



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

---

**REGULATION (GRK) NO 13/2024 ON THE PHYSICAL SECURITY OF  
CLASSIFIED INFORMATION<sup>1</sup>**

---

<sup>1</sup> Regulation (GRK) No. 13/2024 on the Physical security of Classified Information, was approved on the 203 meeting of the Government of Kosovo, with the Decision No. 04/203 dated 08.05.2024.

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

Pursuant to the Article 93 (4) of the Constitution of the Republic of Kosovo, in accordance with Article 45 paragraph 6 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 Regulation No. 09/2011 on the Rules of Procedure of the Government,

Approves:

## **REGULATION (GRK) NO 13/2024 ON THE PHYSICAL SECURITY OF CLASSIFIED INFORMATION**

### **Article 1 Purpose**

1. This regulation aims to establish standards for the physical security of classified information for all public institutions, economic operators, the provision of spaces where classified information is kept, as well as setting the standards for the physical transportation of classified information.

2. This regulation is in harmony with EU legislation, as follows:

2.1. Council Decision of 23 September 2013 on the security rules for protecting EU classified information.

### **Article 2 Scope**

This regulation is applied by all institutions of the Republic of Kosovo and economic operators, which produce, maintain and administer classified information in compliance with security standards.

### **Article 3 Definitions**

1. The terms used in this regulation have the following meaning:

1.1. **Physical Security** - Physical security is the set of physical, technical, electronic and procedural measures for the preservation of areas, buildings, offices, rooms, spaces and equipment where classified information is produced, recorded, used, transmitted, stored, archived and destroyed, including the process of risk management to prevent unauthorized access to security areas;

1.2. **The outer perimeter of the security zone** – represents the minimum distance from the object where the classified information is kept and administered, using active and passive means, to prevent the detection of unauthorized access to the facility;

1.3. **Fence** - represents the physical barrier and identifies the border of the place that requires the protection of the space where the classified information is stored;

1.4. **Material/cases** - includes documents as well as any machinery, equipment, weaponry that has been produced or is under production;

1.5. **Guard post** - represents the designated place which is guarded by authorized persons for physical security;

1.6. **Assessment Form** - It is a document based on which AMCI assesses the security standards of the external and internal security perimeter where classified information is stored.

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

#### **Article 4** **Criteria for physical storage of classified information**

1. All facilities, offices, rooms, spaces and equipment where classified information is stored must be protected with special security measures according to the following criteria:

1.1. Level of classification;

1.2. The amount, volume and form of information (document written on paper or electronically);

1.3. Security certificate and need to know from official person;

1.4. Risk assessment from possible interventions of foreign intelligence services, terrorism, sabotage and other criminal activities;

1.5. Entry of unauthorized persons;

1.6. Theft, damage or loss;

1.7. Timely detection and response in case of technical breakdowns;

1.8. Regular checking of inventory and equipment to protect against potential interception before entering the areas where information is stored.

#### **Article 5** **Physical security of classified information**

1. The physical security of classified information represents only one aspect of the protection of classified information which is supported by other disciplines of the protection of classified information provided for in the relevant Law on the Protection of Classified Information, which are:

- 1.1. Personnel security;
- 1.2. electronic security;
- 1.3. industrial security; and
- 1.4. security of information.

2. The security level of the space where the classified information is stored must be at the appropriate level of protection and classification level of the information, its quantity and volume.

3. The plan for physical security is approved by the institution approved by order from the head of the relevant institution where classified information is stored in accordance with the security standards defined by this regulation and with the construction, material and height of the facility.

