

DEFENSE

Security of Information

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

Signed at Nur-Sultan August 20, 2019

Entered into force October 23, 2019



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 KAZAKHSTAN
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 Kazakhstan ("Kazakhstan") (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 or distribution. 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 / CEKPETHO 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.

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

1. 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.

2. This Agreement also shall not apply to the exchange of data defined by the United States in accordance with U.S. law as Restricted Data, pursuant to the U.S. Atomic Energy Act of 1954, as amended (the "AEA"), or 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: Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy, U.S. Department of Defense; and

b. for Kazakhstan: National Security Committee [Komitet Natsionalnoi Bezopasnosti (KNB)] of the Republic of Kazakhstan. The point of contact at the KNB is the Director of the Department for the Protection of State Secrets.

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:

| UNITED STATES | KAZAKHSTAN |
|----------------------|--|
| TOP SECRET | COBEPILIEHHO CEKPETHO (TOP SECRET) |
| SECRET | CEKPETHO (SECRET) |
| CONFIDENTIAL | NO EQUIVALENT (see paragraph 2 below) |

2. Classified Information designated as "CONFIDENTIAL" that is released by the United States to Kazakhstan shall be protected by Kazakhstan as "CEKPETHO" ("SECRET").

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 / CEKPETHO 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 in accordance with the respective national laws and regulations of the Parties.

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 / CEKPETHO 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 Nur-Sultan in the case of U.S. visitors, and by the Embassy of the Republic of Kazakhstan in Washington, D.C., in the case of Kazakh 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 equivalency 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 – AMENDMENTS

This Agreement shall be amended only by mutual agreement of the Parties. Any such amendments shall be concluded as a separate document, which shall enter into force in accordance with Paragraph 1 of Article 24 (Final Provisions) of this Agreement.

ARTICLE 24 – FINAL PROVISIONS

1. This Agreement and any amendments to this Agreement shall enter into force on the date of the later note in an exchange of diplomatic notes by which the Parties indicate that each Party has completed its necessary internal procedures for the entry into force of this Agreement or an amendment thereto.

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.

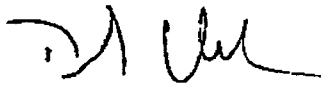
3. Notwithstanding the termination of this Agreement, all Classified Information exchanged or otherwise provided pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein.

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

DONE at Nur-Sultan, this 20 day of August, 2019, in duplicate, in the English, Kazakh, and Russian languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

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

**FOR THE GOVERNMENT OF
THE REPUBLIC OF KAZAKHSTAN:**



АМЕРИКА ҚҰРАМА ШТАТТАРЫНЫҢ ҮКІМЕТІ

МЕН

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҮКІМЕТІ

АРАСЫНДАҒЫ

**ҚҰПИЯ АҚПАРАТТЫ ҚОРҒАУ ЖӨНІНДЕГІ ҚАУІПСІЗДІК ШАРАЛАРЫНА
ҚАТЫСТЫ КЕЛІСІМ**

КІРІСПЕ

Америка Құрама Штаттарының Үкіметі («АҚШ») және Қазақстан Республикасының Үкіметі («Қазақстан») (әрқайсысы - «Тарап», бірге - «Тараптар»),

Тараптардың, халықаралық қатынастар, қорғаныс, қауіпсіздік, құқық қорғау қызметі, ғылым, өнеркәсіп және технология салаларындағы ынтымақтастықты қоса алғанда, бірақ олармен шектелмей, және

құпиялылық негізінде Тараптар алмасатын құпия ақпаратты қорғауға қатысты өзара мүддені қолдай отырып,

төмендегілер туралы келісті:

1-БАП. АНЫҚТАМАЛАР

Осы Келісімнің мақсаттары үшін:

1. Құпия ақпарат - ұлттық қауіпсіздік мақсатында және осы себептен рұқсат стілмеген жариялаудан немесе таратудан қорғауды талап ететін, беруші Тарап құпия ретінде белгілейтін, бір Тараптан екінші Тарапқа берілетін ақпарат. Ақпарат ауызша, визуалды, электрондық немесе құжаттық түрде не материалдар түрінде, оның ішінде жабдық немесе технологиялар түрінде берілуі мүмкін.

2. Құпия жұмыстар жүргізу туралы шарт - шартты орындау барысында құпия ақпаратқа немесе оның жасалуына оны орындаушылардың немесе оның жұмыскерлерінің қол жеткізуін талап ететін немесе талап етілетін шарт.

3. Орындаушы - шарттарды жасасуға құқықтық қабілеті бар, құпия жұмыстар жүргізу туралы шарттың Тарапы болып табылатын Тараптың заңды немесе жеке тұлғасы.

4. Құпия жұмыстарды жүргізуге рұқсат - 4-бапта белгіленген Тараптың ұлттық қауіпсіздік органы, осы Тараптың юрисдикциясындағы орындаушының объектісіне беретін, осы объектіге белгілі бір дәрежеде рұқсат берілгенін, сондай-ақ осы объектіде құпия ақпаратты қорғау үшін белгілі бір дәрежеде қажетті қауіпсіздік шаралары қолданылғанын растайтын куәлік. Мұндай куәліктің берілуі «CONFIDENTIAL/ҚҰПИЯ» дәрежесіндегі немесе одан жоғары дәрежедегі құпия ақпаратты осы Келісімнің ережесіне

сәйкес құпия жұмыстарды жүргізуге рұқсат (ҚЖЖР) берілген орындаушы қорғайтынын және бұл ережелердің орындалуын тиісті ұлттық қауіпсіздік органы қадағалайтынын және қамтамасыз ететінін білдіреді.

5. Персоналдың рұқсаты (ПР):

а. Осы Тараптың мемлекеттік органында немесе осы Тараптың юрисдикциясындағы орындаушыда қызметте жүрген тұлға құпиялылықтың белгілі бір дәрежесіне дейінгі құпия ақпаратқа қол жеткізуге уәкілетті екені туралы 4-бапта айқындалған Тараптың ұлттық қауіпсіздік органының шешімі.

б. Бір Тараптың азаматы болып табылатын, бірақ екінші Тараптың немесе екінші Тарап орындаушыларының бірінің қызметіне қабылдануды күтіп жүрген тұлға құпиялылықтың белгілі деңгейіне дейінгі құпия ақпаратқа қол жеткізуге уәкілетті екені туралы 4-бапта айқындалған Тараптың ұлттық қауіпсіздік органының шешімі.

6. Қызметтік қажеттіліктің қағидасы – құпия ақпаратты ықтимал алушыға мемлекет айқындаған құқыққа сыйымды және рұқсат етілген функцияларды орындау үшін немесе жәрдемдесу үшін оның белгілі бір түріне қолжетімділіктің талап етілетіні туралы құпия ақпараттың уәкілетті иесі болып табылатын тұлғаның шешімі.

