

**DEFENSE**

**Security of Information**

**Agreement Between the  
UNITED STATES OF AMERICA  
and KOSOVO**

Signed at Pristina August 24, 2023

Entered into force August 24, 2023



NOTE BY THE DEPARTMENT OF STATE

Pursuant to Public Law 89—497, approved July 8, 1966  
(80 Stat. 271; 1 U.S.C. 113)—

“ . . .the Treaties and Other International Acts Series issued under the authority of the Secretary of State shall be competent evidence . . . of the treaties, international agreements other than treaties, and proclamations by the President of such treaties and international agreements other than treaties, as the case may be, therein contained, in all the courts of law and equity and of maritime jurisdiction, and in all the tribunals and public offices of the United States, and of the several States, without any further proof or authentication thereof.”

**AGREEMENT BETWEEN  
THE GOVERNMENT OF THE UNITED STATES OF AMERICA  
AND  
THE GOVERNMENT OF THE REPUBLIC OF KOSOVO  
CONCERNING SECURITY MEASURES FOR THE PROTECTION OF  
CLASSIFIED INFORMATION**

**PREAMBLE**

The Government of the United States of America (the “United States”) and the Government of the Republic of Kosovo (“Kosovo”) (each a “Party,” and collectively the “Parties”),

Considering that the Parties cooperate in matters including, but not limited to, foreign affairs, defense, security, law enforcement, science, industry, and technology, and

Having a mutual interest in the protection of Classified Information exchanged in confidence between the Parties,

Have agreed as follows:

**ARTICLE 1 – DEFINITIONS**

For the purpose of this Agreement:

1. Classified Information: Information provided by one Party to the other Party that is designated as classified by the releasing Party for national security purposes and therefore requires protection against unauthorized disclosure. The information may be in oral, visual, electronic, or documentary form, or in the form of material, including equipment or technology.
2. Classified Contract: A contract that requires, or will require, access to, or production of, Classified Information by a Contractor or by its employees in the performance of the contract.
3. Contractor: An individual or a legal entity, possessing the legal capacity to conclude contracts, who is a party to a Classified Contract.
4. Facility Security Clearance: A certification provided by the National Security Authority of a Party, as designated in Article 4, for a Contractor facility under the Party’s jurisdiction that indicates the facility is cleared to a specified level and also has suitable security safeguards in place at a specified level to safeguard Classified Information. Such a certification shall signify that Classified Information at the CONFIDENTIAL / KONFIDENCIALE level or above shall be protected by the Contractor for which the Facility Security Clearance (FSC) is provided in accordance with the provisions of this Agreement and that compliance shall be monitored and enforced by the relevant National Security Authority. An FSC is not required for a Contractor to undertake Contracts that only require the receipt or production of Classified Information at the E KUFIZUAR level.

5. Personnel Security Clearance (PSC):

a. A determination by the National Security Authority of a Party, as designated in Article 4, that an individual who is employed by a government agency of that Party or a Contractor under the jurisdiction of that Party is authorized to access Classified Information up to a specified level.

b. A determination by the National Security Authority of a Party, as designated in Article 4, that an individual who is a citizen of one Party but is to be employed by the other Party or by one of the other Party's Contractors is authorized access to Classified Information up to a specified level.

6. Need to Know: A determination made by an authorized holder of Classified Information that a prospective recipient of Classified Information requires access to specific Classified Information in order to perform or assist in a lawful and authorized governmental function.

**ARTICLE 2 – LIMITATIONS ON SCOPE OF THE AGREEMENT**

This Agreement shall not apply to Classified Information within the scope of the terms of another agreement or arrangement between the Parties or agencies thereof providing for the protection of a particular item or category of Classified Information exchanged between the Parties or agencies thereof, except to the extent that such other agreement or arrangement expressly makes this Agreement's terms applicable. This Agreement also shall not apply to the exchange of Restricted Data, as defined in the U.S. Atomic Energy Act of 1954, as amended (the "AEA"), or to Formerly Restricted Data, which is data removed from the Restricted Data category in accordance with the AEA but still considered to be defense information by the United States.

**ARTICLE 3 – COMMITMENT TO THE PROTECTION OF CLASSIFIED INFORMATION**

1. Each Party shall protect Classified Information of the other Party according to the terms set forth herein.

2. Classified Information shall be protected by the recipient Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party.

3. Each Party shall promptly notify the other of any changes to its laws and regulations that would affect the protection of Classified Information under this Agreement. The obligations in this Agreement shall not be affected by such changes in domestic law. In such cases, the Parties shall consult regarding possible amendments to this Agreement or other measures that may be appropriate to maintain protection of Classified Information exchanged under this Agreement.

**ARTICLE 4 – NATIONAL SECURITY AUTHORITIES**

1. The Parties shall inform each other of the National Security Authorities responsible for implementation of this Agreement and any subsequent changes to these Authorities.

2. For the purpose of this Agreement, the National Security Authorities shall be:

a. for the United States: Assistant Director, International Engagement Directorate, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy, U.S. Department of Defense.

b. for the Republic of Kosovo: Kosovo Intelligence Agency/Security Vetting Department.

3. The Parties may conclude supplemental implementing arrangements to this Agreement where additional technical security measures may be required to protect Classified Information transferred to the recipient Party through foreign military sales or cooperative programs for co-production or co-development of defense articles or services. Such implementing arrangements may include Special Security Agreements or Industrial Security Agreements.

#### **ARTICLE 5 – DESIGNATION OF CLASSIFIED INFORMATION**

1. Classified Information shall be designated, and stamped or marked where possible, by the releasing Party as classified at one of the following national security classification levels. For purposes of ensuring equivalent treatment, the Parties agree that the following security classification levels are equivalent:

<b>UNITED STATES</b>	<b>KOSOVO</b>
TOP SECRET	TEPËR SEKRET
SECRET	SEKRET
CONFIDENTIAL	KONFIDENCIALE
No equivalent	E KUFIZUAR

2. During the implementation of this Agreement, if Kosovo provides Classified Information designated as “E KUFIZUAR,” the United States shall handle it in accordance with the Appendix to this Agreement.

3. Classified Information shall be designated, and stamped or marked where possible, with the name of the releasing Party.

#### **ARTICLE 6 – RESPONSIBILITY FOR CLASSIFIED INFORMATION**

The recipient Party shall be responsible for the protection of all Classified Information of the releasing Party in a manner that is at least equivalent to the protection afforded to Classified Information by the releasing Party while the Classified Information is under its control. While in transit, the releasing Party shall be responsible for all Classified Information until custody of the Classified Information is formally transferred to the recipient Party.

## **ARTICLE 7 – PROTECTION OF CLASSIFIED INFORMATION**

1. No individual shall be entitled to have access to Classified Information solely by virtue of rank, position, appointment, or PSC. Access to such information shall be granted only to individuals who have a Need to Know and who have been granted the requisite PSC in accordance with the prescribed standards of the recipient Party.
2. Except as otherwise provided in this Agreement, the recipient Party shall not release Classified Information of the releasing Party to any third party, including any third-party government, individual, firm, institution, organization, or other entity, without the prior written consent of the releasing Party.
3. The recipient Party shall not use or permit the use of Classified Information of the releasing Party for any other purpose than that for which it was provided without the prior written consent of the releasing Party.
4. The recipient Party shall respect any private rights that are associated with Classified Information of the releasing Party, including those rights with respect to patents, copyrights, or trade secrets, and shall not release, use, exchange, or disclose such Classified Information in a manner inconsistent with those rights without the prior written authorization of the owner of those rights.
5. The recipient Party shall ensure that each facility or establishment that handles Classified Information covered by this Agreement maintains a list of individuals at the facility or establishment who are authorized to have access to such information.
6. Each Party shall develop accountability and control procedures to manage the dissemination of, and access to, Classified Information.
7. Each Party shall comply with any and all limitations on use, disclosure, release, and access to Classified Information as may be specified by the releasing Party when it discloses such Classified Information. If a Party is unable to comply with the specified limitations, that Party shall immediately consult with the other Party and shall undertake all lawful measures to prevent or minimize any such use, disclosure, release, or access.

## **ARTICLE 8 – PERSONNEL SECURITY CLEARANCES**

1. The Parties shall ensure that all individuals who in the conduct of their official duties require access or whose duties or functions may afford access to Classified Information pursuant to this Agreement receive an appropriate PSC before they are granted access to such information.
2. The Party granting the PSC shall conduct an appropriate investigation in sufficient detail to determine an individual's suitability for access to Classified Information. The determination to grant a PSC will be made in accordance with the national laws and regulations of the granting Party.

3. Before an official or representative of one Party releases Classified Information to an official or representative of the other Party, the recipient Party shall provide to the releasing Party an assurance that the official or representative has the necessary PSC level and a Need to Know and that the Classified Information will be protected by the recipient Party in accordance with this Agreement.

#### **ARTICLE 9 – RELEASE OF CLASSIFIED INFORMATION TO CONTRACTORS**

1. Classified Information received by a recipient Party may be provided by the recipient Party to a Contractor or prospective Contractor whose duties require access to such information with the prior written consent of the releasing Party. Prior to releasing any Classified Information to a Contractor or prospective Contractor, the recipient Party shall:

a. Confirm that such Contractor or prospective Contractor and the Contractor's facility have the capability to safeguard the information in accordance with the terms of this Agreement;

b. Confirm that such Contractor or prospective Contractor and the Contractor's facility have been granted appropriate PSCs and FSCs, as applicable;

c. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that all individuals having access to the information are informed of their responsibilities to protect the information in accordance with applicable laws and regulations;

d. Carry out periodic security inspections of cleared facilities to ensure that the information is protected as required by this Agreement; and,

e. Confirm that the Contractor or prospective Contractor has procedures in place to ensure that access to the information is limited to those individuals who have a Need to Know.

#### **ARTICLE 10 – CLASSIFIED CONTRACTS**

1. When a Party proposes to place, or authorizes a Contractor in its country to place, a Classified Contract that is classified at the CONFIDENTIAL / KONFIDENCIALE level or above, with a Contractor in the country of the other Party, the Party that is to place or authorize the Contractor to place such Classified Contract shall request an assurance that an FSC has been issued from the National Security Authority of the other Party. The National Security Authority of the requested Party shall monitor and take all appropriate steps to ensure the security conduct by the Contractor will be in accordance with applicable laws and regulations.

