



**Republika e Kosovës**  
**Republika Kosova – Republic of Kosovo**  
*Qeveria – Vlada – Government*

---

**REGULATION (GRK) NO. 12/2024 ON THE PROTECTION OF  
CLASSIFIED INFORMATION IN THE INDUSTRIAL FIELD<sup>1</sup>**

---

<sup>1</sup> Regulation (GRK) No. 12/2024 on the Protection of Classified Information in the Industrial Field, was approved on the 203 meeting of the Government of Kosovo, with the Decision No. 03/203 dated 08.05.2024.

## **Government of the Republic of Kosovo,**

Pursuant to Article 93 (4) of the Constitution of the Republic of Kosovo, in accordance with Article 38 paragraph 5 of Law No. 08/L-175 on the Protection of Classified Information, and Article 8, paragraph 4, sub-paragraph 4.5 of Law No. 08/L-117 On the Government of the Republic of Kosovo, as well as Article 19, paragraph 6, sub-paragraph 6.2 of Rules of Procedure of the Government, Regulation No. 09/2011,

Approves:

### **REGULATION NO. 12/2024 ON THE PROTECTION OF CLASSIFIED INFORMATION IN THE INDUSTRIAL FIELD**

#### **Article 1 Purpose**

1. The purpose of this Regulation is to define the procedures for the protection of classified information in the industrial field.
2. This regulation is in harmony with EU legislation, as follows:
  - 2.1. Council Decision of 23 September 2013 on security rules for the protection of EU classified information.

#### **Article 2 Scope**

1. This Regulation applies only to cases of procurements in the field of defense and security which contain classified information, according to the applicable legislation.
2. The provided rules are applicable by the national authority for the security of classified information, the economic operators concerned, as well as any other state institution, which:
  - 2.1. It is included in a procurement in the field of defense and security that contains classified information, in the capacity of contracting authorities or even the beneficiary institution;
  - 2.2. Participates in carrying out security and financial sustainability verification procedures of interested economic operators.

#### **Article 3 Definitions**

1. Terms used in this Regulation shall have the following meaning:

1.1. "**Industrial Safety Questionnaire**", is the document that the economic operator completes, the set of requirements based on which is assessed if an economic operator meets the criteria to be provided with an Industrial Safety Certificate;

1.2. "**Briefing**"/"**Debriefing**"- are a set of security instructions and guidelines related to the procedures for providing classified information and the individual responsible for violations of security rules, to which individuals who seek to have access to classified information or are equipped with CPS and the CSI are subject;

1.3. "**Project security guide**" - the set of security rules and procedures, mandatory, to be implemented in the specific project of the classified contract;

1.4. "**Cargo security plan**" - the document approved by the contracting authority, which includes measures that guarantee the security of the transport of classified material;

1.5. "**Visits**" - which are carried out within the framework of obligations arising from international agreements, after a request from the competent authority of one party or on the basis of an invitation from the contracting authority;

1.6. "**Visitors**" - official representatives of a state or international organization, who, on the basis of official duties, request to visit the contractor's facilities;

1.7. "**Person**" - means a natural or legal person.

2. Other expressions used in this regulation have the same meaning as those used in the relevant Law on the Protection of Classified Information.

#### **Article 4 General Principles**

1. The economic operator interested in participating in a procurement in the field of defense and security, which contains information classified at the "SECRET" and "Confidential" level, must first be equipped with the required level of the Industrial Security Certificate (ISC).

2. In any procurement in the field of defense and security that contains information classified at the "SECRET" and "Confidential" level, the personnel representing the economic operator and other persons who will have access to the classified information must be equipped with the level the required Personnel Security Certificate (PSC), according to the requirements of the applicable legislation.

3. The engagement of consultants, auditors and various experts for the account and in the interest of the parties is possible in any procurement in the field of defense and security that contains classified information, only when each of them:

3.1. ensure the right to recognition by the head of the institution or the Contractor's Industrial Safety Officer due to the task they perform;

3.2. are previously informed / briefed on the recognition of classified information security procedures and individual responsibilities for security breaches and have signed the information security declaration;

3.3. respects the same security standards and requirements, determined by the contracting authority, the economic operator and, as the case may be, by the beneficiary institution;

3.4. for cases of acquaintance with information classified at the "Confidential", "Secret" level, has been previously equipped with a valid CPS.

### **Article 5** **Levels and types of ISC**

1. APCI is the authority for issuing ISC at the "Confidential", and "Secret", level.

2. When there are circumstances provided by the applicable legislation, APCI also issues ISC for the recognition of NATO and EU classified information, at one of the levels provided for in paragraph 1 of this article.