2-БАП. КЕЛІСІМНІҢ ҚОЛДАНЫЛУ АЯСЫНА ШЕКТЕУЛЕР

1. Осы Келісім Тараптар мен олардың ведомстволары арасындағы Тараптар немесе олардың ведомстволары өзара алмасатын құпия ақпараттың белгілі бір түр тармақтары мен санаттарын қорғауды көздейтін басқа келісімдер немесе уағдаластық шарттарымен айқындалған әрекеттер аясына кіретін құпия ақпаратқа, осы Келісімнің шарттары осындай басқа келісімдерге немесе уағдаластыққа сай сөзсіз қолдануға жарамды болып табылатын жағдайларды қоспағанда, қолданылмайды.

2. Осы Келісім АҚШ заңнамасына және түзетулерімен қоса алғанда 1954 жылғы Атом энергиясы туралы АҚШ Заңына («АЭЗ») сәйкес Шектеулі қолжетімді деректермен немесе Бұрын шектеулі қолжетімді деректер деп айқындалған деректермен, яғни АЭЗ-на сәйкес Бұрын шектеулі қолжетімді деректері санатынан алынып тасталған, бірақ АҚШ әлі қорғаныс сипатындағы деректер деп қарастыратын деректермен аямасуға қолданылмайды.

3-БАП. ҚҰПИЯ АҚПАРАТТЫ ҚОРҒАУ ЖӨНІНДЕГІ МІНДЕТТЕМЕЛЕР

1. Әр Тарап осы құжатта жазылған шарттарға сәйкес екінші Тараптың құпия ақпаратын қорғайды.

2. Алушы Тарап құпия ақпаратты кем дегенде құпия ақпаратты беруші Тарап қамтамасыз ететін қорғауға баламалы тәсілмен қорғайды.

3. Әр Тарап осы Келісімге сәйкес өз заңдары мен заңға тәуелді актілеріндегі құпия ақпаратты қорғауға ықпал етуі мүмкін қандай да бір өзгерістер туралы басқа Тарапқа дереу хабарлайды. Ұлттық заңнаманың мұндай өзгерістері осы Келісім міндеттемелеріне ықпал етпейді. Мұндай жағдайларда Тараптар осы Келісімге ықтимал түзетулерге және

онымен алмасу осы Келісімге сәйкес жүргізілетін құпия ақпараттың қорғалуын қолдау үшін қажет болатын басқа да шараларға қатысты консультациялар өткізеді.

4-БАП. ҰЛТТЫҚ ҚАУІПСІЗДІК ОРГАНДАРЫ

1. Тараптар бір-бірін осы Келісімді орындауға жауапты ұлттық қауіпсіздік органдары және осы органдарға қатысты кез келген кейінгі өзгерістер туралы хабардар етеді.

2. Осы Келісімнің мақсатында ұлттық қауіпсіздік органдары:

а. АҚШ-тан: АҚШ Қорғаныс министрлігінің әскери-саяси мәселелер жөніндегі Қорғаныс министрінің орынбасары аппаратының Қорғаныс технологияларының қауіпсіздігі басқармасының халықаралық қауіпсіздік бағдарламаларының директоры; және

б. Қазақстаннан: Қазақстан Республикасы Ұлттық қауіпсіздік комитеті (ҰҚК) болып табылады. ҰҚК-дан жасайтын адам Мемлекеттік құпияларды қорғау департаментінің бастығы болып табылады.

3. Тараптар әскери тауарларды шетелге сату немесе қорғаныс тауарларын немесе көрсетілетін қызметтерді бірлесіп жасауға немесе бірлесіп әзірлеуге бағытталған ынтымақтастық бағдарламаларын жүзеге асыру барысында алушы Тарапқа берілетін құпия ақпаратты қорғау үшін техникалық қауіпсіздіктің қосымша шараларына қажеттілік туындаған жағдайда осы Келісімге қосымша атқарушылық уағдаластықтарды жасай алады. Мұндай атқарушылық уағдаластықта қауіпсіздіктің арнайы шаралары туралы келісімдер немесе өнеркәсіптік қауіпсіздік туралы келісімдер қамтылуы мүмкін.

5-БАП. ҚҰПИЯ АҚПАРАТТЫҢ БЕЛГІЛЕНУІ

1. Беруші Тарап құпия ақпаратты белгілейді және мүмкіндігіне қарай ұлттық қауіпсіздіктің мынадай белгілерінің бірімен мөртаңба басады және таңбалайды. Баламалы жолдауды қамтамасыз ету мақсатында Тараптар құпиялылықтың мынадай белгілерінің баламалылығы туралы келіседі:

| АҚШ | Қазақстан |
|--------------|---|
| TOP SECRET | ӨТЕ ҚҰПИЯ (TOP SECRET) |
| SECRET | ҚҰПИЯ (SECRET) |
| CONFIDENTIAL | БАЛАМАСЫ ЖОҚ (осы баптың 2-тармағын қараңыз) |

2. АҚШ Қазақстанға беретін «CONFIDENTIAL» белгісімен белгіленген құпия ақпарат «ҚҰПИЯ» белгісімен белгіленетін құпия ақпарат сияқты дәл сондай қорғау шараларын қолдануды қажет етеді.

3. Құпия ақпарат белгіленеді және мүмкіндігіне қарай беруші Тараптың атауымен мөртаңба басылады немесе таңбаланады.

6-БАП. ҚҰПИЯ АҚПАРАТ ҮШІН ЖАУАПТЫЛЫҚ

Алушы Тарап кем дегенде құпия ақпаратты беруші Тарап құпия ақпарат өзінің бақылауында болған кезде қамтамасыз ететін қорғауға баламалы тәсілмен беруші Тараптың барлық құпия ақпаратын қорғау үшін жауапты болады. Тасымалдау кезінде беруші Тарап алушы Тарапқа сақтауға құпия ақпаратты ресми жіберген кезге дейін барлық құпия ақпарат үшін жауапты болады.

7-БАП. ҚҰПИЯ АҚПАРАТТЫ ҚОРҒАУ

1. Ешбір жеке тұлға тек қана дәрежесіне, қызмет жағдайына, лауазымына немесе ПР-ға қарай құпия ақпаратқа қол жеткізуге құқылы емес. Мұндай ақпаратқа қолжетімділік тек қана қызметтік қажеттілік қағидатының негізінде және алушы Тараптың көзделген нормаларына сай талап етілетін ПР болған кезде жекелеген тұлғаларға беріледі.

2. Осы Келісімде өзгеше көзделген жағдайларды қоспағанда, алушы Тарап беруші Тараптың құпия ақпаратын үкіметті, тұлғаны, фирманы, мекемені, ұйымды немесе үшінші жақтың өзге де заңды тұлғасын қоса алғанда, қандай да бір үшінші жаққа беруші Тараптың алдын ала жазбаша келісімінсіз жария етпейді.

3. Алушы Тарап беруші Тараптың құпия ақпаратын оны арнайы берілген мақсаттан басқа қандай да бір өзге мақсатта беруші Тараптың алдын ала жазбаша келісімінсіз пайдаланбайды және пайдалануға рұқсат етпейді.

4. Алушы Тарап беруші Тараптың құпия ақпаратымен байланысты кез келген жеке құқықтарына, оның ішінде патенттерге, авторлық құқықтарға немесе коммерциялық құпияларға қатысты құқықтарына құрмет білдіреді және мұндай құпия ақпаратты осы құқықтар иесінің алдын ала жазбаша рұқсатынсыз осы құқықтармен сыйыспайтын тәсілмен таратпайды, пайдаланбайды, алмастырмайды немесе жарияламайды.