2. The National Security Authority of a Party negotiating a Classified Contract to be performed in the country of the other Party shall incorporate in the Classified Contract, request for proposal, or subcontract document appropriate security clauses and other relevant provisions, including costs for security. This includes provisions requiring any Contractors to include appropriate security clauses in their subcontract documents.

## **ARTICLE 11 – RESPONSIBILITY FOR FACILITIES**

Each Party shall be responsible for the security of all government and private facilities and establishments where it stores Classified Information of the other Party and shall ensure that such facilities or establishments have qualified and appropriately cleared individuals appointed with the responsibility and authority for the control and protection of such information.

## **ARTICLE 12 – STORAGE OF CLASSIFIED INFORMATION**

Classified Information exchanged between the Parties shall be stored in a manner that ensures access only by those individuals who have been authorized access.

## **ARTICLE 13 – TRANSMISSION**

1. Classified Information shall be transmitted between the Parties through government-to-government channels or other channels mutually approved in advance in writing.

2. The minimum requirements for the security of Classified Information during transmission shall be as follows:

a. Documents or other media:

(1) Documents or other media containing Classified Information shall be transmitted in double, sealed envelopes. The inner envelope shall indicate only the classification of the documents or other media and the organizational address of the intended recipient. The outer envelope shall indicate the organizational address of the intended recipient, the organizational address of the sender, and the document control number, if applicable.

(2) No indication of the classification of the enclosed documents or other media shall be made on the outer envelope. The double sealed envelope shall be transmitted according to the prescribed procedures of the Parties.

(3) Receipts shall be prepared by the recipient for packages containing documents or other media containing Classified Information that are transmitted between the Parties, and such receipts shall be signed by the final recipient and returned to the sender.

b. Material:

(1) Material, including equipment, that contains Classified Information shall be transported in sealed, covered vehicles, or shall otherwise be securely packaged or protected in order to prevent identification of its shape, size, or contents, and kept under continuous control to prevent access by unauthorized persons.

(2) Material, including equipment, that contains Classified Information that must be stored temporarily awaiting shipment shall be placed in protected storage areas. Such areas shall be protected by intrusion detection equipment or guards with requisite PSCs who shall maintain



continuous surveillance of those areas. Only authorized personnel with the requisite PSC shall have access to the protected storage areas.

(3) Receipts shall be obtained whenever material that contains Classified Information, including equipment, changes hands during transit, and a receipt for such material shall be signed by the final recipient and returned to the sender.

c. Electronic transmissions:

(1) Classified Information that is classified at the CONFIDENTIAL / KONFIDENCIALE level or above that is to be transferred electronically shall be transmitted using secure means that have been approved by each Party's National Security Authority.

**ARTICLE 14 – VISITS TO FACILITIES AND ESTABLISHMENTS OF THE PARTIES**

1. Visits by representatives of one Party to facilities and establishments of the other Party that require access to Classified Information, or visits for which a PSC is required to permit access, shall be limited to those necessary for official purposes. Authorization shall only be granted to representatives who possess a valid PSC.

2. Authorization to visit such facilities and establishments shall be granted only by the Party in whose territory the facility or establishment to be visited is located. The visited Party, or its designated officials, shall be responsible for advising the facility or establishment of the proposed visit, and the scope and highest level of Classified Information that may be furnished to the visitor.

3. Requests for visits by representatives of the Parties shall be submitted by the Embassy of the United States in Pristina in the case of U.S. visitors, and by the Embassy of Kosovo in Washington, D.C., in the case of Kosovo visitors.

**ARTICLE 15 – SECURITY VISITS**

Implementation of security requirements set out in this Agreement may be verified through reciprocal visits by security personnel of the Parties. The security representatives of each Party, after prior consultation, shall be permitted to visit the other Party to discuss and observe the implementing procedures of the other Party in the interest of achieving reasonable comparability of security systems. The host Party shall assist the visiting security representatives in determining whether Classified Information received from the other Party is being adequately protected.

**ARTICLE 16 – SECURITY STANDARDS**

On request, each Party shall provide the other Party with information about its security standards, practices, and procedures for safeguarding of Classified Information.

## **ARTICLE 17 – REPRODUCTION OF CLASSIFIED INFORMATION**

When Classified Information is reproduced, all of the original security markings thereon shall also be reproduced, stamped, or marked on each reproduction of such information. Such reproductions shall be subject to the same controls as the original information. The number of reproductions shall be limited to the minimum number required for official purposes.

## **ARTICLE 18 – DESTRUCTION OF CLASSIFIED INFORMATION**

1. Documents and other media containing Classified Information shall be destroyed by burning, shredding, pulping, or other means that prevent reconstruction of the Classified Information contained therein.
2. Material, including equipment, containing Classified Information shall be destroyed through means that render it no longer recognizable so as to preclude reconstruction of the Classified Information in whole or in part.

## **ARTICLE 19 – DOWNGRADING AND DECLASSIFICATION**

1. The Parties agree that Classified Information should be downgraded in classification as soon as the information ceases to require that higher degree of protection or should be declassified as soon as the information no longer requires protection against unauthorized disclosure.
2. The releasing Party has complete discretion concerning downgrading or declassification of its Classified Information. The recipient Party shall not downgrade the security classification or declassify Classified Information received from the releasing Party, notwithstanding any apparent declassification instructions on the document, without the prior written consent of the releasing Party.

## **ARTICLE 20 – LOSS OR COMPROMISE**

The recipient Party shall inform the releasing Party immediately upon discovery of all losses or compromises, as well as possible losses or compromises, of Classified Information of the releasing Party. In the event of an actual or possible loss or compromise of such information, the recipient Party shall initiate an investigation immediately to determine the circumstances of the actual or possible loss or compromise. The results of the investigation and information regarding measures taken to prevent recurrence shall be provided to the releasing Party.

## **ARTICLE 21 – DISPUTES**

Disagreements between the Parties arising under or relating to this Agreement shall be settled solely through consultations between the Parties and shall not be referred to a national court, an international tribunal, or any other person or entity for settlement.

**ARTICLE 22 – COSTS**

Each Party shall be responsible for bearing its own costs incurred in implementing this Agreement. All obligations of the Parties under this Agreement shall be subject to the availability of funds.


**ARTICLE 23 – FINAL PROVISIONS**

1. This Agreement shall enter into force upon the date of the last signature by the Parties.
2. Either Party may terminate this Agreement by notifying the other Party in writing through diplomatic channels ninety days in advance of its intention to terminate the Agreement.
3. Notwithstanding the termination of this Agreement, all Classified Information exchanged or otherwise provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.


**IN WITNESS WHEREOF**, the undersigned, being duly authorized thereto by their respective Governments, have signed this Agreement.

Done in duplicate in *Pristina* this *24* day of *August 2023* in the English, Albanian, and Serbian languages, each being equally authentic.

**FOR THE GOVERNMENT OF  
THE UNITED STATES OF AMERICA:**

  
\_\_\_\_\_  
Jeffrey M. Hovenier  
Ambassador

**FOR THE GOVERNMENT OF  
THE REPUBLIC OF KOSOVO:**

  
\_\_\_\_\_  
Albin Kurti  
Prime Minister

## APPENDIX

### PROCEDURES FOR PROTECTING KOSOVO E KUFIZUAR CLASSIFIED INFORMATION PROVIDED TO THE UNITED STATES

1. Upon receipt, Kosovo Classified Information provided to the United States and designated as “E KUFIZUAR” shall be protected by the United States in accordance with the following procedures.
2. Information designated as “E KUFIZUAR” shall be stored in locked containers or closed areas that prevent access by unauthorized personnel.
3. “E KUFIZUAR” information shall not be disclosed to unauthorized persons or entities without the prior written approval of the Government of Kosovo except as required by U.S. law, including the Freedom of Information Act.
4. “E KUFIZUAR” information shall, as applicable, be stored, processed, or transmitted electronically using government- or Contractor-accredited systems. In particular, before any system is used to store, process, or transmit “E KUFIZUAR” information, it must receive security approval, known as Accreditation. An Accreditation is a formal statement by the appropriate accrediting authority confirming that the use of a system meets the appropriate security requirements and does not present an unacceptable risk. Security Standard Operating Procedures are technical procedures to implement security policies and requirements unique to a specific facility to protect automated information systems processing Classified Information. For stand-alone automated information systems such as desktop and laptop computers utilized in U.S. Government establishments, the system registration document together with the Security Standard Operating Procedures shall fulfill the role of the required Accreditation. For Contractors, guidance on the use of communications and information systems shall be incorporated into the Restricted Conditions Requirements Clause in the Contract.
5. “E KUFIZUAR” information shall be transmitted by first class mail within the United States in one sealed envelope. Transmission outside the United States shall be in double, sealed envelopes, with the inner envelope marked “KOSOVO E KUFIZUAR.” Transmission outside the United States shall be by traceable means such as commercial courier or other means agreed upon by the Parties in writing.
6. U.S. documents that contain “KOSOVO E KUFIZUAR” information shall bear on the cover and the first page the marking “KOSOVO E KUFIZUAR.” The portion of the documents containing “KOSOVO E KUFIZUAR” information also shall be identified with the same marking.
7. “E KUFIZUAR” information may be transmitted or accessed electronically via a public network like the Internet using government or commercial encryption devices mutually accepted by the Parties. Telephone conversations, video conferencing, or facsimile transmissions containing “E KUFIZUAR” information may be conducted if an encryption system is not available and subject to the approval of the releasing Party’s National Security Authority.
8. An FSC is not required for a Contractor to undertake contracts that require only the receipt or production of Classified Information at the “E KUFIZUAR” level.

9. Access to such “E KUFIZUAR” information shall be granted only to those individuals who have a Need to Know. A PSC is not required to access “E KUFIZUAR” information.