### **Article 6** **Minimum security standards**

1. The minimum security standards that must be met by the space where classified information is stored are:

- 1.1. classified information is not stored on the ground floor nor on the top floor, if the building is a multi-storey facility;
- 1.2. the width of the wall must comply with security standards;
- 1.3. the doors of the spaces must be protected with iron bars, and be secured from the inside with an emergency exit with an iron bolt, or a strong padlock that exceeds the width of the door;
- 1.4. entrance doors must be secured with locks with built-in three-position combinations, or in special cases, other locks approved by the competent authority, only for rooms where “TOP SECRET”, “SECRET” and “CONFIDENTIAL” information is stored;
- 1.5. internal and external acoustic insulation;
- 1.6. ventilation and air conditioning;
- 1.7. metal shelves;
- 1.8. the keys to the spaces where the metal shelves are located must be secured;
- 1.9. keys to metal racks should not be taken outside the offices of the building;
- 1.10. recognition of combinations should be limited to the smallest possible number of employees;

- 1.11. working and spare keys should be kept in different metal shelves;
- 1.12. the envelopes where the keys and combinations are placed must be stored at the level of the information to which access is enabled;
- 1.13. keys and combinations must be changed at time intervals no longer than 12 months;
- 1.14. keys and combinations must also be changed in the following cases:
  - 1.14.1. in securing shelves before first use;
  - 1.14.2. whenever employees who know that combination change;
  - 1.14.3. whenever there is reasonable suspicion that danger has arisen.
- 1.15. ground level windows, or other windows that can be easily reached (through the roof, terraces and annexes) must be protected with material that ensures them from forced entry;
- 1.16. the protection given to the windows must be equal to the strength of the continuous walls of the windows;
- 1.17. installation of external and internal cameras that monitor access to security areas;
- 1.18. entry-exit control;
- 1.19. transmission of the alarm signal (Police or institution's security center);
- 1.20. detectors at the entrance of the facility;
- 1.21. metal racks for leaving weapons;
- 1.22. mobile phones and other technical and electronic devices should not be allowed in areas where classified information is stored;
- 1.23. the perimeter of the space must contain physical barriers that are in compliance with safety standards;
- 1.24. security locations and administrative areas within the building where classified information is kept must be defined;
- 1.25. signs of security sites and administrative areas should be made visible.

**Article 7**  
**Inspection of security standards**

1. APCI is the only authority in the Republic of Kosovo for the inspection and assessment of security

standards implemented by the institutions of the Republic of Kosovo and economic operators that produce and administer classified information.

2. The minimum security standards defined in Article 6 of this regulation are appropriately applied by institutions that produce and administer classified information depending on the location of the institution and the possibilities of applying the external security perimeter.
3. The inspection of security standards is done through the application of the external and internal perimeter scoring system.
4. In case the security standards are applied in the external perimeter, the public institution can apply appropriate security measures within the internal perimeter.
5. In cases where the security measures of the external perimeter are not applicable due to the location of the public institution, the public institution is obliged to take additional measures in the internal perimeter.
6. The public institution where it stores and administers classified information is obliged to apply security measures within the external and internal perimeter, achieving the minimum security standards.
7. APCI assesses security standards based on assessment forms with the determination of the minimum threshold.
8. APCI helps public institutions to achieve classified information security standards.

### **Article 8** **Storing information by classification level**

1. Mechanical barriers are set for RESTRICTED level information.
2. For CONFIDENTIAL level information, mechanical barriers and an electronic security alarm are placed.
3. For SECRET and TOP SECRET level information, mechanical barriers, access control system, electronic alarm system, and fire alarm system are installed.

### **Article 9** **Controlling entrances and exits to security areas**

1. Access to security sites and administrative areas is carried out through a passing permit.
2. The entry of vehicles into security sites and administrative areas is allowed only if necessary.
3. Vehicles are subject to a detailed check by the authorized person before each entry and exit to the areas and places referred to in paragraph 2 of this article.

**Article 10**  
**Entry of persons into security areas**

1. The entry of accompanied visitors to security sites and areas is subject to:
  - 1.1. previously performed security check;
  - 1.2. application of the "need to know" principle;
  - 1.3. whether the visitor is local or foreign; and
  - 1.4. requests for additional control.
2. Visitors must be escorted at all times. When several departments or other employees are visited, the visitors must be handed over to the authorized attendants in the respective departments and must be noted as a remark on the pass permit.