5. Алушы Тарап осы Келісімнің қолданысына жататын құпия ақпаратпен жұмыс істейтін әрбір объектінің немесе мекеменің осындай құпия ақпаратқа қол жеткізуге рұқсаты бар осы объектідегі немесе осы мекемедегі жеке тұлғалардың тізімін жүргізуін қамтамасыз етеді.

6. Әр Тарап құпия ақпаратты тарату және оған қол жеткізу мәселелерін реттейтін есепке алу және бақылау тәртібін әзірлейді.

7. Әр Тарап Құпия ақпаратты ашқан кезде беруші Тарап ескертетін құпия ақпаратты пайдалануға, ашуға, жариялауға және оған қол жеткізуге барлық шектеулерді сақтайды. Егер Тараптың бірі көрсетілген шектеулерді сақтай алмаса, бұл Тарап дереу екінші Тараппен консультация жүргізеді және кез келген мұндай пайдалануды, ашуды, жариялауды немесе қолжетімділікті болғызбауға немесе барынша азайтуға бағытталған, заңмен рұқсат етілген барлық шараларды қолданады.

8-БАП. ПЕРСОНАЛДЫҢ РҰҚСАТЫ

1. Тараптар қызметтік міндеттерін орындау барысында рұқсат талап етілетін немесе кімнің міндеттері немесе функциялары осы Келісімге сәйкес құпия ақпаратқа қолжетімділікті алуға мүмкіндік беретін барлық тұлғалардың олар осындай ақпаратқа рұқсат алудың алдында ПР-дың қажетті дәрежесін алуын қамтамасыз етеді.

2. ПР беретін Тарап құпия ақпаратқа рұқсатты алуға осы тұлғаның жарамдылығын айқындау мақсатында жеткілікті дәрежедегі егжей-тегжейлікке қажетті тергеп-тексеруді жүргізеді. ПР-ды беру туралы шешім беруші Тараптың ұлттық заңнамасына сәйкес қабылданады.

3. Бір Тараптың ресми тұлғасы немесе өкілі құпия ақпаратты екінші Тараптың ресми тұлғасына немесе өкіліне берердің алдында алушы Тарап беруші Тарапқа өзінің ресми адамының немесе өкілінің қажетті дәрежедегі ПР-ы болуы және қызметтік қажеттілік қағидатын сақтайтыны, сондай-ақ осы Келісімге сәйкес алушы Тараптың құпия ақпаратты қорғайтыны туралы растама береді.

9-БАП. ОРЫНДАУШЫЛАРҒА ҚҰПИЯ АҚПАРАТТЫ АШУ

1. Алушы Тарап алған құпия ақпаратты беруші Тараптың алдын ала жазбаша келісімімен алушы Тарап орындаушыға немесе осындай ақпаратқа қолжетімділікті талап ететін ықтимал орындаушыға беруі мүмкін. Орындаушыға немесе ықтимал орындаушыға қандай да бір құпия ақпаратты берердің алдында алушы Тарап:

a. Мұндай орындаушының немесе ықтимал орындаушының, сондай-ақ орындаушының ұйымының осы Келісімнің шарттарына сәйкес ақпаратты қорғауды қамтамасыз ету мүмкіншілігін растайды;

b. Осындай орындаушыға немесе ықтимал орындаушыға, сондай-ақ орындаушының ұйымына мән-жайларға байланысты тиісті ПР және ҚЖЖР берілгенін растайды;

c. Осындай орындаушыға немесе ықтимал орындаушыға ақпаратқа қолжетімділігі бар барлық адамдардың қолдануға болатын заңдар мен заңнан туындайтын актілерге сәйкес өзінің ақпаратты қорғау үшін жауаптылығы туралы хабардар болуын қамтамасыз ету тәртібі бар екендігін растайды;

d. Осы Келісімнің талаптарына сәйкес ақпараттың қорғалуын қамтамасыз ету үшін ҚЖЖР алған объектілерге мерзімді қауіпсіздік инспекциясын жүргізеді;

e. Орындаушыда немесе ықтимал орындаушыда ақпаратқа қолжетімділіктің ақпаратқа қызметтік қажеттілігі бар адамдармен шектелуін қамтамасыз ету тәртібі бар екендігін растайды.

10-БАП. ҚҰПИЯ ЖҰМЫСТАР ЖҮРГІЗУ ЖӨНІНДЕГІ КЕЛІСІМДЕР

1. Егер Тарап құпия жұмыстар жүргізу туралы шарт жасасуды көздесе немесе екінші Тарап елінде орындаушы «CONFIDENTIAL/ҚҰПИЯ» немесе одан да жоғары құпиялылық дәрежесі берілген құпия жұмыстар жүргізу туралы шарт жасасуға өз еліндегі

орындаушыға рұқсат берсе, құпия жұмыстар жүргізу туралы шарт жасасатын немесе орындаушыға рұқсат беретін Тарап екінші Тараптың ұлттық қауіпсіздік органынан ҚЖЖР беру туралы растаманы сұратуы тиіс. Сұрау салуды алған Тараптың ұлттық қауіпсіздік органы орындаушының қауіпсіздікке қойылатын барлық талаптарды орындауының қолданылатын заңдар мен заңға тәуелді актілерге сәйкес келуін қадағалайды және оны қамтамасыз ету үшін барлық қажетті шараларды қабылдайды.

2. Тараптың екінші Тарап елінде орындалуға тиіс құпия жұмыстар жүргізу туралы шарт жасасатын ұлттық қауіпсіздік органы құпия жұмыстар жүргізу туралы шартқа, ұсыныстарға салынған сауалға немесе қосалқы мердігерлік туралы құжатқа қауіпсіздік туралы қажетті ескертулерді және басқа да тиісті ережелерді, оның ішінде қауіпсіздікті қамтамасыз етуге арналған шығыстар туралы ескертулерді енгізеді. Бұған барлық орындаушылардан өздерінің қосалқы мердігерлік туралы құжаттарына қауіпсіздік жөніндегі тиісті ескертулерді енгізуін талап ететін ережелер кіреді.

11-БАП. ОБЪЕКТИЛЕР ҮШІН ЖАУАПТЫЛЫҚ

Әр Тарап өзі екінші Тараптың құпия ақпаратын сақтайтын барлық мемлекеттік және жекеменшік объектілер мен мекемелердің қауіпсіздігі үшін жауаптылықта болады және осындай объектілерде немесе осындай мекемелерде білікті және тиісті рұқсатты алған адамдардың болуын қамтамасыз етеді, олардың тағайындалуы осындай ақпаратты бақылау және қорғау саласындағы жауаптылық пен өкілеттіктердің болуын көздейді.

12-БАП. ҚҰПИЯ АҚПАРАТТЫҢ САҚТАЛУЫ

Тараптар өзара алмасатын құпия ақпарат оған рұқсаты бар адамдардың ғана қолжетімділігіне мүмкіндік беретіндей болып сақталады.