**MARRËVESHJE NDËRMJET**  
**QEVERISË SË SHTETEVE TË BASHKUARA TË AMERIKËS**  
**DHE**  
**QEVERISË SË REPUBLIKËS SË KOSOVËS**  
**PËR MASAT E SIGURISË PËR MBROJTJEN E**  
**INFORMACIONIT TË KLASIFIKUAR**

**HYRJJE**

Qeveria e Shteteve të Bashkuara të Amerikës ("Shtetet e Bashkuara") dhe Qeveria e Republikës së Kosovës ("Kosova") (secila më vete "Pala" dhe së bashku "Palët"),

Duke pasur parasysh se Palët bashkëpunojnë në çështje që përfshijnë por që nuk kufizohen vetëm me politikën e jashtme, mbrojtjen, sigurinë, zbatimin e ligjit, shkencën, industrinë dhe teknologjinë, dhe

Duke pasur interes të ndërsjellë në mbrojtjen e Informacionit të Klasifikuar që shkëmbehet në mirëbesim midis Palëve,

Kanë rënë dakord si më poshtë:

**NENI 1 - PËRKUFIZIMET**

Për qëllim të kësaj Marrëveshjeje:

- 1. Informacion i Klasifikuar:** Informacioni që njëra Palë i ofron Palës tjetër dhe që emërtohet i klasifikuar nga Pala dhënëse për qëllime të sigurisë kombëtare dhe si rrjedhojë kërkon mbrojtje ndaj publikimit të paautorizuar. Ky informacion mund të jetë verbal, vizual, elektronik ose në formë dokumentesh ose materialesh, përfshi edhe pajisje ose teknologji.
- 2. Kontratë e klasifikuar:** Një kontratë që kërkon, ose do të kërkojë, qasje në, ose prodhim të, Informacionit të Klasifikuar nga një Kontraktor ose punonjësit e tij në zbatim të kontratës.
- 3. Kontraktor:** Një individ ose një entitet ligjor, që ka kapacitet ligjor për të përmbyllur kontrata, i cili është palë në një Kontratë të Klasifikuar.
- 4. Verifikim i sigurisë së objektit:** Një certifikatë që lëshohet nga Autoriteti i Sigurisë Kombëtare të një Pale, siç përcaktohet në Nenin 4, për një objekt kontraktues në juridiksionin e Palës që vërteton se objekti është verifikuar për një nivel të specifikuar dhe zbaton masat e duhura të mbrojtjes për nivelin e specifikuar të ruajtjes së Informacionit të Klasifikuar. Një certifikatë e tillë do të nënkuptojë se Informacioni i Klasifikuar në nivelin KONFIDENCIAL ose më lart do të mbrohet nga Kontraktori të cilit i është lëshuar Verifikimi i Sigurisë së Objektit (VSO) në përputhje me dispozitat e kësaj Marrëveshjeje dhe se përputhshmëria do të monitorohet dhe zbatohet nga Autoriteti përkatës i Sigurisë Kombëtare. Nuk kërkohet një VSO për një Kontraktor që ndërmerr kontrata që kërkojnë vetëm marrjen ose prodhimin e Informacionit të Klasifikuar në nivelin I KUFIZUAR.

## 5. Verifikim sigurie i personelit (VSP):

a. Një vendim nga Autoriteti i Sigurisë Kombëtare i një Pale, siç përcaktohet në Nenin 4, që një individ, i punësuar nga një agjenci qeveritare e asaj Pale ose një Kontraktor nën juridiksionin e asaj Pale autorizohet të ketë qasje në Informacionin e Klasifikuar deri në një nivel të specifikuar.

b. Një vendim nga Autoriteti i Sigurisë Kombëtare i një Pale, siç përcaktohet në Nenin 4, që një individ, i cili është shtetas i një Pale por që do të punësohet nga Pala tjetër ose nga Kontraktorë të Palës tjetër, autorizohet të ketë qasje në Informacionin e Klasifikuar deri në një nivel specifik.

6. Nevoja për të ditur: Një vendim i marrë nga një bartës i autorizuar i Informacionit të Klasifikuar që një marrës potencial i Informacionit të Klasifikuar kërkon qasje në një Informacion të Klasifikuar specifik për të kryer ose ndihmuar në një funksion të ligjshëm ose të autorizuar qeveritar.

## **NENI 2 - KUFIZIMET NË FUSHËVEPRIMIN E MARRËVESHJES**

Kjo Marrëveshje nuk do të aplikohet për Informacionin e Klasifikuar brenda fushëveprimit të kushteve të një marrëveshjeje ose akordi tjetër ndërmjet Palëve ose agjencive të tyre që sigurojnë mbrojtjen e një zëri ose kategorie të caktuar të Informacionit të Klasifikuar të shkëmbyer ndërmjet Palëve ose agjencive të tyre, përveç rasteve kur një marrëveshje ose akord i tillë shprehimisht i bën të aplikueshme kushtet e kësaj Marrëveshjeje. Gjithashtu kjo Marrëveshje nuk do të zbatohet për shkëmbimin e të Dhënave të Kufizuara, siç përcaktohet në amendamentin e Ligjit për Energjinë Atomike të SHBA të vitit 1954, ("AEA"), ose për të Dhënat e Vjetruara të Kufizuara që janë të dhëna të hequra nga kategoria e të Dhënave të Kufizuara në përputhje me AEA, por që ende konsiderohen si informacion i mbrojtur nga Shtetet e Bashkuara.

## **NENI 3 - ANGAZHIM PËR MBROJTJEN E INFORMACIONIT TË KLASIFIKUAR**

1. Secila Palë do të mbrojë Informacionin e Klasifikuar të Palës tjetër në përputhje me dispozitat e parashtruara si më poshtë.

2. Informacioni i Klasifikuar do të mbrohet nga Pala marrëse në një mënyrë që është së paku ekuivalente me mbrojtjen që i jepet Informacionit të Klasifikuar nga Pala dhënëse.

3. Secila Palë do të njoftojë menjëherë Palën tjetër për çdo ndryshim në ligjet dhe rregulloret e saj që mund të ndikojnë mbrojtjen e Informacionit të Klasifikuar sipas kësaj Marrëveshjeje. Detyrimet që rrjedhin nga kjo Marrëveshje nuk do të preken nga këto ndryshime në ligjet e brendshme. Në raste të tilla, Palët duhet të konsultohen në lidhje me amendamentet e mundshme të kësaj Marrëveshjeje ose masat e tjera që mund të jenë të përshtatshme për të ruajtur mbrojtjen e Informacionit të Klasifikuar të shkëmbyer sipas kësaj Marrëveshjeje.

#### **NENI 4 - AUTORITET E SIGURISË KOMBËTARE**

1. Palët do të informojnë njëra-tjetrën për Autoritetet e Sigurisë Kombëtare përgjegjëse për zbatimin e kësaj Marrëveshjeje dhe çdo ndryshim të mëvonshëm të këtyre Autoriteteve.

2. Për qëllim të kësaj Marrëveshjeje, Autoritetet e Sigurisë Kombëtare do të jenë:

a. Për Shtetet e Bashkuara: Ndihmës Drejtori, Drejtoria e Angazhimit Ndërkombëtar, Administrata e Sigurisë së Teknologjisë së Mbrojtjes, Zyra e Nënsekretarit të Mbrojtjes për Politikën, Departamenti Amerikan i Mbrojtjes.

b. Për Republikën e Kosovës: Agjencia e Inteligjencës së Kosovës/Departamenti i Vetingut të Sigurisë.

3. Palët mund të miratojnë rregullore plotësuese zbatuese ndaj kësaj Marrëveshjeje ku mund të kërkohen masa shtesë të sigurisë teknike për të mbrojtur Informacionin e Klasifikuar të transferuar tek Pala marrëse nga shitjet e pajisjeve ushtarake të huaja ose programet bashkëpunuese për bashkëprodhimin ose zhvillimin e përbashkët të artikujve ose shërbimeve të mbrojtjes. Rregullore të tilla zbatuese mund të përfshijnë Marrëveshje Speciale të Sigurisë ose Marrëveshje të Sigurisë Industriale.

#### **NENI 5 - EMËRTIMI I INFORMACIONIT TË KLASIFIKUAR**

1. Informacioni i Klasifikuar do të emërtohet dhe vuloset ose shënohet kur është e mundur, nga Pala dhënëse si i klasifikuar në një nga nivelet e mëposhtme të klasifikimit të sigurisë kombëtare. Për qëllim të garantimit të trajtimit të barabartë, Palët bien dakord që nivelet e mëposhtme të klasifikimit të sigurisë janë ekuivalente:

<b>SHTETET E BASHKUARA</b>	<b>KOSOVA</b>
TOP SECRET	TEPËR SEKRET
SECRET	SEKRET
CONFIDENTIAL	KONFIDENCIAL
No equivalent	I KUFIZUAR

2. Gjatë zbatimit të kësaj Marrëveshjeje, nëse Kosova ofron Informacion të Klasifikuar të emërtuar si "I KUFIZUAR", Shtetet e Bashkuara do ta trajtojnë atë në përputhje me Shtojcën e kësaj Marrëveshjeje.

3. Informacioni i Klasifikuar do të emërtohet, vuloset ose shënohet kur është e mundur, me emrin e Palës dhënëse.



## **NENI 6 - PËRGJEGJËSIA PËR INFORMACIONIN E KLASIFIKUAR**

Pala marrëse do të jetë përgjegjëse për mbrojtjen e të gjithë Informacionit të Klasifikuar të Palës dhënëse në një mënyrë që është të paktën ekuivalente me mbrojtjen që i jepet Informacionit të Klasifikuar nga Pala dhënëse ndërsa Informacioni i Klasifikuar është nën kontrollin e saj. Ndërsa ndodhet në tranzit, Pala dhënëse do të jetë përgjegjëse për të gjithë Informacionin e Klasifikuar derisa kujdestaria e Informacionit të Klasifikuar t'i transferohet zyrtarisht Palës marrëse.

## **NENI 7 - MBROJTJA E INFORMACIONIT TË KLASIFIKUAR**

1. Asnjë individ nuk do të ketë të drejtë të ketë qasje në Informacionin e Klasifikuar për shkak të gradës, pozicionit, emërimit ose VSP. Qasja në një informacion të tillë do t'u lejohe vetëm individëve që kanë Nevojë për të Ditur dhe që janë pajisur me VSP përkatëse në përputhje me standardet e përcaktuara të Palës marrëse.

2. Me përjashtim të rasteve kur parashikohet ndryshe në këtë Marrëveshje, Pala marrëse nuk do t'ia kalojë Informacionin e Klasifikuar nga Pala dhënëse asnjë pale të tretë, përfshirë çdo qeverie, individ, firmë, institucion, organizatë ose entiteti tjetër të një pale të tretë, pa pëlqimin paraprak me shkrim të Palës dhënëse.