**Article 11**  
**Guarded security**

1. In the environments where classified information is stored and administered, it is necessary, in addition to the measures mentioned in Article 6 of this Regulation, to take other necessary measures for security with static and mobile guards during 24 hours.
2. Guards are responsible for protecting the environment and safety zones from the risks mentioned in Article 4 of this Regulation.
3. The patrols carry out the security of areas during holidays, after working hours and in emergency situations.
4. The rules and place of service of the guards and patrols are determined by the authority in possession of the classified information.
5. Guards and patrols are subject to constant checks, especially after hours and at night.
6. Guards and patrols must be clear about the tasks they perform and be given constant instructions for the service.
7. When the premises need more guarding or security, their security can also be done with a camera monitoring system, alarm system, entry-exit surveillance in accordance with Article 5 of this Regulation.
8. During the physical movement of classified information within the city, one guard escort is provided, while outside the city, two armed guards serve as escort.

9. The guards have the right to stop any individual moving in the premises and areas where there is classified information if the person does not clearly show the identification/distinctive sign.

## **Article 12**

### **Electronic space security**

1. The purpose of electronic security is that, in addition to other security measures, devices, tools and signaling systems are installed, in order to take measures in cases of intervention by unauthorized persons in the premises and in "security zones".

2. In the environments where "TOP SECRET" classified information is stored and administered, in addition to the other protection measures and systems provided for in Article 6 of this Regulation, electronic security devices and systems (signaling and camera surveillance systems) should be installed.

3. In cases of electronic control system defects, the responsible persons must be determined, who will intervene for their repair.

## **Article 13**

### **Distribution of classified information**

1. The initial distribution of classified information is determined by the institution that created the information.

2. The distribution of classified information is sent to public institutions which, for legal purposes, must be familiar with this type of information.

3. Distribution of classified information is done inside and outside the institution.

4. The distribution of classified documents up to the secret level is done physically or electronically through the cryptographic system.

5. The distribution of classified documents at the top secret level is done only physically.

## **Article 14**

### **Transfer of classified information**

1. The original classification authority has the exclusive right to transfer that information, only to public institutions.

2. Classified information received by the public institution is not allowed to be transferred to the other public institution, unless the original classification authority authorizes such a thing.



3. If the original classification Authority transfers the information to the public institution together with the transfer of functions, the institution that received such information is considered the institution that created that information.
4. In the event that the original classification authority transfers the information to the public institution only for the purpose of preservation, the institution that has received such information does not allow opening without the authorization of the original authority.
5. If the public institution that created that information no longer exists and the transfer of classified information to any successor institution has not been made, the public authority specifies with a decision on its termination, the method of transferring classified information to any public institution that is considered as the institution from which they originate.
6. The transfer of classified documents up to the "SECRET" level is done physically or electronically through the cryptography system.
7. The transfer of documents classified at the "TOP SECRET" level is done only physically.
8. Documents must be carried in double envelopes, the approved envelope and secure container must be used as the outer cover. The inner cover must be similarly addressed and clearly labeled "TOP SECRET", and marked "To Be Opened Only By (addressee, or return to sender)".
9. The public institution transferring classified information records all documents transferred as well as the public institution receiving those documents.
10. The public institution that received the classified information registers all the documents received as well as the public institution from which the information was transferred.

## **Article 15**

### **Physical transportation of classified correspondence between public institutions within the city**

1. The physical transport of classified correspondence between public institutions within the city is carried out with the means and personnel of each institution. The physical transport is carried out by the relevant classified mail courier of the institution and the driver of the vehicle after having previously obtained the security certificate from the Verifying Authority. They are appointed and authorized by the head of the institution.
2. The institution's classified mail courier receives classified correspondence from his institution's classified information office. After ensuring the regularity of the classified correspondence, the accuracy of the records made by the employee of this office, in the classified information correspondence submission book, he/she takes them over.
3. Classified correspondence is submitted to the classified information office of the receiving institution. In the event that the classified correspondence is missing or inaccurate, the employee of the classified information office of the receiving institution does not receive it and returns it to the

sending office for completion, through the classified mail courier. If everything is in order, he/she signs the receipt of any classified mail item or package in the sender's classified information correspondence delivery book.

4. The courier of classified mail, after delivery of objects and classified postal packages, returns to the classified information office of his institution, the book of delivery of correspondence of classified information.