13-БАП. БЕРУ

1. Құпия ақпарат Тараптар арасында алдын ала жазбаша түрде өзара мақұлданған үкіметаралық арналар арқылы немесе басқа да арналар арқылы Тараптардың ұлттық заңнамаларына сәйкес беріледі.

2. Құпия ақпаратты беру барысында оның қауіпсіздігіне қойылатын ең аз талаптар төмендегілер:

а. Құжаттар немесе басқа да тасымалдағыштар:

(1) Құпия ақпаратты қамтитын құжаттар немесе басқа да тасымалдағыштар мөр басылған қос конверттермен беріледі. Ішкі конвертте тек қана құжаттардың немесе басқа да тасымалдағыштардың құпиялылық белгісі, сондай-ақ болжанған алушының мекенжайы көрсетіледі. Сыртқы конвертте болжанған алушының мекенжайы, жөнелтушінің мекенжайы және қажет болған жағдайда құжаттың тіркеу нөмірі көрсетіледі.

(2) Сыртқы конвертте оған салынған құжаттардың немесе басқа да тасымалдағыштардың құпиялылық дәрежесі көрсетілмейді. Қос мөр басылған конверт Тараптардың алдын ала белгілеген тәртібіне сәйкес жіберіледі.

(3) Тараптар арасында берілетін құпия ақпарат қамтылған құжаттарды немесе басқа да тасымалдағыштарды қамтитын пакеттерді алушылар қолхаттарды дайындайды, бұл орайда мұндай қолхаттарға соңғы алушы қол қояды және жөнелтушіге қайтарылады.

б. Материалдар:

(1) Құпия ақпаратты қамтитын материалдар, оның ішінде жабдық пломбаланған жабық көлік құралдарымен тасымалданады, не олардың нысандарын, мөлшерін немесе ішіндегісін танып-білуді болғызбайтындай өзге де тәсілдермен сенімді түрде буыптүйіледі немесе қорғалады және уәкілеттік берілмеген адамдардың қол жеткізуінің алдын алу үшін олар тұрақты бақылауда болады.

(2) Құпия ақпаратты қамтитын және жөнелтілуін күтіп уақытша сақтауға жататын материалдар, оның ішінде жабдық қорғалған қоймаларда орналастырылады. Мұндай қоймалар рұқсатсыз енуді байқау жабдығының көмегімен қорғалады немесе қажетті ПР-ы бар күзетшілердің тұрақты бақылауында болады. Қажетті ПР алған уәкілетті персонал ғана қорғалған қоймаларға кіре алады.

(3) Материалдар, оның ішінде құпия ақпаратты қамтитын жабдық тасымалдау барысында бір қолдан екіншісіне өткен кезде қолхат табысталады, бұл орайда мұндай материалдар үшін берілетін қолхатқа соңғы алушы қол қояды және жөнелтушіге қайтарылады.

с. Электрондық беру:

(1) Электрондық тәсілмен беруге жататын «CONFIDENTIAL/ҚҰПИЯ» дәрежесіндегі белгісі бар немесе одан да жоғары дәрежедегі құпия ақпарат, Тараптардың әрқайсысының ұлттық қауіпсіздік органы мақұлдаған, қорғалған құралдар арқылы беріледі.

14-БАП. ТАРАПТАРДЫҢ ОБЪЕКТІЛЕРІНЕ ЖӘНЕ МЕКЕМЕЛЕРІНЕ ЖАСАЛАТЫН САПАРЛАР

1. Бір Тараптың өкілдерінің екінші Тараптың объектілері мен мекемелеріне құпия ақпаратқа қол жеткізуді талап ететін сапарлары немесе ПР болуы талап етілетін сапарлар ресми мақсаттар үшін қажет болатын сапарлармен ғана шектелуге тиіс. Рұқсаттама жарамды ПР-ды бар өкілдерге ғана беріледі.

2. Осындай объектілерге және осындай мекемелерге баруға рұқсаттаманы аумағында баратын объект немесе мекеме орналасқан Тарап қана береді. Қабылдаушы Тарап немесе оның тағайындалған ресми өкілдері ықтимал сапар туралы, сондай-ақ келушіге ұсынылуы мүмкін ақпараттың көлемі мен құпиялылығының ең жоғары дәрежесі туралы объектіні немесе мекемені хабардар етуге жауапты болады.

3. Тараптардың өкілдері сапар жасауға арналған сұрау салуларды америкалық келушілер болған кезде АҚШ-тың Нұр-Сұлтандағы Елшілігі және Қазақстаннан келушілер болған кезде Қазақстан Республикасының Вашингтондағы Елшілігі береді.

15-БАП. ҚАУІПСІЗДІКТІ ТЕКСЕРУ МАҚСАТЫНДА ЖАСАЛАТЫН САПАРЛАР

Осы Келісімде баяндалған қауіпсіздікке қойылатын талаптарды орындау Тараптардың қауіпсіздік қызметтері өкілдерінің өзара сапар жасауы арқылы тексерілуі мүмкін. Алдын ала консультациялар өткізгеннен кейін Тараптардың әрқайсысының қауіпсіздік қызметтерінің өкілдеріне қауіпсіздік жүйелерінің баламалылығына қол жеткізу мақсатында екінші Тараптың имплементтеу тәртіптерін талқылау және қадағалау үшін екінші Тарапқа сапармен баруға рұқсат етіледі. Қабылдаушы Тарап екінші Тараптан алынған құпия ақпаратты қорғаудың барабарлығын айқындауда қауіпсіздік қызметінің келуші өкілдеріне жәрдем көрсетеді.

16-БАП. ҚАУІПСІЗДІК СТАНДАРТТАРЫ

Сұрау салу бойынша әрбір Тарап екінші Тарапқа өзінің қауіпсіздік стандарттары, құпия ақпаратты қорғаудың тәжірибелері мен тәртіптері туралы ақпаратты ұсынады.

17-БАП. ҚҰПИЯ АҚПАРАТТЫ КӨБЕЙТУ

Құпия ақпаратты көбейткенде оның әрбір көшірмесі көбейтіледі, мөртабан басылады немесе қауіпсіздіктің барлық тиісті құпиялылық белгілерімен белгіленеді. Мұндай көшірмелер түпнұсқа ақпарат сияқты шектеулерге жатады. Көшірмелер саны ресми мақсаттар үшін қажетті ең аз санмен шектеледі.

18-БАП. ҚҰПИЯ АҚПАРАТТЫ ЖОЮ

1. Құпия ақпаратты қамтитын құжаттар және басқа да тасымалдағыштар оларда қамтылған құпия ақпаратты қалпына келтіруге жол берілмейтін жағу, кесу, ұсақтау немесе басқа да тәсілдер арқылы жойылады.

2. Құпия ақпаратты қамтитын жабдықты қоса алғанда, материалдар оларды тану мүмкін болмайтын және құпия ақпараттың толық немесе ішінара қалпына келуін болғызбайтын тәсілмен жойылады.