3. Pala marrëse nuk do të përdorë ose lejojë përdorimin e Informacionit të Klasifikuar të Palës dhënëse për ndonjë qëllim tjetër përveç atij për të cilin është ofruar, pa pëlqimin paraprak me shkrim të Palës dhënëse.

4. Pala marrëse do të respektojë çdo të drejtë private që lidhet me Informacionin e Klasifikuar të Palës dhënëse, përfshirë të drejta në lidhje me patentat, të drejtat e autorit ose sekretet tregtare, dhe nuk do të publikojë, përdorë, shkëmbejë ose zbulojë një informacion të tillë të Klasifikuar në mospërputhje me këto të drejta pa një autorizim paraprak me shkrim të pronarit të këtyre të drejtave.

5. Pala marrëse do të sigurojë që çdo objekt ose institucion që trajton Informacionin e Klasifikuar të mbuluar nga kjo Marrëveshje të ketë një listë të individëve në objekt ose institucion që janë të autorizuar të kenë qasje në një informacion të tillë.

6. Secila Palë do të zhvillojë procedurat e përgjegjësive dhe kontrollit për të menaxhuar shpërndarjen dhe qasjen në Informacionin e Klasifikuar.

7. Secila Palë do të respektojë çdo dhe të gjitha kufizimet për përdorimin, zbulimin, publikimin dhe qasjen në Informacionin e Klasifikuar siç mund të specifikohet nga Pala dhënëse kur ajo zbulon një informacion të tillë të Klasifikuar. Nëse një Palë nuk është në gjendje të përmbushë kufizimet e specifikuara, kjo Palë do të konsultohet menjëherë me Palën tjetër dhe do të ndërmarrë të gjitha masat ligjore për të parandaluar ose minimizuar çdo përdorim, zbulim, publikim ose qasje të tillë.

## **NENI 8 - VERIFIKIMI I SIGURISË SË PERSONELIT**

1. Palët do të sigurojnë që të gjithë individët, të cilët gjatë kryerjes së detyrave të tyre zyrtare kërkojnë qasje ose detyrat ose funksionet e të cilëve mund të lejojnë qasje në Informacionin e Klasifikuar në përputhje me këtë Marrëveshje, të pajisen me VSP-në e duhur përpara se t'u lejohej qasja në një informacion të tillë.

2. Pala që lëshon VSP-në do të kryejë një hetim të përshtatshëm me hollësi të mjaftueshme për të përcaktuar përshtatshmërinë e një individi për qasje në Informacionin e Klasifikuar. Vendimi për të lëshuar një VSP do të merret në përputhje me ligjet dhe rregulloret kombëtare të Palës dhënëse.

3. Përpara se një zyrtar ose përfaqësues i njërës Palë t'i japë Informacion të Klasifikuar një zyrtari ose përfaqësuesi të Palës tjetër, Pala marrëse do t'i paraqesë Palës dhënëse një garanci se zyrtari ose përfaqësuesi ka nivelin e nevojshëm të VSP-së dhe Nevojën për të Ditur dhe se Informacioni i Klasifikuar do të mbrohet nga Pala marrëse në përputhje me këtë Marrëveshje.

## **NENI 9 - LËSHIMI I INFORMACIONIT TË KLASIFIKUAR PËR KONTRAKTORËT**

1. Informacioni i Klasifikuar i marrë nga një Palë marrëse mund t'i jepet nga Pala marrëse një Kontraktori ose Kontraktori të mundshëm, detyrat e të cilit kërkojnë qasje në një informacion të tillë me pëlqimin paraprak me shkrim të Palës dhënëse. Përpara lëshimit të çdo informacioni të klasifikuar një kontraktori ose kontraktori të mundshëm, Pala marrëse do të:

a. Konfirmojë se ky Kontraktor ose Kontraktori i mundshëm dhe objekti i Kontraktorit kanë kapacitete të mbrojnë informacionin në përputhje me dispozitat e kësaj Marrëveshjeje;

b. Konfirmojë që këtij Kontraktori ose Kontraktorit të mundshëm dhe objektit të Kontraktorit i është lëshuar një VSP dhe VSO e përshtatshme, sipas ligjit;

c. Konfirmojë që Kontraktori ose Kontraktori i mundshëm ka zbatuar procedurat për të garantuar që të gjithë individët që kanë qasje në informacion të informohen për përgjegjësitë e tyre për të mbrojtur informacionin në përputhje me ligjet dhe rregulloret në fuqi;

d. Kryejë inspektime periodike të sigurisë së objekteve të verifikuara për të siguruar që informacioni është i mbrojtur siç kërkohet nga kjo Marrëveshje; dhe,

e. Konfirmojë që Kontraktori ose Kontraktori i mundshëm ka zbatuar procedurat për të siguruar që qasja në informacion të jetë e kufizuar vetëm për ata individë që kanë Nevojë për të Ditur.

## **NENI 10 - KONTRATA TË KLASIFIKUARA**

1. Kur një Palë propozon të lidhë, ose të autorizojë një Kontraktor të vendit të saj të lidhë një Kontratë të klasifikuar në nivelin KONFIDENCIAL ose më lart, me një Kontraktor në vendin e Palës tjetër, Pala që do të lidhë ose do të autorizojë Kontraktorin të lidhë një Kontratë të tillë të Klasifikuar, do të kërkojë afirmimin se Autoriteti i Sigurisë Kombëtare të Palës tjetër ka lëshuar

një VSO. Autoriteti i Sigurisë Kombëtare i Palës kërkuese do të monitorojë dhe do të marrë të gjithë hapat e duhur për të siguruar që masat e sigurisë nga Kontraktori të jenë në përputhje me ligjet dhe rregulloret në fuqi.

2. Autoriteti i Sigurisë Kombëtare i një Pale që negocion një Kontratë të Klasifikuar që do të zbatohet në vendin e Palës tjetër do të përfshijë në Kontratën e Klasifikuar, kërkesën për propozim ose klauzola dhe dispozita të tjera të përshtatshme për dokumentim të nën kontraktimit, përfshirë kostot për sigurinë. Kjo përfshin dispozitat që kërkojnë që çdo Kontraktor të përfshijë klauzola të përshtatshme sigurie në dokumentet e nënkontratës.

### **NENI 11 - PËRGJEGJËSIA PËR OBJEKTET**

Secila Palë do të jetë përgjegjëse për sigurinë e të gjitha objekteve dhe institucioneve qeveritare dhe objekteve private ku ruhet Informacioni i Klasifikuar i Palës tjetër dhe do të sigurojë që objekte ose institucione të tilla të kenë individë të kualifikuar dhe të verifikuar përshtatshëm të caktuar me përgjegjësinë dhe autoritetin për kontrollin dhe mbrojtjen e një informacioni të tillë.

### **NENI 12 - RUAJTJA E INFORMACIONIT TË KLASIFIKUAR**

Informacioni i klasifikuar i shkëmbyer ndërmjet Palëve do të ruhet në një mënyrë që siguron qasje vetëm nga ata individë të cilët kanë qasje të autorizuar.

### **NENI 13 - TRANSFERIMI**

1. Informacioni i klasifikuar do të transferohet nga njëra Palë te Pala tjetër nëpërmjet kanaleve qeveritare ose kanaleve të tjera të miratuara paraprakisht me shkrim.

2. Kërkesat minimale për sigurinë e Informacionit të Klasifikuar gjatë transferimit do të jenë si më poshtë:

a. Dokumente ose media të tjera:

(1) Dokumentet ose media të tjera që përmbajnë Informacion të Klasifikuar do të transferohen në zarfe të dyfishtë, të vulosur. Zarfi i brendshëm do të tregojë vetëm klasifikimin e dokumenteve ose mediave të tjera dhe adresën e institucionit të marrësit të synuar. Zarfi i jashtëm do të tregojë adresën e institucionit të marrësit të synuar, adresën e institucionit të dërguesit dhe numrin e kontrollit të dokumentit, nëse është i aplikueshëm.

(2) Në zarfin e jashtëm nuk duhet të vendoset asnjë tregues klasifikimi i dokumenteve të bashkangjitura ose mediave të tjera. Zarfi i dyfishtë i vulosur do të transferohet sipas procedurave të përcaktuara nga Palët.

(3) Do të përgatiten dëftesa vërtetimi nga marrësi për pakot që përmbajnë dokumente ose media të tjera me Informacion të Klasifikuar që transferohen nga njëra Palë te tjetra. Këto dëftesa do të nënshkruhen nga marrësi përfundimtar dhe do t'i kthehen dërguesit.

b. Materialet:

(1) Materialet, përfshirë pajisjet, që përmbajnë Informacion të Klasifikuar, do të transportohen në automjete të vulosura, të mbuluara, ose do të paketohen ose mbrohen në mënyrë të sigurt për të parandaluar identifikimin e formës, madhësisë ose përmbajtjes së tyre dhe do të mbahen nën kontroll të vazhdueshëm për të parandaluar qasjen nga persona të paautorizuar.

(2) Materialet, përfshirë pajisjet, që përmbajnë Informacion të Klasifikuar që duhet të ruhen përkohësisht në pritje për tu dërguar, do të vendosen në zona të mbrojtura ruajtjeje. Këto zona do të mbrohen nga pajisje për zbulimin e ndërhyrjeve ose me roje me VSP-të të përshtatshme, të cilët do të mbajnë në mbikëqyrje të vazhdueshme këto zona. Vetëm personeli i autorizuar me VSP-në e nevojshme do të ketë qasje në zonat e mbrojtura të ruajtjes.

(3) Dëftesa vërtetimi do të merren sa herë që materiali që përmban Informacion të Klasifikuar, përfshirë edhe pajisjet, ndryshon kujdestari gjatë tranzitit dhe një dëftesë për këtë material duhet të nënshkruhet nga marrësi përfundimtar dhe t'i kthehet dërguesit.

#### c. Transmetimet elektronike:

(1) Informacion i Klasifikuar në nivelin KONFIDENCIAL ose më lart që do të transferohet elektronikisht, do të transmetohet duke përdorur mjete të sigurta që janë miratuar nga Autoriteti i Sigurisë Kombëtare i secilës Palë.