### **Article 6** **ISC validity period**

1. The ISC issued by AMCI is valid for a period of five (5) years from the date of its issuance.

2. The extension of the term of the ISC is done in accordance with the extension of the term of the CPS.

3. The ISC may be revoked before the expiration of the issuance period, when the circumstances defined in this Regulation exist.

### **Article 7** **Validity of ISC**

1. ISC issued by APCI is valid:

1.1. For access to classified information only;

1.2. For access, the right to store and administer classified information in the facilities of the economic operator;

1.3. For access, the right to store and administer classified information, as well as to use accredited communication and information systems in the economic operator's facilities.

**Article 8**  
**Basic economic operator criteria for access to classified information**

1. The economic operator has the right to access classified information, only when:
  - 1.1. possesses valid ISC, confirmed by the authority responsible for the security of classified information;
  - 1.2. the security officer has previously briefed CPS equipped personnel on security procedures and responsibilities;
  - 1.3. access to classified information is subject to the application of the "need to know" principle;
  - 1.4. the contracting authority and, as the case may be, the beneficiary institution that possesses the classified information has offered the interested economic operator normal working conditions in its facilities, within the security zones.

**Article 9**  
**Criteria for access, storage and administration of classified information in the facilities of the economic operator**

1. Every economic operator has the right to access, store and manage classified information in its facilities, when:
  - 1.1. it meets the criteria provided for in Article 8, of this Regulation;
  - 1.2. has set up the internal security structure which, under the supervision of the security officer, is responsible for the security of classified information in accordance with the requirements of the applicable legislation;
  - 1.3. the institution that possesses the classified information, has given written consent, addressed to APCI;
  - 1.4. APCI has made written confirmation for the contracting authority and the economic operator, having previously verified through direct security inspection, that the economic operator meets all the requirements provided by the legislation in force for the administration of classified information in its facilities, within security zones.

**Article 10**  
**Validation of ISC and CPS**

1. APCI recognizes and confirms the validity period, level and type of ISC and CPS which are issued by a competent authority responsible for the security of classified information of a member country of NATO, the EU, or a country with which it has a Security Cooperation Agreement.

2. The contracting authority is responsible for collecting and addressing complete identification data to APCI, in order to confirm the past of ISC for the foreign economic operator and of CPS for its personnel.
3. The recognition of the validity period, level and type of ISC and CPS, according to paragraph 1 of this article, is carried out only after official correspondence between the counterpart authorities.
4. APCI confirms the past for economic operators that will be part of the phases of procurement in the field of defense and security, which contain classified information, providing the required information to the contracting authority, regarding the validity period, level, type of ISC, as well as personnel equipped with appropriate CPS.

### **Article 11** **ISC application prerequisites**

1. For equipment with CSI for participation in a procurement in the field of defense and security which contains classified information, according to the methods provided in Article 12 of this Regulation, provided with a Unique Identification Number (NUI) in our country, the economic operator must meet all the following conditions:

- 1.1. To have an organizational structure;
- 1.2. At least during the last three years it results in positive balances, referring to the financial statements certified by the Tax Administration of Kosovo;
- 1.3. During the last three years, has not been excluded from participating in public procurement procedures;
- 1.4. During the last three years, has not been excluded from participating in procurement procedures in the field of defense and security that contain classified information. This condition is considered unfulfilled for the economic operators who are in the judicial process for the exclusion procedure, until the moment when the competent court takes a final decision;
- 1.5. During the last ten years, the Industrial Security Certificate (ISC) has not been refused or revoked;
- 1.6. It turns out that the person/entity is equipped with the professional license/s, in relation to the activity for which he is registered, certified by relevant original documentation, or notarized;
- 1.7. Is not subject to liquidation, in the process of bankruptcy or awaiting bankruptcy proceedings, certified by a notarial declaration of the administrator of the economic operator and by a certificate issued by the competent Court;
- 1.8. Is not in the conditions of the prohibition of the exercise of the activity, certified by a notarial statement of the administrator of the economic operator;

1.9. The administrator, the owner/owners, the economic operator are not convicted, confirmed with evidence from the competent court;

1.10. Referring to the certification issued by the competent Court, it results that the economic operator has not been sentenced by a final verdict;

1.11. It turns out that the Economic Operator has paid the taxes, confirmed through the certificate issued by the Tax Administration of Kosovo;

1.12. The Economic Operator which has loans received in the banking system, it turns out that it repays them regularly, confirmed through the certification issued by the Central Bank of Kosovo;

1.13. The Economic Operator who has taken loans, turns out to repay them regularly, confirmed through the Declaration under oath of the Owner/Administrator/notarized.