19-БАП. ҚҰПИЯЛЫЛЫҚ ДӘРЕЖЕСІН ТӨМЕНДЕТУ ЖӘНЕ ҚҰПИЯСЫЗДАНДЫРУ

1. Тараптар құпия ақпарат қорғаудың жоғарырақ дәрежесін қажет етуден қалған сәттен бастап оның құпиялылық дәрежесін төмендету қажеттілігімен немесе мұндай ақпарат заңсыз жария етуден қорғауды бұдан кейін қажет етпейтін сәттен бастап оны құпиясыздандыру қажеттігімен келіседі.

2. Беруші Тараптың құпиялылық дәрежесін төмендетуге немесе өзінің құпия ақпаратын құпиясыздандыруға қатысты өз қалауы бойынша әрекет етуге барлық өкілеттіктері болады. Алушы Тарап беруші Тараптың алдын ала жазбаша келісімінсіз беруші Тараптан алынған құпия ақпараттың құпиялылық дәрежесін төмендетпейді және құжаттағы құпиясыздандыру жөніндегі қандай да болсын нұсқауға қарамастан, оны құпиясыздандырмайды.

20-БАП. ЖОҒАЛТУ НЕМЕСЕ ЖАРИЯ ЕТУ

Қабылдаушы Тарап жоғалған немесе жария етілген кез келген фактілер туралы, сондай-ақ беруші Тараптың құпия ақпаратының жоғалуының немесе жария етілуінің ықтимал фактілері туралы беруші Тарапты дереу хабардар етеді. Осындай ақпарат нақты жоғалған немесе жария етілген, не болмаса жоғалуы немесе жария етілуі ықтимал болатын жағдайда қабылдаушы Тарап нақты немесе ықтимал жоғалу немесе жария етілудің мән-жайларын айқындау мақсатында тергеп-тексеруді дереу бастайды. Беруші Тарапқа тергеп-тексеру нәтижелері және осы жағдайлардың қайталануын болғызбау үшін қабылданған шаралар туралы ақпарат беріледі.

21-БАП. ДАУЛАР

Тараптар арасында осы Келісімді іске асыру барысында немесе онымен байланысты туындайтын келіспеушіліктер Тараптар арасындағы консультациялар арқылы ғана шешіледі және реттеу үшін ұлттық сотқа да, халықаралық сотқа да, қандай да бір жеке немесе заңды тұлғаға да берілмейді.

22-БАП. ШЫҒЫНДАР

Әр Тарап осы Келісімді іске асыру барысында өзінің шеккен шығындары үшін жауапты болады. Тараптардың осы Келісім шеңберіндегі барлық міндеттемелері қаражаттың болуына байланысты.

23-БАП. ТҮЗЕТУЛЕР

Осы Келісімге өзгерістер мен толықтырулар Тараптардың екіжақты келісімі бойынша ғана енгізіледі. Кез келген өзгерістер мен толықтырулар осы Келісімнің 24-бабының 1-тармағына сәйкес күшіне енетін бөлек құжат түрінде рәсімделуі керек.

24-БАП. ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР

1. Осы Келісім және осы Келісімге енгізілетін кез келген өзгерістер мен толықтырулар Тараптар әрбір Тарап осы Келісімнің немесе келісімге енгізілген өзгерістердің күшіне енуі үшін қажетті өзінің мемлекетішілік рәсімдерді орындағаны туралы хабарлаған дипломатиялық ноталармен алмасу барысындағы соңғы дипломатиялық нота күнінен бастап күшіне енеді.

2. Кез келген Тарап өзінің осы Келісімнің қолданысын тоқтату ниеті туралы тоқсан күн бұрын дипломатиялық арналар арқылы екінші Тарапты жазбаша түрде хабардар етіп, оның қолданысын тоқтатуы мүмкін.

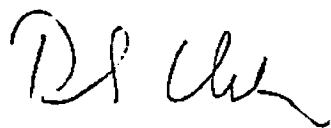
3. Осы Келісімнің қолданысы тоқтатылғанына қарамастан, осы Келісімге сәйкес айырбасталған немесе өзгеше түрде ұсынылған барлық құпия ақпарат осы Келісімнің ережелеріне сәйкес одан әрі қорғалады.

ОСЫНЫ КУӘЛАНДЫРУ ҮШІН өздерінің тиісті Үкіметтері тиісті түрде уәкілеттік берген төменде қол қоюшылар осы Келісімге қол қойды.

2019 жылғы «20» тамызда Нұр-Сұлтан қаласында әрқайсысы ағылшын, қазақ және орыс тілдерінде екі данада ЖАСАЛДЫ, әрі барлық мәтіндердің күші бірдей. Осы Келісімнің ережелерін түсіндіру кезінде келіспеушіліктер туындаған жағдайда, ағылшын тіліндегі мәтін басым болады.

АМЕРИКА ҚҰРАМА ШТАТТАРЫНЫҢ
ҮКІМЕТІ ҮШІН:

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ
ҮКІМЕТІ ҮШІН:



**СОГЛАШЕНИЕ
МЕЖДУ ПРАВИТЕЛЬСТВОМ СОЕДИНЕННЫХ ШТАТОВ АМЕРИКИ И
ПРАВИТЕЛЬСТВОМ РЕСПУБЛИКИ КАЗАХСТАН
КАСАТЕЛЬНО МЕР БЕЗОПАСНОСТИ
ПО ЗАЩИТЕ СЕКРЕТНОЙ ИНФОРМАЦИИ**

ПРЕАМБУЛА

Правительство Соединенных Штатов Америки («США») и Правительство Республики Казахстан («Казахстан») (каждое – «Сторона», вместе «Стороны»), учитывая сотрудничество Сторон в областях, включая, но, не ограничивая, международные отношения, оборону, безопасность, правоохранительную деятельность, науку, промышленность и технологии, и разделяя взаимный интерес к защите секретной информации, которой Стороны обмениваются на основе конфиденциальности, согласились о нижеследующем:

СТАТЬЯ 1 – ОПРЕДЕЛЕНИЯ

Для целей настоящего Соглашения:

1. Секретная информация: информация, предоставляемая одной Стороной другой Стороне, которая обозначается передающей Стороной как секретная в целях национальной безопасности и по этой причине требующая защиты от несанкционированного раскрытия или распространения. Информация может предоставляться в устной, визуальной, электронной или документальной форме, либо в форме материалов, в том числе оборудования или технологий.
2. Договор о проведении секретных работ: договор, который требует или будет требовать доступа к секретной информации или ее производства исполнителем или его работниками в ходе выполнения договора.
3. Исполнитель: физическое или юридическое лицо Стороны, обладающее правоспособностью на заключение договоров, которое является Стороной договора о проведении секретных работ.
4. Разрешение на проведение секретных работ: удостоверение, выдаваемое национальным органом безопасности Стороны, определенным в Статье 4, объекту исполнителя, находящемуся в юрисдикции данной Стороны, подтверждающее, что этому объекту присвоено разрешение определенного уровня, а также что на этом объекте предприняты необходимые меры безопасности определенного уровня для защиты секретной информации. Выдача такого удостоверения означает, что секретная информация уровня CONFIDENTIAL/СЕКРЕТНО или выше защищается тем исполнителем, которому в соответствии с положениями настоящего Соглашения выдано разрешение на проведение секретных работ (РПСР), и что выполнение этих

положений отслеживается и обеспечивается соответствующим национальным органом безопасности.