### **NENI 14 - VIZITAT NË OBJEKTET DHE INSTITUCIONET E PALËVE**

1. Vizitat nga përfaqësuesit e njërës Palë në objektet dhe institucionet e Palës tjetër që kërkojnë qasje në Informacionin e Klasifikuar, ose vizitat për të cilat kërkohet një VSO për të lejuar qasjen, do të kufizohen tek vizitat e nevojshme për qëllime zyrtare. Autorizimi do tu jepet përfaqësuesve që kanë një VSP të vlefshme.

2. Autorizimi për të vizituar këto objekte dhe institucione do të jepet vetëm nga Pala në territorin e së cilës ndodhet objekti ose institucioni që do të vizitohet. Pala që viziton, ose zyrtarët e caktuar prej saj, kanë për detyrë të njoftojnë objektin ose institucionin për vizitën e paramenduar, si dhe për shtrirjen dhe nivelin më të lartë të Informacionit të Klasifikuar që mund t'i jepet vizitorit.

3. Kërkesat për vizita nga përfaqësuesit e Palëve do të dorëzohen nga Ambasada e Shteteve të Bashkuara në Prishtinë në rastin e vizitorëve amerikanë dhe nga Ambasada e Kosovës në Uashington, D.C., në rastin e vizitorëve të Kosovës.

### **NENI 15 - SIGURIA E VIZITAVE**

Zbatimi i kërkesave të sigurisë të parashtruara në këtë Marrëveshje mund të verifikohet nëpërmjet vizitave reciproke nga personeli i sigurisë së Palëve. Përfaqësuesit e sigurisë të secilës Palë, pas konsultimeve paraprake, do të lejohen të vizitojnë Palën tjetër për të diskutuar dhe vëzhguar procedurat që zbatohen nga Pala tjetër me qëllim arritjen e një ngjashmërie të arsyeshme të

sistemeve të sigurisë. Pala pritëse do të ndihmojë përfaqësuesit vizitorë të sigurisë të përcaktojnë nëse Informacioni i Klasifikuar i marrë nga Pala tjetër mbrohet në mënyrën e duhur.

#### **NENI 16 - STANDARDET E SIGURISË**

Sipas kërkesës, secila Palë do t'i japë Palës tjetër informacion për standardet, praktikat dhe procedurat e sigurisë lidhur me mbrojtjen e Informacionit të Klasifikuar.

#### **NENI 17 - RIPRODHIMI I INFORMACIONIT TË KLASIFIKUAR**

Kur riprodhohet Informacion i Klasifikuar, të gjitha shenjat origjinale të sigurisë që ndodhen në to duhet të riprodhohen, vulosen dhe shënohen në çdo riprodhim të një informacioni të tillë. Riprodhime të tilla duhet të jenë subjekt i të njëjtave masa kontrolli si dhe informacioni origjinal. Numri i riprodhimeve do të kufizohet në numrin minimum të kërkuar për qëllime zyrtare.

#### **NENI 18 - SHKATËRRIMI I INFORMACIONIT TË KLASIFIKUAR**

1. Dokumentet dhe mjetet e tjera që përmbajnë Informacion të Klasifikuar do të shkatërrohen duke u djegur, copëzuar, brumuar ose me mënyra të tjera që nuk do të lejojnë mundësinë për rindërtimin e Informacionit të Klasifikuar që përmbahet aty.

2. Materialet, duke përfshirë pajisjet, që përmbajnë Informacion të Klasifikuar do të shkatërrohen me mënyra që i bëjnë ato të papërdorshme me qëllim që të parandalohet rindërtimi tërësisht ose pjesërisht i Informacionit të Klasifikuar.

#### **NENI 19 - DEGRADIMI DHE DEKLASIFIKIMI**

1. Palët bien në ujdë që Informacioni i Klasifikuar duhet të degradohet në klasifikim sa më shpejt pasi informacioni pushon së kërkuari një shkallë më të lartë mbrojtjeje ose duhet të deklasifikohet sa më shpejt kur informacioni nuk kërkon më mbrojtje nga një publikim i paautorizuar.

2. Pala dhënëse ka diskrecion të plotë në lidhje me degradimin ose deklasifikimin e informacionit të saj të klasifikuar. Pala marrëse nuk do të degradojë klasifikimin e sigurisë ose nuk do të deklasifikojë informacionin e klasifikuar të marrë nga Pala dhënëse, pavarësisht ndonjë udhëzimi të qartë deklasifikimi në dokument, pa miratimin paraprak me shkrim të Palës dhënëse.

#### **NENI 20 - HUMBJA OSE KOMPROMENTIMI**

Pala marrëse do të informojë Palën dhënëse menjëherë pas zbulimit të të gjitha humbjeve ose komprometimeve, si dhe humbjeve ose komprometimeve të mundshme, të informacionit të klasifikuar të Palës dhënëse. Në rast të një humbjeje ose komprometimi të ndodhur ose të mundshëm të një informacioni të tillë, Pala marrëse do të fillojë menjëherë një hetim për të përcaktuar rrethanat e humbjes ose komprometimit të ndodhur ose të mundshëm. Rezultatet e hetimit dhe informacioni në lidhje me masat e marra për të parandaluar përsëritjen do t'i njoftohen Palës dhënëse.

## NENI 21 - MOSMARRËVESHJET

Mosmarrëveshjet ndërmjet Palëve që lindin ose lidhen me këtë Marrëveshje do të zgjidhen vetëm nëpërmjet konsultimeve ndërmjet Palëve dhe nuk do t'i referohen për zgjidhje një gjykate kombëtare, një gjykate ndërkombëtare ose ndonjë personi ose subjekti tjetër.

## NENI 22 - KOSTOT

Secila Palë do të jetë përgjegjëse për bartjen e kostos që rrjedh nga zbatimi i kësaj Marrëveshjeje. Të gjitha detyrimet e Palëve sipas kësaj Marrëveshjeje do t'i nënshtrohen disponueshmërisë së fondeve.

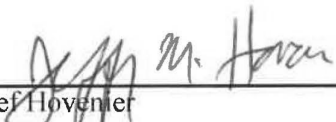
## NENI 23 - DISPOZITAT PËRFUNDIMTARE

1. Kjo Marrëveshje hyn në fuqi në datën e nënshkrimit përfundimtar nga Palët.
2. Secila Palë mund ta përfundojë këtë Marrëveshje duke njoftuar Palën tjetër me shkrim nëpërmjet kanaleve diplomatike, nëntëdhjetë ditë përpara për qëllimin e saj për të përfunduar Marrëveshjen.
3. Pavarësisht përfundimit të kësaj Marrëveshjeje, i gjithë Informacioni i Klasifikuar, i shkëmbyer ose i dhënë në përputhje me këtë Marrëveshje, do të vazhdojë të jetë i mbrojtur në përputhje me dispozitat e përcaktuara sa më lart.

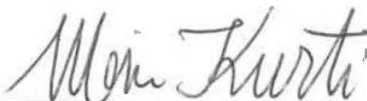
**NË CILËSI TË DËSHMITARËVE**, nënshkruesit e mëposhtëm, të autorizuar sipas detyrës nga qeveritë e tyre përkatëse, kanë nënshkruar këtë Marrëveshje.

Hartuar në dy kopje në Prishtinë më 24 të gusht, 2023, në gjuhën angleze, shqipe dhe serbe, tekstet në secilën gjuhë janë njëllorj autentikë.

**PËR QEVERINË E  
SHTETEVE TË BASHKUARA  
TË AMERIKËS:**

  
Xhef Hovenet  
Ambassador

**PËR QEVERINË E  
RËPUBLIKËS SË KOSOVËS:**

  
Albin Kurti  
Kryeministër

## SHTOJCË

### PROCEDURAT PËR MBROJTJEN E INFORMACIONIT TË KLASIFIKUAR TË KUFIZUAR DHËNË SHTETEVE TË BASHKUARA

1. Pas marrjes, Informacioni i Klasifikuar i Kosovës i dhënë Shteteve të Bashkuara dhe i përcaktuar si "I KUFIZUAR" do të mbrohet nga Shtetet e Bashkuara në përputhje me procedurat e mëposhtme.
2. Informacioni i përcaktuar si "I KUFIZUAR" do të ruhet në objekte të mbyllur ose zona të mbyllura që ndalojnë hyrjen e personelit të paautorizuar.
3. Informacioni "I KUFIZUAR" nuk do t'u zbulohet personave ose subjekteve të paautorizuara pa miratimin paraprak me shkrim nga Qeveria e Kosovës, me përjashtim kur parashikohet nga ligji i SHBA-së, duke përfshirë Aktin e Lirisë së Informacionit.
4. Informacioni "I KUFIZUAR", sipas rastit, do të ruhet, përpunohet ose transmetohet në mënyrë elektronike duke përdorur sisteme të akredituara qeveritare ose nga Kontraktori. Në veçanti, përpara se çdo sistem të përdoret për të ruajtur, përpunuar ose transmetuar informacionin "I KUFIZUAR", ai duhet të ketë marrë miratimin e sigurisë, i njohur si Akreditim. Akreditimi është një deklaratë zyrtare nga autoriteti përkatës akreditues që konfirmon se përdorimi i një sistemi plotëson kërkesat përkatëse të sigurisë dhe nuk paraqet një rrezik të papranueshëm. Procedurat Operuese Standarde të Sigurisë janë procedura teknike për zbatimin e politikave dhe kërkesave të sigurisë unike për një strukturë specifike për të mbrojtur sistemet e automatizuara të informacionit që përpunojnë Informacionin e Klasifikuar. Për sistemet e shkëputura (stand-alone) të automatizuara të informacionit, të tilla si kompjuterët desktop dhe laptopët që përdoren në institucionet e Qeverisë së SHBA-së, dokumenti i regjistrimit të sistemit së bashku me Procedurat Operative Standarde të Sigurisë do të përmbushin rolin e Akreditimit të kërkuar. Për Kontraktorët, udhëzimet për përdorimin e sistemeve të komunikimit dhe informacionit do të përfshihen në Klauzolën e Kërkesave për Kushte të Kufizuara në Kontratë.
5. Informacioni "I KUFIZUAR" do të transferohet me postë të klasës së parë brenda Shteteve të Bashkuara në një zarf të vulosur. Dërgesat jashtë Shteteve të Bashkuara do të bëhen në zarfe të dyfishtë, të vulosur, ku në zarfin e brendshëm shënohet "KOSOVA I KUFIZUAR". Dërgesat jashtë Shteteve të Bashkuara do të bëhet me mjete të gjurmueshme, të tilla si korrier komercial ose mjete të tjera të rëna dakord nga Palët me shkrim.
6. Dokumentet e Shteteve të Bashkuara që kanë shënimin informacion "KOSOVA I KUFIZUAR" do të kenë shënim në kopertinë dhe faqen e parë "KOSOVA I KUFIZUAR". Pjesa e dokumenteve që përmban informacionin "KOSOVA I KUFIZUAR" gjithashtu duhet të identifikohet me të njëjtën shenjë.
7. Informacioni "I KUFIZUAR" mund të transmetohet ose ketë qasje në mënyrë elektronike nëpërmjet një rrjeti publik si interneti duke përdorur pajisje qeveritare ose komerciale enkriptimi të pranuar reciprokisht nga Palët. Bisedat telefonike, video-konferencat ose transmetimet faksimile që përmbajnë informacionin "I KUFIZUAR" mund të kryhen nëse një sistem enkriptimi nuk është i disponueshëm dhe pasi është marrë miratimi nga Autoriteti i Sigurisë Kombëtare të Palës që dërgon.

8. Nuk kërkohet një VSO kur një Kontraktor ndërmerr kontrata që kërkojnë vetëm marrjen ose prodhimin e Informacionit të Klasifikuar në nivel "I KUFIZUAR".

9. Qasja në një informacion të tillë "I KUFIZUAR" do t'u jepet vetëm atyre individëve që kanë Nevojë për të Ditur. Nuk kërkohet VSP për të hyrë në informacionin "I KUFIZUAR".



**SPORAZUM IZMEĐU  
VLADE SJEDINJENIH AMERIČKIH DRŽAVA  
I  
VLADE REPUBLIKE KOSOVO  
U VEZI SA MERAMA ZA ZAŠTITU  
POVERLJIVIH INFORMACIJA**

**PREAMBULA**

Vlada Sjedinjenih Američkih Država (u daljem tekstu "Sjedinjene Države") i vlada Republike Kosovo (u daljem tekstu "Kosovo") (u daljem tekstu pojedinačno "Strana" i kolektivno "Strane").

Uzimajući u obzir da Strane saraduju u pitanjima koja uključuju, ali se ne ograničavaju na, spoljne poslove, odbranu, bezbednost, policiju, nauku, industriju i tehnologiju, i

Imajuću zajednički interes u zaštiti Poverljivih informacija koje se razmenjuju tajno između Strana,

Saglasne su sa sledećim:

**ČLAN 1 - DEFINICIJE**

U svrhu ovog Sporazuma:

1. Poverljive informacije: Informacije koje je jedna Strana pružila drugoj Strani a koje je Strana koja ih je pružila označila kao poverljive u svrhu državne bezbednosti i prema tome zahteva zaštitu od neovlašćenog obelodanjivanja. Informacije mogu da budu usmene, vizuelne, eletronske ili u obliku dokumenta, ili u obliku materijala, uključujući opremu ili tehnologiju.
2. Poverljivi ugovor: Ugovor koji zahteva ili će zahtevati pristup Poverljivim informacijama ili proizvodnju istih od strane Ugovarača ili njegovih zaposlenih prilikom izvršenja ugovora.
3. Ugovarač: Fizičko ili pravno lice koje ima pravnu sposobnost da zaključuje ugovore, a koje je strana u Poverljivom ugovoru.
4. Bezbednosna provera objekta: Serifikat koji je izdao organ Državne bezbednosti jedne Strane, kao što je navedeno u članu 4, za objekat Ugovarača u nadležnosti te Strane, koji pokazuje da je objekat odobren do određenog nivoa i takođe da ima odgovarajuće bezbednosne mere na određenom nivou za zaštitu Poverljivih informacija. Takav sertifikat će značiti da će Poverljive informacija na nivou POVJERLJIVO / KONFIDENCIALE ili na višem nivou da budu zaštićene od strane Ugovarača za kojeg je izdat sertifikat o bezbednosnoj proveri objekta u skladu sa odredbama ovog Sporazuma i da će pridržavanje toga da bude praćeno i sprovedeno od strane relevantnog organa Državne bezbednosti. Bezbednosna provera objekta nije obavezna za Ugovarača koji preduzima izvršenje ugovora koji zahtevaju samo prijem ili proizvodnju Poverljivih informacija na nivou E KUFIZUAR.

## 5. Bezbednosna provera osoblja:

a. Odluka organa Državne bezbednosti jedne Strane, kako je navedeno u članu 4, da je pojedinac, kojeg zapošljava vladina agencija te Strane ili Ugovarač u nadležnosti te Strane, ovlašćen da ima pristup Poverljivim informacijama do određenog nivoa.

b. Odluka organa Državne bezbednosti jedne Strane, kako je navedeno u članu 4, da je pojedinac koji je državljanin jedne Strane, ali će biti zaposlen kod druge Strane ili kod jednog od Ugovarača druge Strane, ovlašćen da ima pristup Poverljivim informacijama do određenog nivoa.

6. Potreba da se zna Odluka ovlašćenog vlasnika Poverljivih informacija da je potencijalnom primaocu Poverljivih informacija potreban pristup određenim Poverljivim informacijama kako bi obavljao ili pomagao u obavljanju zakonite i ovlašćene vladine funkcije.

## **ČLAN 2 - OGRANIČENJA OBIMA OVOG SPORAZUMA**

Ovaj Sporazum se neće primenjivati na Poverljive informacije u okviru obima drugog sporazuma ili aranžmana između Strana ili njihovih agencija koji obezbeđuje zaštitu određene stavke ili kategorije Poverljivih informacija koje se razmenjuju između Strana ili njihovih agencija, osim u meri u kojoj takav drugi sporazum ili aranžman izričito čini primenjivim odredbe ovog Sporazuma. Ovaj Sporazum se takođe neće primenjivati na razmenu Ograničenih podataka, kako je definisano u Zakonu o atomskoj energiji SAD-a iz 1954. godine, s izmenama i dopunama (u daljem tekstu „AEA“), ili na Ranije ograničene podatke, koji su podaci uklonjeni iz kategorije Ograničenih podataka u skladu sa AEA, ali se u Sjedinjenim Državama i dalje smatraju odbrambenim informacijama.

## **ČLAN 3 - OBAVEZA ZAŠTITE POVERLJIVIH INFORMACIJA**

1. Svaka Strana će da zaštiti Poverljive informacije druge Strane u skladu s uslovima navedenim u ovom dokumentu.

2. Poverljive informacije će da zaštiti Strana primalac na način koji je u najmanjoj meri ekvivalentan zaštiti koju Poverljivim informacija pruža Strana koja ih dostavlja.

3. Svaka Strana će odmah da obavesti drugu o svim promenama svojih zakona i propisa koje bi uticale na zaštitu Poverljivih informacija prema ovom Sporazumu. Takve promene domaćeg zakona neće uticati na obaveze iz ovog Sporazuma. U takvim slučajevima, Strane će da se konsultuju u vezi sa mogućim izmenama i dopunama ovog Sporazuma ili drugim merama koje bi mogle biti primerene za održavanje zaštite Poverljivih informacija koje se razmenjuju u skladu sa ovim Sporazumom.

## **ČLAN 4 - ORGANI DRŽAVNE BEZBEDNOSTI**

1. Strane će jedna drugu obavestiti o organima Državne bezbednosti odgovornim za sprovođenje ovog sporazuma i o svim naknadnim promenama ovih organa.

2. U svrhu ovog Sporazuma, organi Državne bezbednosti će biti:

a. za Sjedinjene Države: Pomoćnik direktora, Direkcija za međunarodne angažmane, Uprava za obezbeđenje odbrambene tehnologije, Kancelarija podsekretara odbrane za politiku, Ministarstvo odbrane SAD-a.

b. za Republiku Kosovo Obaveštajna služba Kosova/Odelenje za bezbednosnu proveru.

3. Strane mogu da zaključe dodatne sporazume o sprovođenju ovog Sporazuma gde mogu biti potrebne dodatne tehničke bezbednosne mere za zaštitu Poverljivih informacija koje se prenose Strani primaocu putem strane vojne prodaje ili programa saradnje za koprodukciju ili zajednički razvoj odbrambenih artikala ili usluga. Takvi aranžmani implementacije mogu da uključuju posebne bezbednosne sporazume ili sporazume o industrijskoj bezbednosti.

#### **ČLAN 5 - OZNAČAVANJE POVERLJIVIH INFORMACIJA**

1. Poverljive informacije će biti označene, obeležene pečatom ili drugom znakom kad je to moguće, od Strane koja ih dostavlja na jednom od sledećih stepena tajnosti državne bezbednosti. U svrhu obezbeđenja jednakog tretmana, Strane su saglasne da su sledeći stepeni tajnosti sa stanovišta bezbednosti ekvivalentni:

<b>SJEDINJENE DRŽAVE</b>	<b>KOSOVO</b>
DRŽAVNA TAJNA	TEPËR SEKRET
STROGO POVERLJIVO	SEKRET
POVERLJIVO	KONFIDENCIALE
Nema ekvivalent	E KUFIZUAR

2. Tokom sprovođenja ovog Sporazuma, ako Kosovo pruži Poverljive informacije označene kao "E KUFIZUAR", Sjedinjene Države će da postupaju s njima u skladu s Dodatkom ovom Sporazumu.

3. Poverljive informacije će biti označene, obeležene pečatom ili drugm znakom gde je to moguće, s imenom Strane koja ih dostavlja.

#### **ČLAN 6 - ODGOVORNOST ZA POVERLJIVE INFORMACIJE**

Strana primalac će biti odgovorna za zaštitu svih Poverljivih informacija Strane koja ih dostavlja na način koji je barem ekvivalentan zaštiti koju Poverljivim informacija pruža Strana koja ih dostavlja dok su Povjerljive informacije pod njenom kontrolom. Strana koja ih dostavlja će biti odgovorna za sve Poverljive informacije dok su u tranzitu, sve dok se čuvanje Poverljivih informacija formalno ne prenese na Stranu primaoca.