2. Finding that one or more of the criteria provided for in paragraph 1 of this article is not met is sufficient reason for not starting or immediately terminating the procedures for issuing an ISC;

## **Article 12**

### **Method of application for ISC**

1. The application for being issued with an ISC is addressed to APCI. The application methods to be equipped with ISC are:

1.1. At the request of the contracting authority;

1.2. At the request of the competent authority responsible for the security of classified information of a member country of NATO, the EU, or a country with which it has a Security Agreement;

1.3. At the request of the competent authority responsible for the security of classified information of NATO, the EU or another structure within these two organizations in the capacity of contracting authority;

1.4. At the direct request of the local economic operator, only when:

1.4.1. The interested economic operator fulfills all the preliminary conditions provided for in paragraph 1, of Article 11 of this Regulation;

1.4.2. The interested economic operator, during the last 3 (three) years, has been a party at least 1 (one) time to a contract/subcontract in the field of defense and security which handled classified information, certified in writing by the relevant contracting authority.

2. Application according to sub-paragraphs 1.1., 1.2. and 1.3. of paragraph 1 of this article is conducted when:

2.1. there is an interest in participating in a procurement in the field of defense and security, which contains classified information, or when the economic operator is in the conditions of the implementation of the contract/subcontract containing classified information;

2.2. the interested economic operator fulfills all the preliminary conditions provided for in paragraph 1, of Article 11 of this Regulation;

2.3. the application request with ISC is accompanied by the application documentation, according to the provisions made in Article 13, of this Regulation.

### **Article 13** **Application documentation for ISC**

1. The application documentation to be equipped with ISC, contains:

1.1. The request for the issuance of ISC, directed to APCI, according to the model defined and approved by this authority;

1.2. The Industrial Security Questionnaire and the authorization for granting consent for verifications and the preservation of "classified information", according to the model defined and approved by APCI;

1.3. Business certificate for the data of the economic operator;

1.4. The certificate issued by the Court, which certifies that there is no criminal process against the Economic Operator;

1.5. The certificate issued by the Chamber of Executors, which certifies that there is no Enforcement order for the capitals/assets of the Economic Operator;

1.6. The certificate issued by the Tax Administration of Kosovo, which certifies that the economic operator has fulfilled the tax obligations;

1.7. The certificate issued by the Central Bank of Kosovo, which certifies, if the Economic Operator has loans received in the banking system and repays them regularly;

2. The application documents, according to this article, must be original, issued by the relevant authority within the last three months. They are addressed to APCI, accompanied by Security Questionnaires for the verification of personnel who will be familiar with classified information.

### **Article 14** **Criteria for initiating security verification**

1. The economic operator which has applied to be equipped with ISC according to the criteria provided in this Regulation, is subject to following the security verification procedures, only when APCI finds that:



1.1. the interested economic operator has provided the complete documentation of the application and all the required information, according to the requirements of the applicable legislation;

1.2. the economic operator fulfills all the preliminary conditions provided for in paragraph 1, of Article 11 of this Regulation;

1.3. the administrator of the economic operator has given written consent to collect data and carry out security verification procedures for the economic operator concerned, referring to the requirements of the applicable legislation;

2. APCI examines the request and within 30 (thirty) calendar days from the day of being served whereof, addresses the corresponding answer to the state institution or the economic operator concerned.

### **Article 15**

#### **Time limit for carrying out security verification procedures and for re-application cases**

1. The general deadline for performing security verification procedures lasts up to 120 (one hundred and twenty) calendar day. This period begins only after complete submission and confirmation in writing by APCI.

2. The procedures for security verification may continue beyond the general term defined in paragraph 1 of this article, in cases where:

2.1. The verifications are conditioned by carrying out procedures in cooperation with the competent authorities responsible for the security of classified information of other countries.

3. In cases where, during the implementation of the contract, it turns out that the contractor or subcontractor's validity period of the ISC expires, the contracting authority and, as the case may be, the beneficiary institution, have the obligation to, in cooperation with the economic operator, complete the documentation required according to Article 10 of this Regulation and address to APCI, not later than 150 (one hundred and fifty) calendar days before the expiration of the validity period of the ISC.

4. In cases where, during the implementation of the contract, the contractor or subcontractor turns out to be a foreign economic operator whose validity period of the ISC expires, then the contracting authority and, as the case may be, the beneficiary institution, have the obligation to, in cooperation with the foreign economic operator, present the requested information to APCI, no later than 240 (two hundred and forty) calendar days before the expiration of the validity period of the ISC and CPS. After receiving complete information regarding the data of the foreign economic operator and its personnel, AMCI initiates formal correspondence with the peer authority for the issuance of ISC and CPS and confirmation of the relevant past.

**Article 16**  
**Subject of security verification**

1. For an economic operator applying for an ISC, the object of security verification is:
  - 1.1.ownership structure and its origin including subsidiaries/branches;
  - 1.2.activity of economic operator;
  - 1.3.local and foreign close partners;
  - 1.4.financial stability;
  - 1.5.fulfillment of financial obligations to state institutions and third parties;
  - 1.6.the ability, technical, physical capacities and those for the security of classified information, referring to the requirements of the applicable legislation, in cases where they administer classified information within the premises of the economic operator;
  - 1.7.the persons owning the ownership of the economic operator;
  - 1.8.the administrator and other persons who are part of the management staff at the time of application for being issued with ISC;
  - 1.9.employees who will have access to classified information;
  - 1.10. the persons proposed by the administrator for the position of industrial security officer and his deputy.

**Article 17**  
**Industrial security verification procedures**

1. APCI requests the necessary information in order to verify the security of the economic operator that has applied to be equipped with ISC.
2. Holders of public or non-public institutions have the obligation to officially, in writing, provide the requested data within 5 working days from the date of the request submitted by APCI.
3. APCI, on the basis of necessity, invites to the interview the person who is subject to the verification procedure, requests from them the submission of additional documentation for the purpose of security verification.
4. The Industrial Safety Questionnaire is an Appendix to this regulation.

**Article 18**  
**Basic criteria for assessing unacceptable security risk**

1. An economic operator interested in being equipped with ISC does not constitute an unacceptable security risk when:
  - 1.1. It completes and implements the general requirements provided for in this Regulation;
  - 1.2. It is financially sustainable;
  - 1.3. It is reliable for security purposes and possesses the capability and technical capacity for the security of classified information.
2. An economic operator is not financially sustainable if it results that:
  - 2.1. Has gone bankrupt or is in liquidation, has made an agreement with creditors, has suspended business activities or is in a similar situation;
  - 2.2. It is subject to bankruptcy proceedings, there is a compulsory liquidation or administration order;
  - 2.3. Has not fulfilled the obligations related to the payment of taxes and duties, in accordance with the applicable legislation;
  - 2.4. It turns out that it has been banned from carrying out commercial activities;
  - 2.5. There is negative business performance proven through 1 (one) or more negative balances in the last 3 (three) years of activity;
  - 2.6. The co-owners are in conflicting economic-financial circumstances related to the ownership structure of the economic operator.
3. Economic operators can provide information about their financial viability and the necessary financial capacities by means of bank statements.
4. An economic operator is not reliable for classified information security purposes when:
  - 4.1. It turns out that during the last 10 (ten) years the ISC was revoked for violating the security rules of classified information, or violated the security rules in the conditions of procurement of a contract/subcontract which contains classified information;
  - 4.2. During the application for equipment with ISC has provided false information and false documents or has concealed information related to aspects of security verification;
  - 4.3. It turns out that it has income obtained from criminal or unjustified activities, referring to the discrepancy between capital and property and income regularly declared by it;

4.4. It turns out that he is in partnership, or close business relations with persons, who have been referred to by verified data or reasonable suspicions of involvement in espionage, terrorism, organized crime, corruption, or any other form of threat to national security;

4.5. The owner/owners, the administrator, are convicted of criminal activity, or with proven data or reasonable suspicion of their involvement in espionage, terrorism, organized crime, corruption, or any other form of threat to national security;

4.6. It refuses to take the measures recommended by APCI to “reduce” to acceptable limits the security risk from the potential of influence exerted on behalf of foreign interests, according to Article 19 of this Regulation.

### **Article 19** **Criteria for the assessment of foreign influence and impact**

1. Foreign ownership, as a form of control or influence, refers to a situation when an individual foreign third party (person, economic operator or government) is assessed as having influence or authority over a domestic economic operator, to such a degree, where a third party may gain access to classified information.

2. The assessment of foreign influence aims to identify the actual degree or the potential of possible influence, exercised on behalf of foreign interests, through which unauthorized access to classified information is intended.

3. APCI conducts the assessment of foreign influence, referred to:

3.1. ownership or the majority of owned shares;

3.2. the positions of the administrator, managerial staff or personnel in key positions in the activity of the economic operator concerned.

4. An economic operator can be placed under the influence exercised on behalf of foreign interests, when it turns out that a foreign interest has power, direct or indirect, whether exercised or not, to direct or decide on matters that affect the management or operations of the economic operator, in a way that may result in unauthorized access or may adversely affect the completion of contracts containing classified information.

5. It is considered to be under the possible influence exerted on account of foreign interests:

5.1. Any domestic economic operator, who has in the position of administrator, member of the managerial staff or key positions of management and supervision of his activity, persons who have the citizenship of countries that are not members of NATO, the EU of a country with which the Republic of Kosovo does not have a Security Agreement;

6. APCI examines the assessment matrix related to the potential influence exercised on behalf of foreign interests, using the levels of ownership or the majority of shares they own for each interested economic operator.

7. APCI, in cooperation with the interested economic operator, use restrictive and protective security measures to "reduce" to acceptable limits the security risk from the potential of influence exerted on behalf of foreign interests, which in their entirety aim to prevent unauthorized access to classified information.

## **Article 20**

### **Unacceptable security risk assessment**

1. APCI performs the assessment of the unacceptable security risk of the economic operator, before issuing the ISC.

2. The assessment of unacceptable security risk is carried out based on:

2.1. Obtained information and verifications for the economic operator that will be provided with the ISC and the categories of persons that will be provided with the CPS;

2.2. The preliminary inspection report of the central offices of the economic operator, related to the possession of technical, physical skills and capacities and those for the security of classified information, referring to the requirements of the applicable legislation;

2.3. The assessment related to the degree of the possible influence exerted on account of foreign interests and security risk limitation measures.

## **Article 21**

### **Issuance of ISC**

1. APCI issues the ISC for the economic operator, when it assesses that:

1.1. There is no unacceptable risk to the security of classified information;

1.2. The interested economic operator possesses the ability and technical capacities for the security of classified information, according to the requirements provided in this Regulation and by the applicable legislation.

2. In the case when the ISC is not issued, APCI notifies in writing the institution or structure that requested the issuance with the ISC of the economic operator.

3. Issuing the ISC of a subsidiary or branch of the economic operator is carried out by the competent authority responsible for the security of classified information, of the country where the subsidiary or branch is registered and equipped with a Unique Identification Number (UIN).

4. Issuance of CPS for employees of the subsidiary or branch of the economic operator is carried out by the competent authority responsible for the security of classified information of the country of which they hold citizenship.

## **Article 22**

### **Removal of ISC**

1. APCI, makes the decision to remove the ISC, in cases where:

1.1. Through the contracting authorities, or the inspections carried out, it receives official reports, verified information or in the framework of reasonable suspicion, according to which, reasoned conclusions are reached, that the further retention of the ISC issued to an economic operator, constitutes an unacceptable risk for the security of classified information, referring to the requirements defined in this Regulation and the relevant Law on the Protection of Classified Information;

1.2. The existence of the circumstances provided in paragraph 2 and 4 of Article 18 of this Regulation is verified.

## **Article 23**

### **Temporary suspension of ISC**

1. APCI takes the Decision on the temporary suspension of ISC, when it is established that:

1.1. The economic operator is under the possible potential of influence exerted on account of foreign interests, until taking measures to limit the security risk;

1.2. Violations of security rules or non-fulfillment of the obligations provided for in the Project Security Guide have been found;

1.3. Information or official reports have been provided, according to which suspicions are created that must be confirmed, that the further retention of the ISC issued to an economic operator constitutes an unacceptable risk for the security of classified information.

2. The decision on the suspension of the ISC is valid until the clarification of the facts or cessation of circumstances, which constitute an unacceptable risk to the security of classified information, or until the moment when the ISC expires.

## **Article 24**

### **Obligations of AMCI, when removing or suspending ISC**

1. APCI, in any case when it removes or temporarily suspends the ISC, about the decision, informs:

1.1. contracting authorities and economic operators involved in the performance of a classified contract as well as, where applicable, the competent authority responsible for information security of another country;

1.2. The competent authority responsible for the information security of another country, when the economic operator against whom the measure of suspension or revocation of the CSI has been taken, is a party to an international contract/subcontract in the field of defense and security, which contains classified information.

2. The notification information includes the legal reasoning related to the temporary suspension or removal of the ISC, when it does not contain classified information according to the applicable legislation.

### **Article 25**

#### **Right of appeal**

1. The economic operator whose Industrial Security Certificate or Personnel Security Certificate has been refused, suspended or removed has the right to file a complaint with APCI within fifteen (15) days from the date of receipt of the notification.

2. The complaint is reviewed by the Complaints Commission according to the Regulation on Personnel Security Verification Procedures and the Complaint Procedure.

### **Article 26**

#### **Issuance and adjustment of CPS for employees of the economic operator**

1. The procedures for issuing, removing, suspending and rejecting CPS issuance and any other aspects for the safety of the personnel of the economic operators concerned, are carried out in accordance with the provisions of the applicable legislation.

2. In cases where a person, who possesses a CPS and, is in two or more workplaces, he is transferred to one workplace to an economic operator equipped with ISC or to a state institution, the state institution or economic operator must notify AMCI, which made the adjustment to the new position it holds.

### **Article 27**

#### **Duties of customs authorities, police and other institutions**

1. The Customs Authorities, of the Kosovo Police and, as the case may be, of other state institutions, after receiving the written notification from the authority responsible for the security of classified information, for details related to the transport of the classified shipment, take measures to:

1.1. engage employees of their structures equipped with appropriate CPS for carrying out relevant customs and police procedures without exposing classified information;

1.2. customs officers, customs agents, police officers and any other individual, who will have access to the accompanying documentation of the classified shipment, sign and confirm their knowledge of the elements of the classified shipment.

2. The customs authorities, the state police and, as the case may be, other state institutions, after fulfilling the obligations defined in paragraph 1 of this article, examine the legal documentation of the transport and perform their functional duties, guaranteeing the security of the classified shipment.

2.1. Transport documents, which are an integral part of the classified shipment, must not under any circumstances be exposed as such to unauthorized persons;

2.2. Transport documents are accompanied by data about the origin and destination of the classified shipment, the forecast for the arrival time, the accompanying equipment for delivery (if any), the identification data of the person receiving the classified shipment, etc.

3. The customs authorities, police and, as the case may be, other state institutions take the appropriate measures so that their administrators, regardless of the function and duties they perform, under no circumstances keep the classified shipment in storage in their work environments.

4. The Receiving Party, through the authorized person, confirms the receipt of the classified shipment, by signing the relevant transport documentation and, as the case may be, the relevant documentation held by the customs authorities, police and other state institutions.

## **Article 28** **Transport**

1. The transportation of classified material outside the security zone or abroad is carried out by means that meet the requirements for the provision of classified information, as defined in the classified contract.

2. The contracting authority determines the measures for securing the classified material, which must be applied at all stages during transportation and under any circumstances, from the point of origin to the destination. Transportation by air and sea are carried out under the same security conditions as transportation by land.

3. Measures to secure the classified material being transported must be at the highest level.

4. Personnel transporting classified material must have appropriate security clearance.

5. The transit route is determined on safe roads, but if it has to pass through large cities, measures are taken to ensure that the material is out of danger and crisis.

6. The packaging of the classified material is done with an inventory list, according to the classification level.

7. Classified material is transported in closed metal crates or containers, secured and under the supervision of at least one security officer, as well as marked and sealed. When the transport includes two or more containers, security measures for each must be taken in accordance with the highest level of classification of the classified material they carry.



8. In exceptional circumstances, classified material is transported only by special means, accompanied by armed guards, in coordination with the relevant units of the Ministry of Internal Affairs or the Ministry of Defense.

9. Stopping at certain places during transportation is done in accordance with a prepared security plan.

10. In cases of emergency, accident, vehicle breakdown, natural disaster or similar, the classified material is kept during the whole time of the stop in the designated place, by the security guards, armed, and by the accompanying persons.

11. During the transportation of classified material, continuous communication is maintained, with appropriately certified tools and equipment.

12. In conditions of increased risk for classified material, security guards are appointed. Depending on the assessment of the concrete risk, guards and armed civilians may be assigned. Persons assigned as guards or escorts are trained and given detailed instructions on how to handle classified material.

## **Article 29**

### **Visits**

1. The visits are carried out for legal purposes and authorized by the contracting authority, when it is foreseen that the classified material will be presented by the contractor who has the appropriate Security Certificate.

2. Visits are scheduled over a period of one year. Visits related to the classified contract are carried out for the duration of the contract and with the approval of the contracting authority. The number of visits should be as low as possible. Visits are categorized as follows:

2.1. Special visits, with a specific purpose and duration of up to 30 days and that do not repeat within the year;

2.2. Periodic visits, in certain periods of time, within the year;

2.3. Urgent visits, which are carried out due to a matter of special importance.

3. Visits are made to the contracting authority or to the economic operator. In cases where the subject of the visits is the economic operator, he notifies the contracting authority in writing and requests his approval for the visit. In urgent cases, the request for a visit can be made orally, provided that it is accompanied, then, in writing, within 10 days from the date of the visit.

4. Representatives of public institutions, in the implementation of official duties, may visit the economic operator without prior notice, provided that these representatives present the security clearance and official position identification documents, as well as the relevant authorization. In pre-approved visits not related to the classified contract, classified information is not exposed without the prior approval of the contracting authority.

5. Visitors are given access only to classified information, related to the purpose of the visit and the need to know the information, after being equipped with appropriate security certificates.

6. The visit authorization contains:

6.1.Purpose and reason;

6.2.CSI level, the contractor's name, address, telephone number and e-mail address;

6.3.The name, date, place of birth and citizenship of the person conducting the visit;

6.4.Security clearance verification and special access authorization;

6.5.Names of persons to be contacted;

6.6.The period of validity of the visit authorization documents;

6.7. In any case, the authorized security personnel of the economic operator keeps the protocol of the visits.

7. In previously approved visits related to the classified contract, classified material may be exposed without the approval of the contracting authority, in cases where the economic operator finds it in accordance with the legislation in force.

8. Visits by representatives of a third party are made only with the prior approval of the parties, included in the classified contract.

### **Article 30** **Inspection of Economic Operators and subcontractors**

1. If, during the inspection of economic operators and subcontractors, AMCI finds that classified information is not stored in accordance with the project's security plan, it compiles a report on the findings and recommends the managers of the Public Institution in the capacity of the contracting authority to take the necessary measures for improvement of security within the areas where classified information is stored or administered and the time frame for the implementation of the recommendations.

2. The public institution to which the recommendations have been sent is obliged to take all measures towards the economic operator or the subcontractor for the improvement of security measures for the implementation of APCI's recommendations until the termination of the contract and it must notify APCI for this.

3. If, during the inspection, APCI assesses that the violation of classified information security measures has elements of a criminal offense, it notifies the competent institution.

**Article 31**  
**Repeal**

Upon entry into force of this Regulation, the following shall be repealed: Regulation No. 15/2011, Standards for Classified Information Security for Economic Operators.

**Article 32**  
**Annex**

Attached to this is the Industrial Safety Questionnaire.

**Article 33**  
**Entry into force**

This Regulation enters into force seven (7) days following its' publication on "Official Gazette" of the Republic of Kosovo.

**Albin KURTI**

---

**Prime Minister of the Republic of Kosova**

**10 May 2024**



**Republika e Kosovës  
Republika Kosova – Republic of Kosovo**

**INDUSTRIAL SECURITY QUESTIONNAIRE**

## **Guide on Industrial Security Questionnaire (ISQ)**

**Please follow the following instructions carefully:**

**Before completing, carefully review all sections of the ISQ.**

**Complete each section of the ISQ with complete and accurate information.**

**The administrator/representative of the economic operator writes the data and signs each page of the ISQ in the designated place.**

**In the sections where the administrator/representative of the economic operator has no information to declare, enter "Not applicable"**



**2 PRESENT THE INTERNAL ORGANIZATIONAL STRUCTURE (organogram) OF THE EO**

a. Specify relevant departments and representative personnel:

**3 PRESENT THE ORGANIZATIONAL CHART SHOWING THE OWNERSHIP OF THE EO AND ITS RELATIONSHIP WITH OTHER RELATED Eos**

a. Specify the names and addresses of the associated Eos:









If yes, provide details:

Which EO:

Percentage of shares:

The date since you've owned the shares:

--	--	--	--	--	--	--	--	--	--

h. Does EO own shares directly or through controlled companies (subsidiaries) and/or its branches that are part of foreign capital?

 YES  NO

If yes, provide details:

Name of the foreign EO:

Country of registration of foreign EO:

The percentage of shares in foreign OE possession:

The capital ownership start date:

--	--	--	--	--	--	--	--	--	--

i. Is there any foreign individual or entity, directly or indirectly, an owner in your EO?

 YES  NO

If yes, provide details:

Specifics of the individual (name, surname, date of birth, ID No.) or of the foreign EO:

Place of registration of the foreign OE/citizenship of the foreign individual:

The share of capital owned by the foreign EO/foreign individual, expressed in percentage:

The capital ownership start date:

--	--	--	--	--	--	--	--	--	--

The method of acquiring capital owned by the foreign EO/foreign individual:

j. Do you think that any foreign individual or EO has the ability to control or influence the operations or management sphere of the EO?  YES  NO

If yes, provide details:

Specifics of the individual (name, surname, date of birth, ID No.) or of the foreign EO:

Method of foreign influence/control:

k. Does the EO have other financial investments, other than ownership (such as lending, guarantees, etc.), in other EOs?  YES  NO

If yes, provide details:

EO name and country of registration:

Type of investment and commercial value:

Date of investment:

--	--	--	--	--	--	--	--	--	--

l. Has income been generated from individuals or foreign EOs and/or contracts (contacts, agreements) with individuals or foreign EOs in the last 3 (three) years?  YES  NO

If yes, please provide related information:

Specific details of the individual (name, surname, date of birth, ID No.) or information on the foreign EO from which the income is generated:

Purpose of the contract/agreement:

Date when the contract/agreement was signed:

--	--	--	--	--	--	--	--	--	--

The percentage of total income of the EO, which was generated by the individual/foreign EO:

ll. Does EO have any financial debt or obligation to individuals or foreign EO?  YES  NO

If yes, please provide related information:

Specifics of the individual (name, surname, date of birth, ID No.) or of the foreign EO:

Type of debt/obligation:

Value of debt/obligation:

The period and methods of repayment of debt/obligation:

Collateral used:

Has the repayment of the debt/obligation been made, or is being made according to predetermined conditions:

Procedures foreseen to be followed in case of late repayment of obligations:

Clarify: whether the debt or obligation has an impact on the current assets of the company and its operations:

## 6 INFORMATION ON THE ACTIVITY OF THE ECONOMIC OPERATOR

a. Has EO participated in public procurements in the last 3 (three) years?