5. Допуск персонала (ДП):

а. Решение национального органа безопасности Стороны, определенного в Статье 4, о том, что лицо, пребывающее на службе в государственном органе данной Стороны или у исполнителя, находящегося в юрисдикции этой Стороны, уполномочено на доступ к секретной информации до определенного уровня секретности;

б. Решение национального органа безопасности Стороны, определенного в Статье 4, о том, что лицо, являющееся гражданином одной Стороны, но ожидающее приема на службу другой Стороной или одним из исполнителей другой Стороны, уполномочено на доступ к секретной информации до определенного уровня секретности.

6. Принцип служебной необходимости: решение лица, являющегося уполномоченным хранителем секретной информации, о том, что предполагаемому получателю секретной информации требуется доступ к определенному ее виду для выполнения или для содействия в выполнении определенных государством правомерных и дозволенных функций.

СТАТЬЯ 2 – ОГРАНИЧЕНИЯ НА СФЕРУ ДЕЙСТВИЯ СОГЛАШЕНИЯ

1. Настоящее Соглашение не применяется к секретной информации, входящей в сферу действия, определенную условиями других соглашений или договоренностей между Сторонами или их ведомствами, предусматривающих защиту определенных подвидов или категорий секретной информации, которой обмениваются Стороны или их ведомства, за исключением случаев, когда согласно таким другим соглашениям или договоренностям условия настоящего Соглашения являются однозначно приемлемыми.

2. Настоящее Соглашение также не применяется к обмену данными, определяемыми Соединенными Штатами в соответствии с национальным законодательством, как данные ограниченного доступа, согласно Закону США об атомной энергии с поправками от 1954 г. («ЗАЭ»), или к данным, которые ранее считались данными ограниченного доступа, то есть к данным, изъятым из этой категории согласно ЗАЭ, но по-прежнему рассматриваемыми США как данные оборонного характера.

СТАТЬЯ 3 – ОБЯЗАТЕЛЬСТВА ПО ЗАЩИТЕ СЕКРЕТНОЙ ИНФОРМАЦИИ

1. Каждая Сторона защищает секретную информацию другой Стороны согласно условиям, излагаемым в настоящем документе.

2. Секретная информация защищается получающей Стороной способом, по меньшей мере эквивалентным той защите, которую обеспечивает секретной информации передающая Сторона.

3. Каждая Сторона незамедлительно оповещает другую о каких-либо изменениях в своих законах и подзаконных актах, которые могут повлиять на защиту секретной информации в соответствии с настоящим Соглашением. Такие изменения национального законодательства не влияют на обязательства по настоящему Соглашению. В этих случаях Стороны проводят консультации относительно возможных поправок к настоящему Соглашению и других мер, которые могут оказаться необходимыми для поддержания защиты секретной информации, обмен которой происходит в соответствии с настоящим Соглашением.

СТАТЬЯ 4 – НАЦИОНАЛЬНЫЕ ОРГАНЫ БЕЗОПАСНОСТИ

1. Стороны уведомляют друг друга о национальных органах безопасности, отвечающих за выполнение настоящего Соглашения, и о любых последующих изменениях, касающихся этих органов.

2. В целях настоящего Соглашения национальными органами безопасности являются:

а. от США: директор программ международной безопасности Управления безопасности оборонных технологий аппарата заместителя министра обороны по военно-политическим вопросам Министерства обороны США; и

б. от Казахстана: Комитет национальной безопасности Республики Казахстан (КНБ). Контактным лицом от КНБ является начальник Департамента по защите государственных секретов.

3. Стороны могут заключать дополнительные исполнительные договоренности к настоящему Соглашению в случае возникновения необходимости в дополнительных мерах технической безопасности для защиты секретной информации, передаваемой получающей Стороне в ходе продажи военных товаров за границу или реализации программ сотрудничества, направленных на совместное производство или совместную разработку оборонных товаров или услуг. Такие исполнительные договоренности могут включать соглашения о специальных мерах безопасности или соглашения о промышленной безопасности.

СТАТЬЯ 5 – ОБОЗНАЧЕНИЕ СЕКРЕТНОЙ ИНФОРМАЦИИ

1. Секретная информация обозначается и, по возможности, штампуются и маркируется передающей Стороной одним из следующих грифов национальной

безопасности. В целях обеспечения эквивалентного обращения Стороны соглашаются об эквивалентности следующих грифов секретности:

| США | Казахстан |
|---------------------|---|
| TOP SECRET | СОВЕРШЕННО СЕКРЕТНО (TOP SECRET) |
| SECRET | СЕКРЕТНО (SECRET) |
| CONFIDENTIAL | НЕТ ЭКВИВАЛЕНТА (см. пункт 2 ниже) |

2. Секретная информация, обозначенная грифом «CONFIDENTIAL», передаваемая Соединенными Штатами Америки Казахстану, должна подлежать таким же мерам защиты, как и секретная информация, обозначаемая грифом «СЕКРЕТНО».

3. Секретная информация обозначается и, по возможности, штампуются или маркируется названием передающей Стороны.

СТАТЬЯ 6 – ОТВЕТСТВЕННОСТЬ ЗА СЕКРЕТНУЮ ИНФОРМАЦИЮ

Получающая Сторона несёт ответственность за защиту всей секретной информации передающей Стороны способом, по меньшей мере эквивалентным той защите, которую обеспечивает секретной информации передающая Сторона при нахождении секретной информации под её контролем. При перевозке передающая Сторона несёт ответственность за всю секретную информацию до момента формальной передачи секретной информации получающей Стороне на хранение.

СТАТЬЯ 7 – ЗАЩИТА СЕКРЕТНОЙ ИНФОРМАЦИИ

1. Ни одно физическое лицо не имеет права доступа к секретной информации только лишь в силу его ранга, положения, должности или ДП. Доступ к такой информации предоставляется отдельным лицам лишь на основе принципа служебной необходимости и при наличии требуемого ДП согласно предусмотренным нормам получающей Стороны.

2. За исключением случаев, когда настоящим Соглашением предусмотрено иное, получающая Сторона не раскрывает секретную информацию передающей Стороны какой-либо третьей стороне, включая правительству, лицу, фирме, учреждению, организации или иному юридическому лицу третьей стороны без предварительного письменного согласия передающей Стороны.

3. Получающая Сторона не использует и не разрешает использовать секретную информацию передающей Стороны с какой-либо иной целью, кроме

той, для которой она была предоставлена, без предварительного письменного согласия передающей Стороны.

4. Получающая Сторона уважает любые частные права, связанные с секретной информацией передающей Стороны, в том числе права в отношении патентов, авторских прав или коммерческих тайн, и не распространяет, использует, обменивает или разглашает такую секретную информацию способом, несовместимым с этими правами, без предварительного письменного разрешения владельца этих прав.