## **ČLAN 7 - ZAŠTITA POVERLJIVIH INFORMACIJA**

1. Nijedan pojedinac neće imati pravo na pristup Poverljivim informacijama samo na osnovu čina, položaja, imenovanja ili bezbednosne provere. Pristup takvim informacijama će biti odobren samo pojedincima koji imaju potrebu da ih znaju i imaju sertifikat o potrebnoj bezbednosnoj proveri u skladu sa propisanim standardima Strane primaoca.

2. Osim ako je drugačije predviđeno ovim Sporazumom, Strana primalac neće odati Poverljive informacije Strane koja ih dostavlja bilo kojoj trećoj strani, uključujući bilo koju treću vladu, pojedinca, firmu, instituciju, organizaciju ili neki drugi entitet, bez prethodne pismene saglasnosti Strane koja ih dostavlja.

3. Strana primalac neće koristiti niti dozvoliti upotrebu Poverljivih informacija Strane koja ih dostavlja u bilo koju drugu svrhu osim one za koju su dostavljene bez prethodne pismene saglasnosti Strane koja ih dostavlja.

4. Strana primalac će poštovati sva privatna prava koja su povezana s Poverljivim informacijama Strane koja ih dostavlja, uključujući ona prava u vezi s patentima, autorskim pravima ili poslovnim tajnama, i neće objavljivati, koristiti, razmenjivati ili otkrivati takve Poverljive informacije na način koji bi bio u suprotnosti sa tim pravima bez prethodnog pismenog odobrenja vlasnika tih prava.

5. Strana primalac će obezbediti da svaki objekat ili ustanova koja rukuje Poverljivim informacijama obuhvaćenim ovim Sporazumom vodi spisak pojedinaca u objektu ili ustanovi koji su ovlašćeni da imaju pristup takvim informacijama.

6. Svaka Strana će razviti procedure za polaganje računa i kontrolu da bi upravljala širenjem i pristupom Poverljivim informacijama.

7. Svaka Strana će se pridržavati svih ograničenja korišćenja, obelodanjivanja, objavljivanja i pristupa Poverljivim informacijama koje može odrediti Strana koja ih dostavlja kada obelodani takve Poverljive informacije. Ako jedna Strana nije u mogućnosti da ispoštuje navedena ograničenja, ta Strana će odmah da se konsultuje s drugom Stranom i preduzme sve zakonske mere da spreči ili svede na najmanju moguću meru svako takvo korišćenje, obelodanjivanje, objavljivanje ili pristup.

## **ČLAN 8 - BEZBEDNOSNA PROVERA OSOBLJA**

1. Strane će se pobrinuti da svi pojedinci kojima je u vršenju njihovih službenih dužnosti potreban pristup ili čije dužnosti ili funkcije mogu omogućiti pristup Poverljivim informacijama u skladu sa ovim Sporazumom, dobiju odgovarajući sertifikat o bezbednosnoj proveri pre nego im se odobri pristup takvim informacijama.

2. Strana koja dodeljuje serifikat o bezbednosnoj proveru će provesti odgovarajuću istragu dovoljno detaljnu da bi utvrdila podobnost pojedinca za pristup Poverljivim informacijama. Odluka o dodeli serifikata o bezbednosnoj proveru će biti donesena u skladu sa državnim zakonima i propisima Strane koja ga dodeljuje.

3. Pre nego što funkcioner ili predstavnik jedne Strane dostavi Poverljive informacije funkcioneru ili predstavniku druge Strane, Strana primalac će Strani koja ih dostavlja pružiti uverenje da taj funkcioner ili predstavnik ima neophodan nivo bezbednosne provere i potrebu da ih zna i da će Poverljive informacije biti zaštićene od Strane primaoca u skladu s ovim Sporazumom.

## **ČLAN 9 - DOSTAVLJANJE POVERLJIVIH INFORMACIJA UGOVARAČIMA**

1. Poverljive informacije koje je primila, Strana primalac može da pruži Ugovaraču ili potencijalnom Ugovaraču čije dužnosti zahtevaju pristup takvim informacijama uz prethodnu pismenu saglasnost Strane koja ih je dostavila. Pre dostavljanja bilo koje Poverljive informacije Ugovaraču ili potencijalnom Ugovaraču, Strana primalac će:

a. Potvrditi da takav Ugovarač ili potencijalni Ugovarač i objekat Ugovarača imaju sposobnost da zaštite informacije u skladu s odredbama ovog Sporazuma;

b. Potvrditi da su takvom Ugovaraču ili potencijalnom Ugovaraču i objektu Ugovarača izdati odgovarajući sertifikati o bezbednosnoj proveru osoblja i bezbednosnoj proveru objekata, prema potrebi;

c. Potvrditi da Ugovarač ili potencijalni Ugovarač ima uspostavljene procedure koje obezbeđuju da su svi pojedinci koji imaju pristup informacijama obavešteni o svojim dužnostima da štite te informacije u skladu sa primenjivim zakonima i propisima;

d. Vršiti periodične bezbednosne inspekcije proverenih objekata kako bi se obezbedilo da su informacije zaštićene u skladu sa zahtevima ovog Sporazuma; i,

e. Potvrditi da Ugovarač ili potencijalni Ugovarač ima uspostavljene procedure koje obezbeđuju da je pristup informacijama ograničen na one pojedince koji imaju potrebu da ih znaju.

## **ČLAN 10 - POVERLJIVI UGOVORI**

1. Kad jedna Strana predloži da sklopi, ili ovlasti Ugovarača u svojoj zemlji da sklopi Poverljivi ugovor koji ima stepen tajnosti POVERLJIVO / KONFIDENCIALE ili viši, s Ugovaračem u zemlji druge Strane, Strana koja će sklopiti ili ovlastiti Ugovarača da sklopi takav Poverljivi ugovor, će tražiti uverenje da je organ Državne bezbednosti druge Strane izdao sertifikat o bezbednosnoj proveru objekta. Organ Državne bezbednosti Strane od koje se to zahteva će nadgledati i preduzeti sve odgovarajuće korake da bi se pobrinuo da bezbednosno postupanje Ugovarača bude u skladu s važećim zakonima i propisima.

2. Organ Državne bezbednosti Strane koja pregovara o Poverljivom ugovoru koji će se izvršiti u zemlji druge Strane, u Poverljivi ugovor će uključiti zahtev za predlogom ili podugovornim

dokumentom s odgovarajućim bezbednosim klauzulama i drugim relevantnim odredbama, uključujući troškove obezbeđenja. Ovo uključuje odredbe kojima se zahteva od svih Ugovarača da uvrste odgovarajuće bezbednosne klauzule u svoje podugovorne dokumente.

#### **ČLAN 11 - ODGOVORNOST ZA OBJEKTE**

Svaka Strana će biti odgovorna za obezbeđenje svih državnih i privatnih objekata i ustanova u kojima pohranjuje Poverljive informacije druge Strane i obezbediti da takvi objekti ili ustanove imaju kvalifikovane i na odgovarajući način proverene pojedince imenovane s dužnostima i ovlašćenjima za kontrolu i zaštitu takvih informacija.

#### **ČLAN 12 - POHRANJIVANJE POVERLJIVIH INFORMACIJA**

Poverljive informacije koje se razmenjuju između Strana biće pohranjene na način koji obezbeđuje pristup samo onim pojedincima kojima je pristup odobren

#### **ČLAN 13 - PRENOS**

1. Poverljive informacije će se prenositi između Strana putem vladinih kanala ili drugih kanala koji su uzajamno unapred odobreni u pismenoj formi.

2. Minimalni zahtevi za bezbednost Poverljivih informacija tokom prenošenja su sledeći:

a. Dokumenti ili drugi mediji:

(1) Dokumenti ili drugi mediji koji sadrže Poverljive informacije će da se prenose u dvostrukim, zapečaćenim kovertama. Na unutrašnjoj koverti će da se navede samo oznaka tajnosti dokumenata ili drugog medija i adresa organizacije predviđenog primaoca. Na spoljnoj koverti će da se navede adresa organizacije predviđenog primaoca, adresa organizacije pošiljaoca i kontrolni broj dokumenta, ako je primenjivo.

(2) Na spoljnoj koverti ne sme da se navodi oznaka tajnosti priloženih dokumenata ili drugih medija. Dvostruko zapečaćena koverta će da bude prosleđena prema propisanim procedurama Strana.

(3) Primalac će pripremiti potvrde o prijemu za pakete koji sadrže dokumente ili druge medije koji sadrže Poverljive informacije koje se prenose između Strana, a te potvrde potpisuje krajnji primalac i vraća pošiljaocu.

b. Materijal

(1) Materijal, uključujući opremu, koji sadrži Poverljive informacije, će da se prevozi u zapečaćenim, pokrivenim vozilima ili će na drugi način da bude bezbedno upakovan ili zaštićen kako bi se sprečila identifikacija njegovog oblika, veličine ili sadržaja i držao pod stalnom kontrolom radi sprečavanja pristupa neovlašćenim osobama.

(2) Materijal, uključujući opremu, koji sadrži Poverljive informacije koji se mora privremeno pohraniti dok čeka otpremu, će da se stavi u zaštićene skladišne prostore. Takvi prostori će biti zaštićeni opremom za otkrivanje upada ili stražarima s obaveznim sertifikatima o bezbednosnoj proveri koji će održavati kontinuirani nadzor nad tim područjima. Samo ovlašćeno osoblje s obaveznim sertifikatima o bezbednosnoj proveri će imati pristup zaštićenim skladišnim područjima.

(3) Svaki put kada materijal koji sadrži Poverljive informacije, uključujući opremu, pređe iz ruke u ruku tokom tranzita, dobijaju se potvrde, a krajnji primalac potpisuje potvrdu za takav materijal i vraća je pošiljaocu.

#### c. Elektronska transmisija

(1) Poverljive informacije koje su označene stepenom tajnosti **POVERLJIVO / KONFIDENCIALE** ili višem a treba da se prenose elektronski biće prosledene korišćenjem bezbednih sredstava koje je odobrio organ Državne bezbednosti svake Strane.