5. Models of circulation books of correspondence of classified information, determined by the Verification Authority.

6. Escorts with armed guards during the physical movement of classified information should only be done for the Top Secret level.

7. Guards must be provided by the public institution that produced the classified information and the same must take all the necessary actions to preserve it until reaching the addressee.

#### **Article 16**

##### **Physical transport of classified correspondence from public institutions in Prishtina to state institutions in other cities**

1. The physical transport of classified correspondence between public institutions outside the city is carried out with the means and personnel of each institution. It is carried out by the institution's classified mail courier, and the vehicle driver after having previously obtained the appropriate Security Clearance from the Verifying Authority.

2. The driver and post courier are authorized in writing by the owner of the institution.

3. During the physical movement of information classified at the top secret level outside the city, security is provided with an escort of two armed guards.

#### **Article 17**

##### **Physical transport of classified correspondence from public institutions in Prishtina to relevant structures abroad and vice versa**

1. The physical transport of classified correspondence from state institutions in Prishtina to state structures abroad is carried out by 2 (two) diplomatic couriers of the relevant Ministry of Foreign Affairs.

2. A diplomatic courier office is established in the relevant Ministry of Foreign Affairs, which must meet the conditions for the physical security of classified information.

3. Diplomatic couriers of the Ministry of Foreign Affairs are previously provided with all the necessary diplomatic courier documents, as well as "CSP", appropriate from the Verification Authority according to the applicable legislation.

4. Diplomatic couriers keep the classified information correspondence delivery book which is registered in the register of classified information records at the Ministry of Foreign Affairs.
5. Diplomatic couriers are responsible for the maintenance, storage and physical security of classified correspondence during the transport process, up to the respective destination.
6. Each public institution, with its own means and personnel and according to the rules specified in this regulation, sends and delivers classified correspondence addressed abroad, to the diplomatic courier of the Ministry of Foreign Affairs.
7. Classified correspondence addressed abroad, after being packaged according to the relevant rules, is waxed and sealed with the dry seal of the Ministry of Foreign Affairs.
8. The diplomatic courier, before taking delivery, checks the classified correspondence and after making sure that everything is in order, signs in the correspondence delivery book of the classified information of the sending institution. Classified correspondence is transported by securing it (stored) in a diplomatic case. All classified correspondence is recorded in the diplomatic courier's classified information correspondence delivery book, which is kept in the diplomatic bag together with the classified correspondence.
9. Diplomatic couriers deliver classified correspondence to the classified information office of the receiving institution. The receiver checks each classified correspondence and if everything is in order, signs their receipt in the correspondence delivery book of the classified information of the diplomatic courier. In the event that there are deficiencies or inaccuracies in the classified correspondence, the employee of the classified information office of the receiving institution returns it to the sending office through the diplomatic courier.
10. In return, the diplomatic courier also receives the classified correspondence that the relevant institutions have for the public institutions in Prishtina, recording them in the Book of Delivery of Correspondence of Classified Information. The diplomatic courier, before taking delivery, checks from the outside any classified correspondence and after making sure that everything is in order, signs the delivery book of the classified information correspondence of the sending institution.
11. The diplomatic courier delivers the classified correspondence to the classified information offices of the institutions where they are addressed, against the recipient's signature in the diplomatic courier's classified information correspondence delivery book.
12. The diplomatic courier, after having completed the delivery of the classified correspondence to the classified information offices of the receiving institutions in Prishtina, secures the diplomatic suitcase together with the classified information correspondence delivery book in his office, in a safe or closet metal safe.
13. It is forbidden to send materials and other items, during international transportation with classified correspondence from state institutions in Prishtina, to relevant structures abroad and vice versa.

**Article 18**  
**Exchange of information with states and international organizations**

If classified information is exchanged with other countries or international organizations, agreements or protocols may also define standards or other requirements for the security of information networks, means of exchange equipment, interconnection of systems, cryptographic protection of classified information.

**Article 19**  
**Final provisions**

The Agency for the Protection of Classified Information is obliged to supervise the implementation of this regulation.

**Article 20**  
**Repeal**

Upon entry into force of this regulation, the Regulation no. 14/2011 on Physical Security of Classified Information.

**Article 21**  
**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**