YES

NO

If yes, please clarify:

b. Has EO executed contracts from public procurements in the last 3 (three) years?

YES

NO

If yes, provide details of each public contract as follows:

Name of contracting authority:

Purpose of procurement:

Date of entering into contract(s):

Name and surname \_\_\_\_\_

Signature \_\_\_\_\_

Page 11 of 17

Date of completion of the contract(s):

- c. **During the last 3 (three) years, has EO been excluded from participating in public procurement procedures?** *(Confirmed by relevant, original documentation issued by the competent authority)*  YES  NO

*If yes, provide details:*

- d. **Is the EO undergoing any administrative procedure?**  YES  NO

*If yes, provide details:*

Name of contracting authority:

Purpose of procurement:

Reasons for the procedure:

- e. **During the last 3 (three) years, has EO been excluded from participating in public procurement procedures in the field of defense and security?** *(Confirmed by relevant documentation issued by the competent authority)*  YES  NO

*If yes, please clarify:*

- f. **During the last 3 (three) years, has the EO participated in procurements in the field of defense and security, which contain classified information?**  YES  NO

*If yes, provide details:*

- g. **During the last 3 (three) years, has the EO concluded procurement contracts in the field of defense and security, which contain classified information?**  YES  NO

*If yes, please provide the data for each procurement contract in the field of defense and security, which contains information classified as below:*

Name of contracting authority:

Purpose of procurement:

Level of classification:

The date of completion of the contract(s) (Accompanied by certificates of execution of the contract(s):

--	--	--	--	--	--	--	--	--	--

h. During the last 3 (three) years, has EO entered into contracts with other companies?  YES  NO

If yes, please clarify:

i. Is the EO undergoing any administrative or judicial procedure for non-fulfillment of contracts with natural or legal persons?  YES  NO

If yes, please clarify:

Information about the claimant and the date of the lawsuit:

The purpose of the contract for which you have been sued:

The institution that is reviewing it:

**7 SECURITY INFORMATION ON THE ECONOMIC OPERATOR**

a. Is the EO involved in business cooperation with person/s or legal entities for whom you have information that they have had illegal proceeds?  YES  NO

If yes, provide details for:

Specifics of the individual (name, surname, date of birth, ID No.) / name of entity:

Country of registration:

Method of cooperation:

Period of cooperation:

--	--	--	--	--	--	--	--	--	--

b. Has any legal action been initiated against EO, due to any illegal activity?  YES  NO



If yes, provide details for:

Reason for commencing action:

Who initiated it:

At which court:

Start date:

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

c. Do you have information on conflict of interest within the OE related to ownership/co-ownership?

 YES  NO

If yes, provide details for:

Specifics of the individual (name, surname, date of birth, ID No.) /name of EO:

Type of conflict:

Start date:

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

d. Has the EO employed individuals with foreign citizenship?

 YES  NO

If yes, provide details for:

Name:

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Surname:

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Gender:  M  F

Date of birth:

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Place of birth:

Kombësia / Shtetësia:

Home address:

Contact, e-mail, tel, fax:




**9 LIST OF PERSONS WHO WILL BE PROVIDED WITH A CERTIFICATE OF PERSONNEL SECURITY**

No	Name and surname	Date of birth	Phone No.	Position/Function	Remarks
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

**Statement**

In the capacity of the EO Administrator \_\_\_\_\_, by completing and signing this questionnaire, I give my consent to the security, intelligence and law enforcement authorities to control and process the information declared in this document, as well as to undertake the procedures provided by the legislation in force for the implementation of the security verification of the Economic Operator

\_\_\_\_\_.

I agree that verification procedures should be applied by public authorities, which according to current normative acts are responsible for performing such a task.

I agree that the Economic Operator \_\_\_\_\_, is inspected by APCI as part of the procedure for obtaining an Industrial Security Certificate and subsequently throughout all its validity periods.

In the capacity of the Administrator/representative of the EO, I assume full responsibility, to safe-keep and administer classified information according to requirements of legislation in force.