### **ČLAN 14 - POSETE OBJEKTIMA I USTANOVAMA STRANA**

1. Posete predstavnika jedne Strane objektima i ustanovama druge Strane koje zahtevaju pristup Poverljivim informacijama, ili posete za koje je potreban sertifikat o bezbednosnoj proveri da bi se dozvolio pristup, treba da budu ograničene na one koje su neophodne u službene svrhe. Odobrenje se daje samo predstavnicima koji poseduju važeći setifikat o bezbednosnoj proveri.

2. Odobrenje za posetu takvim objektima i ustanovama izdaje samo Strana na čijoj se teritoriji nalazi objekat ili ustanova koja se posećuje. Posećena Strana, ili njeni imenovani funkcioneri, biće odgovorni za obaveštavanje objekta ili ustanove o predloženoj poseti, kao i o obimu i najvišem stepenu tajnosti Poverljivih informacija koje se mogu dati posetiocu.

3. Zahteve za posete predstavnika Strana će podneti Ambasada Sjedinjenih Država u Prištini u slučaju posetilaca iz SAD-a, i Ambasada Kosova u Vašingtonu, D.C., u slučaju posetilaca sa Kosova.

### **ČLAN 15 - BEZBEDNOSNE POSETE**

Sprovođenje bezbednosnih zahteva navedenih u ovom Sporazumu može se proveriti putem recipročnih poseta službenika obezbeđenja Strana. Predstavnicima obezbeđenja svake Strane, nakon prethodnih konsultacija, biće dozvoljeno da posete drugu Stranu kako bi prodiskutovali i posmatrali postupke implementacije druge Strane u interesu postizanja razumne uporedivosti bezbednosnih sistema. Strana domaćin će pomoći predstavnicima obezbeđenja koji dolaze u posetu da utvrde da li su Poverljive informacije primljene od druge Strane adekvatno zaštićene.

## **ČLAN 16 - BEZBEDNOSNI STANDARDI**

Na zahtev, svaka Strana će drugoj Strani pružiti informacije o svojim bezbednosnim standardima, praksi i procedurama za zaštitu Poverljivih informacija.

## **ČLAN 17 - REPRODUKCIJA POVERLJIVIH INFORMACIJA**

Kad se Poverljive informacije reprodukuju, sve originalne bezbednosne oznake na njima će se takođe reprodukovati, obeležiti pečatom ili označiti na svakoj reprodukciji takvih informacija. Takve reprodukcije podležu istim kontrolama kao i originalne informacije. Broj reprodukcija će biti ograničen na minimalni broj potreban u službene svrhe.

## **ČLAN 18 - UNIŠTAVANJE POVERLJIVIH INFORMACIJA**

1. Dokumenti i drugi mediji koji sadrže Poverljive informacije uništavaju se spaljivanjem, usitnjavanjem, cepanjem ili drugim sredstvima koja sprečavaju rekonstrukciju Poverljivih informacija sadržanih u njima.

2. Materijal, uključujući opremu, koji sadrži Poverljive informacije, biće uništen na način koji ga čini neprepoznatljivim kako bi se sprečila rekonstrukcija Poverljivih informacija u celini ili delimično.

## **ČLAN 19 - PROMENA STEPENA TAJNOSTI I OPOZIV TAJNOSTI**

1. Strane su saglasne da se smanji stepen tajnosti Poverljivih informacija čim te informacije prestaju da zahtevaju taj viši stepen zaštite ili da se opozove tajnost čim te informacija više ne zahtevaju zaštitu od neovlašćenog obelodanjivanja.

2. Strana koja ih je dostavila ima potpuno diskreciono pravo u vezi s promenom stepena tajnosti i opozivom tajnosti svojih Poverljivih informacija. Strana primalac neće smanjiti stepen tajnosti ili opozvati tajnost Poverljivih informacija primljenih od Strane koja ih dostavlja, bez obzira na očigledna uputstva za opoziv tajnosti na dokumentu, bez prethodnog pismenog pristanka Strane koja ih dostavlja.

## **ČLAN 20 - GUBITAK ILI KOMPROMITOVANJE**

Strana primalac će obavestiti Stranu koja ih dostavlja odmah po otkrivanju svih gubitaka ili kompromitovanja, kao i mogućih gubitaka ili kompromitovanja, Poverljivih informacija Strane koja ih je dostavila. U slučaju stvarnog ili mogućeg gubitka ili kompromitovanja takvih informacija, Strana primalac će odmah pokrenuti istragu kako bi se utvrdile okolnosti stvarnog ili mogućeg gubitka ili kompromitovanja. Rezultati istrage i informacije o merama koje su preduzete da se spreči da se to ponovi biće pružene Strani koja ih je dostavila.



## ČLAN 21 - SPOROVI

Nesuglasice između Strana koje proizilaze iz ili u vezi s ovim Sporazumom će se rešavati isključivo putem konsultacija između Strana i neće se upućivati na rešavanje državnom sudu, međunarodnom sudu ili bilo kojoj drugoj osobi ili entitetu.

## ČLAN 22 - TROŠKOVI

Svaka Strana će biti odgovorna za snošenje sopstvenih troškova nastalih u sprovođenju ovog Sporazuma. Sve obaveze Strana prema ovom Sporazumu zavise od dostupnosti sredstava.

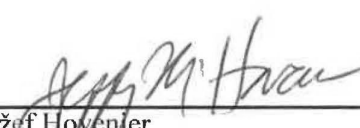
## ČLAN 23 - ZAVRŠNE ODREDBE

1. Ovaj Sporazum stupa na snagu na dan poslednjeg potpisa Strana.
2. Svaka Strana može raskinuti ovaj Sporazum tako što će drugu Stranu obavestiti u pismenoj formi diplomatskim kanalima devedeset dana unapred o svojoj nameri da raskine Sporazum.
3. Bez obzira na raskid ovog Sporazuma, sve Poverljive informacije razmenjene ili na drugi način dostavljene prema ovom Sporazumu i dalje će biti zaštićene u skladu s njegovim odredbama.

**POTVRĐUJUĆI OVO**, dole potpisani, propisno ovlašćeni od strane svojih odgovarajućih vlada, potpisali su ovaj sporazum.

Sačinjeno u Prištini ovog 24 dana avgust 2023, u po dva originalna primerka na engleskom, albanskom i srpskom jeziku, pri čemu su oba teksta podjednako verodostojna.

**ZA VLADU  
SJEDINJENIH AMERIČKIH DRŽAVA:**

  
\_\_\_\_\_  
Džef Hovenjer  
Ambassador

**ZA VLADU  
REPUBLIKE KOSOVO:**

  
\_\_\_\_\_  
Albin Kurti  
Premijer

## DODATAK

### POSTUPAK ZA ZAŠTITU KOSOVSKIH E KUFIZUAR POVERLJIVIH INFORMACIJA DOSTAVLJENIH SJEDINJENIM DRŽAVAMA

1. Kosovske Poverljive informacije dostavljene Sjedinjenim Državama i označene kao "E KUFIZUAR" biće zaštićene od strane Sjedinjenih Država po njihovom prijemu, u skladu sa sledećim procedurama.
2. Informacije označene kao "E KUFIZUAR" će da se čuvaju u zaključanim kontejnerima ili zatvorenim prostorima koji sprečavaju pristup neovlašćenom osoblju.
3. Informacije "E KUFIZUAR" neće biti obelodanjene neovlašćenim licima ili entitetima bez prethodnog pismenog odobrenja Vlade Kosova, osim u skladu sa zakonom SAD-a, uključujući Zakon o slobodi informacija.
4. Informacije "E KUFIZUAR" će, prema potrebi, da budu pohranjene, obrađene ili prenošene elektronskim putem koristeći sisteme akreditovane od strane vlade ili Ugovarača. Konkretno, pre nego što se koristi bilo koji sistem za pohranjivanje, obradu ili prenos "E KUFIZUAR" informacija, mora se dobiti bezbednosno odobrenje, poznato kao akreditacija. Akreditacija je formalna izjava odgovarajućeg organa za akreditaciju koja potvrđuje da korišćenje sistema ispunjava odgovarajuće bezbednosne zahteve i da ne predstavlja neprihvatljiv rizik. Bezbednosni standardni operativni postupci su tehničke procedure za sprovođenje bezbednosne politike i zahteva jedinstvenih za konkretan objekat za zaštitu automatizovanih informatičkih sistema koji obrađuju Poverljive informacije. Za samostalne automatizovane informatičke sisteme kao što su desktop i laptop kompjuteri koji se koriste u ustanovama Vlade SAD-a, dokument o registraciji sistema zajedno sa standardnim bezbednosnim operativnim postupcima će ispuniti ulogu zahtevane akreditacije. Za Ugovarače, smernice o korišćenju komunikacijskih i informatičkih sistema biće uključene u klauzulu o Zahtevima o ograničenim uslovima u Sporazumu.
5. Informacije s oznakom "E KUFIZUAR" će da se šalju poštom prve klase unutar Sjedinjenih Država u jednoj zapečaćenoj koverti. Prenos van Sjedinjenih Država biće u dvostrukim, zapečaćenim kovertama, sa oznakom "KOSOVO E KUFIZUAR" na unutrašnjoj koverti. Prenos izvan Sjedinjenih Država će da se vrši putem sredstava koja se mogu pratiti kao što je komercijalni kurir ili na drugi način o kojem su se Strane saglasile u pisanom obliku.
6. Američki dokumenti koji sadrže informacije "KOSOVO E KUFIZUAR" će imati na naslovnoj strani i na prvoj stranici oznaku "KOSOVO E KUFIZUAR." Deo dokumenata koji sadrži informacije "KOSOVO E KUFIZUAR" takođe će biti obeležen istom oznakom.
7. Informacije "E KUFIZUAR" mogu da se prenose ili da im se ostvaruje pristup elektronskim putem preko javne mreže kao što je Internet koristeći vladine ili komercijalne uređaje za kriptozastitu koje su Strane uzajamno prihvatile. Telefonski razgovori, video konferencije ili faksimilni prenosi koji sadrže informacije "E KUFIZUAR" mogu da se vrše ako sistem kriptozastite nije dostupan i podležu odobrenju organa Državne bezbednosti Strane koja ih je dostavila.
8. Bezbednosna provera objekta nije obavezna da bi Ugovarač preduzeo ugovore koji zahtevaju samo prijem ili proizvodnju Poverljivih informacija na nivou "E KUFIZUAR".