

**AGREEMENT**  
**BETWEEN**  
**THE GOVERNMENT OF THE REPUBLIC OF ESTONIA**  
**AND**  
**THE GOVERNMENT OF THE REPUBLIC OF CYPRUS**  
**ON MUTUAL PROTECTION OF CLASSIFIED**  
**INFORMATION**

The Government of the Republic of Estonia and the Government of the Republic of Cyprus (hereinafter referred to as “the Parties”),

Recognizing the need to set rules on protection of Classified Information mutually exchanged within the scope of political, military, economical, legal, scientific and technological or any other cooperation, as well as Classified Information generated in the process of such cooperation,

Intending to ensure the mutual protection of all Classified Information, which has been classified by one Party and transferred to the other Party or commonly generated in the course of co-operation between the Parties,

Desiring to create a set of rules on the mutual protection of Classified Information exchanged between the Parties,

Considering the mutual interests in the protection of Classified Information, in accordance with the legislation of the Parties,

Have agreed as follows:

## **Article 1**

### **Objective**

The objective of this Agreement is to ensure the protection of Classified Information that is commonly generated or exchanged between the Parties.

## **Article 2**

### **Definitions**

For the purposes of this Agreement:

- a) **“Breach of Security”** means an act or an omission which is contrary to this Agreement or the national legislation of the Parties, the result of which may lead to disclosure, loss, destruction, misappropriation or any other type of compromise of Classified Information;
- b) **“Classified Contract”** means an agreement between two or more Contractors, which contains or the implementation of which requires access to Classified Information;
- c) **“Classified Information”** means any information, irrespective of its form or nature, which requires protection against unauthorised manipulation and has been classified in accordance with the national legislation of the Parties and has been so designated by a security classification level;
- d) **“Competent Authority”** means National Security Authority and any other competent entity which, according to the national legislation of the Parties, is responsible for the implementation of this Agreement;
- e) **“Contractor”** means an individual or a legal entity possessing the legal capacity to conclude Classified Contracts;
- f) **“Facility Security Clearance”** means the determination by the Competent Authority confirming, that the legal entity or an individual has the physical and organizational capability to handle and store Classified Information in accordance with the respective national legislation;

- g) “**National Security Authority**” means the state authority of each Party, which in accordance with its national legislation is responsible for the general implementation and supervision of this Agreement; the respective authorities of the Parties are referred to in Article 4 Paragraph 1 of this Agreement;
- h) “**Need-to-know**” means the necessity to have access to specific Classified Information in the scope of a given official position and for the performance of a specific task;
- i) “**Originating Party**” means the Party which has created Classified Information;
- j) “**Personnel Security Clearance**” means the determination by the Competent Authority confirming, in accordance with the respective national legislation, that the individual is eligible to have access to Classified Information;
- k) “**Receiving Party**” means the Party to which Classified Information of the Originating Party is transmitted;
- l) “**Third Party**” means any state, organization, legal entity or individual, which is not a party to this Agreement.

### **Article 3**

#### **Security Classification Levels**

The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in their national legislation:

For the Republic of Estonia	For the Republic of Cyprus	Equivalent in English
TÄIESTI SALAJANE	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ	TOP SECRET
SALAJANE	ΑΠΟΡΡΗΤΟ	SECRET
KONFIDENTSIAALNE	ΕΜΠΙΣΤΕΥΤΙΚΟ	CONFIDENTIAL
PIIRATUD	ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΧΡΗΣΗΣ	RESTRICTED

**Article 4**  
**Competent Authorities**

1. The National Security Authorities of the Parties are:

**For the Government of the Republic of Estonia:**

Department of the National Security Authority  
Ministry of Defence of the Republic of Estonia

**For the Republic of Cyprus:**

National Security Authority  
Ministry of Defence of the Republic of Cyprus

2. The Parties shall inform each other through diplomatic channels of any modification of the National Security Authorities.
3. Upon request the National Security Authorities shall notify each other about other Competent Authorities.
4. The National Security Authorities shall inform each other of respective national legislation on Classified Information and of any significant amendments thereto and shall exchange information about the security standards, procedures and practices for the protection of Classified Information.

