

**ARTICLE 5  
SECURITY MEASURES**

- (1) Before the delivery of classified information released by one of the Parties to users of the state of the other Party, the receiving Party shall:
- a) Ascertain that within entities of the state of the receiving Party the protection of classified information is ensured in an appropriate manner;
  - b) Issue to these entities a Security Clearance Certificate of the required level, in the case that these entities fulfil the conditions for such issue compliant with national legal regulations;

- c) Issue a Security Clearance Certificate of the required level to individuals who need access to classified information in the exercise of their official duties, in the case that these individuals fulfil the conditions for such issue compliant with national legal regulations;
  - d) Ensure that all persons that will have access to received classified information have been appropriately briefed on security procedures and their security obligations. All such persons shall acknowledge in writing that they fully understand their responsibilities and the consequences which the legal regulations of their nation provide when classified information passes into unauthorised hands either by intent or through negligence.
- (2) During contract negotiations on classified contracts or sub-contracts between a user from the state of one Party and a user from the state of the other Party, the competent Security Authority of the state of the releasing Party shall inform its counterpart of the level of classified information connected with these negotiations.
- (3) A security annex shall be an integral part of each classified contract or sub-contract. In this annex, the competent Security Authority of the state of the releasing Party shall specify which classified information will be released to the receiving Party, and which corresponding level of classification has been assigned to this information. Only the releasing Party may change the level of classification stated in the security annex. The competent Security Authority of the state of the releasing Party shall hand over a copy of the security annex to the competent Security Authority of the state of the receiving Party.
- (4) The measures in place for the protection of classified information as well as the procedure for assessment of and indemnification for losses caused to the contracting entity by unauthorised disclosure of classified information should be specified in more detail in the respective classified contract
- (5) The Parties shall ensure the execution of regular security inspections of entities that handle classified information received from the other Party.

#### **ARTICLE 6**

#### **MARKING OF CLASSIFIED INFORMATION**

- (1) When classified information is received, the receiving Party shall ensure that it is marked with the national level of classification in accordance with Article 4.
- (2) The receiving Party shall provide the same marking of classification for copies and translations as for the original documents, and shall ensure the same protection.
- (3) The competent Security Authorities of the states of the Parties shall promptly inform one another of all changes in the level of classification of released classified information.

**ARTICLE 7**  
**TRANSMISSION OF CLASSIFIED INFORMATION**

- (1) Classified information shall be transmitted between the Parties by diplomatic means. The competent Security Authority of the state of the receiving Party shall confirm in writing the receipt of classified information and further disseminate the received classified information to users.
- (2) In specific cases and after mutual consent, the competent Security Authorities may define other means of transmission of classified information.
- (3) The electromagnetic transmission of classified information shall be carried out only in encrypted form approved by the competent Security Authorities.

**ARTICLE 8**  
**VISITS**

- (1) Visits by nationals of the state of one Party to facilities or premises wherein classified information is used, and which are located in the territory of the state of the other Party, shall be approved on the condition that the competent Security Authority of the state of the host Party approves such a visit in advance and in writing. Visits by persons of a third party that would enable access to classified information of the states of the Parties, or access to places where such information is in use, shall be allowed only after provision of mutual written consent of the competent Security Authorities of both states.
- (2) Requests for visit permission shall usually be delivered through diplomatic channels to the competent Security Authority of the state of the host Party. These requests must be delivered at least three weeks before the requested visit takes place.
- (3) A request for visit permission must contain the following data:
  - a) The visitor's name and surname, date and place of birth, citizenship and passport number,
  - b) The title and work position of the visitor and the name of the entity which the visitor represents,
  - c) The level of Security Clearance of the visitor documented by a copy of Security Clearance Certificate issued by the competent Security Authority of the state of the requesting Party,
  - d) The proposed date and anticipated length of the visit,
  - e) The purpose of the visit, the type and level of classified information to which the visitor shall have access,
  - f) The names of the visited entities, premises and places,

- g) If possible, the names and surnames of the persons who will receive the visitor,
- (h) The date, signature and official stamp of the competent Security Authority of the state of the requesting Party.
- (4) On behalf of their nationals, the competent Security Authorities of the states of the Parties may request visit permission lasting no longer than 12 months. If it is assumed that a certain visit will not end within the time span allowed, or if it is necessary to extend the span of regular visits, the competent Security Authority of the state of the Party making the request must submit a new request no later than three weeks before the expiry of the validity of the permission for the visit under way.
- (5) All visitors must conform to the security regulations in force within the territory of the state of the host Party.
- (6) For each project, programme or contract, the competent Security Authorities of the states of the Parties may agree on the compilation of a list of persons who are allowed repeated visits in accordance with the principles and conditions on which the competent Security Authorities of the states of the Parties have agreed. These lists are initially valid for a period of twelve months, and may be extended after agreement between the competent Security Authorities of the states of the Parties for a further period of twelve months at most.
- (7) The lists referred to in the paragraph (6) of this Article shall be approved by the competent Security Authority of the state of the host Party. As soon as the competent Security Authorities of the states of the Parties approve the lists, the details of individual visits may be negotiated directly with the entities that the persons on the list are to visit.

#### **ARTICLE 9 BREACH OF SECURITY REGULATIONS**

- (1) In the case that a breach of national legal regulations on protection of classified information is not ruled out, or if it is considered to have taken place or ascertained, and in the case where such breach may have an impact on the protection of classified information delivered under this Agreement, this fact must be promptly announced in writing by the competent Security Authority of the state of the receiving Party to the competent Security Authority of the state of the releasing Party.
- (2) Each case of the breach of national legal regulations on protection of classified information as described in paragraph (1) of this Article must be subjected to an investigation and appropriate measures must be taken in accordance with the national legal regulations of the state of the receiving Party. The competent

Security Authority of the state of the releasing Party must be informed of the results of such investigation.

#### **ARTICLE 10 COSTS**

Expenditures incurred to a Party by the implementation of this Agreement are not covered by the other Party.

#### **ARTICLE 11 CONSULTATION AND INSPECTIONS**

(1) In order to ensure close collaboration while implementing this Agreement, the competent Security Authorities of the states of the Parties shall grant one another consultations on request.

(2) In order to maintain comparable security standards, each Party shall provide to the other Party relevant national legal regulations as well as their amendments. On request, procedures and national practice in the field of protection of classified information will be provided as well.

(3) Each Party shall allow the competent Security Authority of the state of the other Party to inspect conditions under which received classified information is kept and used.

#### **ARTICLE 12 FINAL PROVISIONS**

(1) This Agreement is concluded for an indefinite period of time.

(2) This Agreement shall enter into force on the first day of the second month after receipt of the last written notifications between the Parties confirming fulfillment of national procedures that are necessary for its entering into force.

(3) Each Party may in any time submit a written proposal to amend this Agreement. If approved by both Parties, the amendments to this Agreement shall become an integral part of the Agreement and shall enter into force in accordance with the procedure laid down in paragraph (2) of this Article.

(4) Any disagreement in the interpretation or implementation of the provisions of this Agreement shall be resolved through consultations between authorised representatives of the states of the Parties.

(5) Each Party may terminate this Agreement at any time with six months' written notice. In the case of termination of the Agreement, the exchanged or created

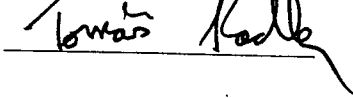


classified information shall continue to be handled in compliance with this Agreement.

Done in Prague ..... on 14th May 2003

in two originals, each in Czech, Ukrainian and English languages, all texts being equally authentic. In the case of different interpretation of the provisions of this Agreement, the English version shall prevail.

On behalf of the Government  
of the Czech Republic

  
\_\_\_\_\_

On behalf of the Cabinet of Ministers  
of Ukraine