5. Получающая Сторона обеспечивает ведение каждым объектом или учреждением, имеющим дело с секретной информацией, которая подпадает под действие настоящего Соглашения, списка физических лиц на этом объекте или в этом учреждении, имеющих разрешение на доступ к такой информации.

6. Каждая Сторона разрабатывает порядок учёта и контроля, регулирующие вопросы распространения секретной информации и доступа к ней.

7. Каждая Сторона соблюдает все ограничения на использование, раскрытие, разглашение и доступ к секретной информации, что может обуславливаться передающей Стороной во время раскрытия секретной информации. Если одна из Сторон не способна соблюдать указанные ограничения, эта Сторона незамедлительно проводит консультации с другой Стороной и предпринимает все дозволенные законом меры, направленные на предотвращение или сведение к минимуму любого такого использования, раскрытия, разглашения или доступа.

СТАТЬЯ 8 – ДОПУСК ПЕРСОНАЛА

1. Стороны обеспечивают получение необходимой степени ДП всеми лицами, которым в ходе выполнения их служебных обязанностей требуется допуск, или же чьи обязанности или функции делают возможным получение доступа к секретной информации в соответствии с настоящим Соглашением, перед получением ими доступа к такой информации.

2. Присваивающая ДП Сторона проводит необходимое расследование с достаточной степенью подробности в целях определения пригодности данного лица для получения доступа к секретной информации. Решение о присвоении ДП будет приниматься в соответствии с национальным законодательством присваивающей Стороны.

3. Перед передачей секретной информации официальным лицом или представителем одной Стороны официальному лицу или представителю другой Стороны получающая Сторона предоставляет передающей Стороне заверения в наличии у своего официального лица или представителя ДП необходимого уровня и в соблюдении принципа служебной необходимости, а также в том, что секретная информация будет защищаться получающей Стороной в соответствии с настоящим Соглашением.

СТАТЬЯ 9 – РАСКРЫТИЕ СЕКРЕТНОЙ ИНФОРМАЦИИ ИСПОЛНИТЕЛЯМ

1. Секретная информация, получаемая получающей Стороной, может предоставляться получающей Стороной исполнителю или вероятному исполнителю, обязанности которого требуют доступа к такой информации, с предварительного письменного согласия передающей Стороны. Перед передачей какой-либо секретной информации исполнителю или вероятному исполнителю получающая Сторона:

а. Подтверждает, что такой исполнитель или вероятный исполнитель, а также предприятие исполнителя располагают возможностью обеспечить защиту информации в соответствии с условиями настоящего Соглашения;

б. Подтверждает, что такому исполнителю или вероятному исполнителю, а также предприятию исполнителя выданы соответствующие ДП и РПСР, в зависимости от обстоятельств;

с. Подтверждает, что у такого исполнителя или вероятного исполнителя имеется в наличии порядок обеспечения того, чтобы все лица, имеющие доступ к информации, были проинформированы о своей ответственности за защиту информации в соответствии с применимыми законами и подзаконными актами;

д. Проводит периодические инспекции безопасности получивших РПСР объектов с тем, чтобы обеспечить охрану информации согласно требованиям настоящего Соглашения;

е. Подтверждает, что у исполнителя или вероятного исполнителя имеется в наличии порядок обеспечения того, чтобы доступ к информации ограничивался теми лицами, у которых есть в ней служебная необходимость.

СТАТЬЯ 10 – ДОГОВОРЫ О ПРОВЕДЕНИИ СЕКРЕТНЫХ РАБОТ

1. Когда Сторона предполагает заключить договор о проведении секретных работ, или даёт разрешение исполнителю в своей стране заключить договор о проведении секретных работ, которому присвоен уровень секретности CONFIDENTIAL/СЕКРЕТНО или выше, с исполнителем в стране другой Стороны, та Сторона, которая заключает или дает разрешение исполнителю заключить договор о проведении секретных работ, должна запросить подтверждение о выдаче РПСР у национального органа безопасности другой Стороны. Национальный орган безопасности Стороны, получившей запрос, следит за тем, чтобы выполнение подрядчиком всех требований к безопасности соответствовало применимым законам и подзаконным актам, и принимает все необходимые меры для обеспечения этого.

2. Национальный орган безопасности Стороны, заключающей договор о проведении секретных работ, который должен выполняться в стране другой Стороны, включает в договор о проведении секретных работ, в запрос на предложение или в документ о субподряде необходимые оговорки о безопасности и другие соответствующие положения, в том числе о расходах на

обеспечение безопасности. Сюда входят положения, требующие от всех исполнителей включения соответствующих оговорок о безопасности в свои документы о субподряде.

СТАТЬЯ 11 – ОТВЕТСТВЕННОСТЬ ЗА ОБЪЕКТЫ

Каждая Сторона несет ответственность за безопасность всех государственных и частных объектов и учреждений, где она хранит секретную информацию другой Стороны, и обеспечивает наличие на таких объектах или в таких учреждениях квалифицированных и получивших надлежащий допуск лиц, назначение которых предполагает наличие ответственности и полномочий в области контроля за такой информацией и ее защиты.

СТАТЬЯ 12 – ХРАНЕНИЕ СЕКРЕТНОЙ ИНФОРМАЦИИ

Секретная информация, которой обмениваются Стороны, хранится, таким образом, который обеспечивает доступ к ней только лиц, имеющих на это разрешение.

СТАТЬЯ 13 – ПЕРЕДАЧА

1. Секретная информация передаётся между Сторонами по межправительственным каналам или по другим каналам, взаимно одобренным заранее в письменном виде, в соответствии с национальными законодательствами Сторон.

2. Минимальные требования к безопасности секретной информации в ходе её передачи нижеследующие:

а. Документы или другие носители:

(1) Документы или другие носители, содержащие секретную информацию, передаются в двойных запечатанных конвертах. На внутреннем конверте указывается только гриф секретности документов или других носителей, а также адрес предполагаемого получателя. На внешнем конверте указывается адрес предполагаемого получателя, адрес отправителя и, в случае необходимости, регистрационный номер документа.

(2) На внешнем конверте не указывается уровень секретности вложенных в него документов или других носителей. Двойной запечатанный конверт передаётся в соответствии с предписанным порядком Сторон.

(3) Получатели пакетов, содержащих документы или другие носители, в/на которых содержится передаваемая между Сторонами секретная информация, готовят расписки, причём такие расписки подписываются последним получателем и возвращаются отправителю.

б. Материалы:

(1) Материалы, в том числе оборудование, содержащие секретную информацию, перевозятся опломбированными крытыми транспортными средствами, либо же надёжно упаковываются или защищаются иным способом

с тем, чтобы предотвратить распознавание их формы, размера или содержимого, и они находятся под постоянным контролем для предотвращения доступа к ним неуполномоченных лиц.

(2) Материалы, в том числе оборудование, содержащие секретную информацию и подлежащие временному хранению в ожидании отправки, размещаются в защищённых хранилищах. Такие хранилища охраняются при помощи оборудования обнаружения несанкционированного проникновения или находятся под постоянным наблюдением охранников с необходимым ДП. Доступ в защищённые хранилища имеет только уполномоченный персонал, получивший необходимый ДП.