**Article 5**  
**Protection Measures and Access to Classified Information**

1. In accordance with their national legislation, the Parties shall take all appropriate measures for the protection of Classified Information, which is exchanged or generated under this Agreement. At least the same level of protection shall be assigned to such Classified Information as is provided for the national Classified Information of the equivalent security classification level in accordance with Article 3.

2. The Originating Party shall inform the Receiving Party in writing about any change of the security classification level of the transmitted Classified Information.
3. Access to Classified Information shall be limited to persons on a Need-to-know basis who are authorised in accordance with the national legislation of the Parties to have access to Classified Information of the equivalent security classification level.
4. Within the scope of this Agreement, each Party shall recognise the Personnel Security Clearances and Facility Security Clearances granted in accordance with the national legislation of the other Party. The security clearances shall be equivalent in accordance with Article 3.
5. The Competent Authorities shall, in accordance with the national legislation, assist each other upon request at carrying out vetting procedures necessary for the application of this Agreement.
6. Within the scope of this Agreement, the Competent Authorities of the Parties shall inform each other without delay about any alteration with regard to Personnel and Facility Security Clearances, in particular about their withdrawal or downgrading.
7. The Receiving Party shall:
  - a) submit Classified Information to any Third Party only upon prior written consent of the Originating Party;
  - b) mark the received Classified Information in accordance with Article 3;
  - c) use Classified Information solely for the purposes it has been provided for.

## **Article 6**

### **Transmission of Classified Information**

1. Classified Information shall be transmitted through diplomatic channels unless otherwise approved by the National Security Authorities. The Receiving Party shall confirm the receipt of Classified Information in writing.

2. Electronic transmission of Classified Information shall be carried out through certified cryptographic means agreed by the National Security Authorities.
3. If necessary, the intelligence, security and police services of the Parties may, in accordance with national legislation, exchange operative and intelligence information directly with each other.

### **Article 7**

#### **Reproduction and Translation of Classified Information**

1. Translations and reproductions of Classified Information shall be made in accordance with the national legislation of the Receiving Party and the following procedures:
  - a) the translations and the reproductions shall be marked and protected as the original Classified Information;
  - b) the translations and the number of copies shall be limited to that required for official purposes;
  - c) the translations shall bear an appropriate note in the language of the translation indicating that it contains Classified Information received from the Originating Party.
2. Classified Information marked SALAJANE/ANIOPPHOTO or above shall be translated or reproduced only upon prior written consent of the Originating Party.

### **Article 8**

#### **Destruction of Classified Information**

1. Classified Information shall be destroyed in a manner that prevents its partial or total reconstruction.

2. Classified Information marked up to SALAJANE/ΑΠΟΡΡΗΤΟ shall be destroyed in accordance with the national legislation.
3. Classified Information marked TÄIESTI SALAJANE/ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ shall not be destroyed. It shall be returned to Competent Authority of the Originating Party.
4. A report on destruction of Classified Information shall be made and its translation in English shall be delivered to the Competent Authority of the Originating Party.
5. In case of a crisis situation in which it is impossible to protect or return Classified Information it shall be destroyed immediately. The Receiving Party shall inform the Competent Security Authority of the Originating Party about this destruction as soon as possible.

## **Article 9**

### **Classified Contracts**

1. The National Security Authority of a Party, wishing to place a Classified Contract with a Contractor of other Party, or wishing to authorise one of its own Contractors to place a Classified Contract in the territory of the other Party shall obtain prior written assurance from the National Security Authority of the other Party that the proposed Contractor is granted Facility Security Clearance of the appropriate security classification level.
2. The Contractor shall submit information about potential sub-contractors for approval to the National Security Authority, in whose territory the work is to be performed.
3. Each Classified Contract concluded in accordance with this Agreement shall include:
  - a) commitment of the Contractor to ensure that its premises have necessary conditions for handling and storing Classified Information of appropriate security classification level;

- b) commitment of the Contractor to ensure that persons who perform duties requiring access to Classified Information are authorised in accordance with the national legislation to have access to Classified Information of the equivalent security classification level;
  - c) requirement that the Contractor shall ensure that all persons with access to Classified Information are informed of their responsibility towards the protection of Classified Information in accordance with the national legislation;
  - d) list of Classified Information and list of areas in which Classified Information can arise;
  - e) procedure for communication of changes in the security classification level of Classified Information;
  - f) communication means and electronic means for transmission;
  - g) procedure for the transmission of Classified Information;
  - h) commitment of the Contractor to notify of any actual or suspected Breach of Security;
  - i) commitment of the Contractor to forward a copy of the Classified Contract to its own Competent Authority;
  - j) commitment of the subcontractor to fulfil the same security obligations as the Contractor.
4. As soon as pre-contractual negotiations begin between potential Contractors, the National Security Authority of the Originating Party shall inform the National Security Authority of the other Party of the security classification level given to the Classified Information related to those pre-contractual negotiations.
5. Copy of each Classified Contract shall be forwarded to the National Security Authority of the Party where the work is to be performed, to allow adequate security supervision and control.



## **Article 10**

### **Visits**

1. Visits related to Classified Contracts and involving access to Classified Information are subject to prior written approval given by the Competent Authority of the host Party.
2. The Competent Authority of the host Party shall receive a request for visit at least ten days in advance.
3. In urgent cases, the request for visit can be transmitted in shorter time.
4. The request for visit shall include:
  - a) visitor's name and surname, place and date of birth, citizenship, passport or identification document number;
  - b) name of the legal entity represented by the visitor and position of the visitor in the legal entity;
  - c) name, address and contact information of the legal entity to be visited;
  - d) confirmation of the visitor's Personnel Security Clearance, its validity and level;
  - e) object and purpose of the visit;
  - f) expected date and duration of the requested visit; in case of recurring visits the total period covered by the visits shall be stated;
  - g) the date, signature and the official seal of the Competent Authority.
5. Once the visit has been approved the Competent Authority of the host Party shall provide a copy of the request for visit to the security officers of the legal entity to be visited.
6. The validity of visit approval shall not exceed one year.

7. The Competent Authorities of the Parties may draw up lists of individuals authorised to make recurring visits. The lists are valid for an initial period of twelve months. The terms of the respective visits shall be directly arranged with the appropriate points of contact in the legal entity to be visited by these individuals, in accordance with the terms and conditions agreed upon.

## **Article 11**

### **Breach of Security**

1. In case of Breach of Security the National Security Authority of the Receiving Party shall inform the National Security Authority of the Originating Party, as soon as possible, and initiate the appropriate investigation.
2. If a Breach of Security arises in a third state, the National Security Authority of the dispatching Party shall take all necessary measures in order to ensure that the actions prescribed in Paragraph 1 are initiated.
3. The Originating Party shall, upon request, co-operate in the investigation in accordance with Paragraph 1.
4. The Originating Party shall be informed of the results of the investigation and shall receive the final report on the reasons and extent of the damage.

## **Article 12**

### **Expenses**

Each Party shall bear its own expenses incurred in the course of application and supervision of this Agreement.

## **Article 13**

### **Settlement of Disputes**

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

**Article 14**  
**Final Provisions**

1. This Agreement is concluded for an indefinite period of time and enters into force on the first day of the second month after the date of the receipt of the latest written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.
2. This Agreement may be amended any time on the basis of mutual written approval of the Parties. The amendments shall enter into force in accordance with Paragraph 1.
3. Each Party may, at any time, terminate this Agreement by written notification to the other Party, through diplomatic channels. In this case, the termination takes effect six months after the date of the receipt of the respective notification.
4. Notwithstanding the termination of this Agreement, the Parties shall ensure that all Classified Information shall continue to be protected until the Originating Party dispenses the Receiving Party from this obligation.

Done at Nicosia on 27 November 2012 in two original sets, each in the Estonian, Greek and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

**For the Government of  
the Republic of Estonia**

**For the Government of  
the Republic of Cyprus**

.....  
**Märt Kraft**  
**Director of the National Security  
Authority**

.....  
**Demetris Eliades**  
**Minister of Defence**