(3) При переходе материалов, в том числе оборудования, содержащих секретную информацию, из рук в руки в ходе перевозки вручаются расписки, причём расписка за такие материалы подписывается последним получателем и возвращается отправителю.

с. Электронная передача:

(1) Секретная информация с грифом уровня CONFIDENTIAL/ СЕКРЕТНО или выше, подлежащая электронной передаче, передаётся защищёнными средствами, одобренными национальным органом безопасности каждой из Сторон.

СТАТЬЯ 14 – ВИЗИТЫ НА ОБЪЕКТЫ И УЧРЕЖДЕНИЯ СТОРОН

1. Визиты представителей одной Стороны на объекты и учреждения другой Стороны, требующие доступа к секретной информации, или визиты, для которых требуется наличие ДП, должны ограничиваться лишь визитами, которые необходимы в официальных целях. Разрешение выдаётся только представителям, имеющим действительный ДП.

2. Разрешение на визит на такие объекты и в такие учреждения выдаётся только той Стороной, на территории которой находится объект или учреждение для посещения. Принимающая Сторона или её назначенные официальные представители несут ответственность за извещение объекта или учреждения о предполагаемом визите, а также объёме и максимальном уровне секретности информации, которая может быть предоставлена посетителю.

3. Запросы на проведение визитов представителями Сторон подаются Посольством США в Нур-Султане в случае американских посетителей и Посольством Республики Казахстан в Вашингтоне в случае посетителей из Казахстана.

СТАТЬЯ 15 – ВИЗИТЫ С ЦЕЛЬЮ ПРОВЕРКИ БЕЗОПАСНОСТИ

Выполнение требований к безопасности, изложенных в настоящем Соглашении, может проверяться путём взаимных визитов представителей

служб безопасности Сторон. Представителям служб безопасности каждой из Сторон разрешается, после проведения предварительных консультаций, посещать с визитом другую Сторону для обсуждения и наблюдения имплементационных порядков другой Стороны в интересах достижения эквивалентности систем безопасности. Принимающая Сторона оказывает содействие посещающим представителям служб безопасности в определении адекватности защиты секретной информации, полученной от другой Стороны.

СТАТЬЯ 16 – СТАНДАРТЫ БЕЗОПАСНОСТИ

По запросу каждая Сторона предоставляет другой Стороне информацию о своих стандартах безопасности, правилах и порядках охраны секретной информации.

СТАТЬЯ 17 – ВОСПРОИЗВЕДЕНИЕ СЕКРЕТНОЙ ИНФОРМАЦИИ

При воспроизведении секретной информации на каждой её копии воспроизводятся, проштамповываются или обозначаются все соответствующие оригинальные грифы секретности. Такие копии подлежат тем же самым ограничениям, что и оригинальная информация. Количество копий ограничивается минимальным числом, необходимым для официальных целей.

СТАТЬЯ 18 – УНИЧТОЖЕНИЕ СЕКРЕТНОЙ ИНФОРМАЦИИ

1. Документы и другие носители, содержащие секретную информацию, уничтожаются путем сжигания, измельчения, размалывания или другим способом, предотвращающим восстановление содержащейся в них секретной информации.

2. Материалы, включая оборудование, содержащие секретную информацию, уничтожаются тем способом, который обеспечивает невозможность их опознания и исключает полное или частичное восстановление секретной информации.

СТАТЬЯ 19 – ПОНИЖЕНИЕ УРОВНЯ СЕКРЕТНОСТИ И РАССЕКРЕЧИВАНИЕ

1. Стороны согласны в том, что уровень секретности секретной информации следует понижать, как только такая информация перестанет требовать более высокой степени защиты, или ее следует рассекречивать, как

только такая информация не будет больше требовать защиты от несанкционированного раскрытия.

2. Передающая Сторона имеет все полномочия действовать по собственному усмотрению в отношении понижения уровня секретности или рассекречивания своей секретной информации. Получающая Сторона не понижает уровень секретности секретной информации, полученной от передающей Стороны, и не рассекречивает ее, невзирая на какие бы то ни было указания по рассекречиванию, присутствующие на документе, без предварительного письменного согласия передающей Стороны.

СТАТЬЯ 20 – УТРАТА ИЛИ РАЗГЛАШЕНИЕ

Получающая Сторона незамедлительно уведомляет передающую Сторону об обнаружении любых фактов утраты или разглашения, а также возможных фактах утраты или разглашения секретной информации передающей Стороны. В случае фактической или возможной утраты или разглашения такой информации получающая Сторона незамедлительно начинает расследование в целях определения обстоятельств фактической или возможной утраты или разглашения. Результаты расследования и информация о мерах, принятых для предотвращения повторения таких случаев, предоставляются передающей Стороне.

СТАТЬЯ 21 – СПОРЫ

Разногласия между Сторонами, возникающие в ходе реализации настоящего Соглашения или связанные с ним урегулируются исключительно посредством консультаций между Сторонами и не передаются для урегулирования ни в национальный суд, ни в международный суд, ни какому-либо другому физическому или юридическому лицу.

СТАТЬЯ 22 – ЗАТРАТЫ

Каждая Сторона несёт ответственность за свои собственные затраты, понесённые ею в ходе реализации настоящего Соглашения. Все обязательства Сторон в рамках настоящего Соглашения зависят от наличия средств.

СТАТЬЯ 23 – ПОПРАВКИ

Изменения и дополнения в настоящее Соглашение могут быть внесены только с обоюдного согласия Сторон. Любые изменения и дополнения должны быть оформлены как отдельный документ, который вступает в силу в соответствии с пунктом 1 статьи 24 настоящего Соглашения.

СТАТЬЯ 24 – ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

1. Настоящее Соглашение и любые изменения и дополнения в настоящее Соглашение вступают в силу с даты последней дипломатической ноты в процессе обмена дипломатическими нотами, в которых Стороны уведомляют о том, что каждая Сторона завершила свои внутригосударственные процедуры, необходимые для вступления в силу настоящего Соглашения или любого изменения к настоящему Соглашению.

2. Любая Сторона может прекратить действие настоящего Соглашения, уведомив другую Сторону о своём намерении прекратить его действие в письменном виде за девяносто дней по дипломатическим каналам.

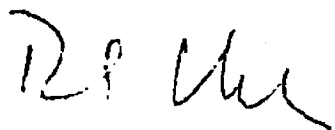
3. Несмотря на прекращение действия настоящего Соглашения, вся секретная информация, обмен которой имел место или которая была предоставлена иным образом в соответствии с настоящим Соглашением, продолжает защищаться согласно положениям настоящего Соглашения.

В УДОСТОВЕРЕНИЕ ЧЕГО нижеподписавшиеся, должным образом на то уполномоченные своими соответствующими Правительствами, подписали настоящее Соглашение.

СОВЕРШЕНО в двух экземплярах в городе Нур-Султане «20» августа 2019 года на английском, казахском, и русском языках, причем все тексты имеют одинаковую силу.

В случае возникновения разногласий при толковании положений настоящего Соглашения, текст на английском языке имеет преимущественную силу.

За Правительство
Соединенных Штатов Америки:



За Правительство
Республики Казахстан:

