AGREEMENT BETWEEN
THE GOVERNMENT OF JAPAN
AND THE GOVERNMENT OF UKRAINE
ON THE SECURITY OF INFORMATION

Preamble

The Government of Japan and the Government of Ukraine (hereinafter referred to as "the Parties" and separately as a "Party"),

Wishing to ensure the reciprocal protection of classified information exchanged between them;

Have agreed as follows:

ARTICLE 1
Definitions

For the purposes of this Agreement:

a. "Classified Information" means information, in any form, including oral, visual, electronic, magnetic or documentary forms, and equipment or technology, which requires protection against unauthorized disclosure in the interests of national security of the Providing Party and which is subject to a Security Classification and generated by, or for the use of, or under the jurisdiction of the Competent Authorities of the Providing Party;

b. "Competent Authorities" means, in relation to Japan, the government agencies, and, in relation to Ukraine, the state authorities, which are respectively designated for the purposes of this Agreement by each Party as the authorities responsible, within their respective competence under the national laws and regulations, for conducting activities related to Classified Information, including its protection;

c. “Contractor” means an individual or an entity, including a subcontractor, that performs a contract with the Receiving Party;

d. “Need to Know” means the need to have access to Classified Information and Transmitted Classified Information for the performance of officially assigned duties;

e. “Personnel Security Clearance” means an eligibility for handling securely Classified Information and Transmitted Classified Information granted to individuals in accordance with each Party’s appropriate procedures;

f. “Providing Party” means the Party, including the Competent Authorities designated in accordance with subparagraph b. of this Article, which transmits Classified Information to the Receiving Party;

g. “Receiving Party” means the Party, including the Competent Authorities designated in accordance with subparagraph b. of this Article, to which Classified Information is transmitted by the Providing Party;

h. “Security Classification” means the identification assigned by a Party to indicate the necessary level of protection that information must be afforded;

i. “Third Party” means any government, individual, firm, institution, organization, other entity of a third country, or an international organization not a party to this Agreement; and

j. “Transmitted Classified Information” means Classified Information which is transmitted between the Competent Authorities of the Parties. Classified Information becomes Transmitted Classified Information upon receipt by the Receiving Party in accordance with its national laws and regulations.

ARTICLE 2
Protection of Transmitted Classified Information

Transmitted Classified Information shall be protected under the terms set forth herein, provided that such terms are consistent with the national laws and regulations of the Receiving Party.

ARTICLE 3
Changes in National Laws and Regulations

Each Party shall notify the other Party of any changes to its national laws and regulations that would affect the protection of Transmitted Classified Information under this Agreement. In such a case, the Parties shall consult each other as provided for in Article 19, to consider possible amendments to this Agreement. In the interim, Transmitted Classified Information shall continue to be protected according to the provisions of this Agreement, provided that those provisions are consistent with the national laws and regulations of the Receiving Party, unless otherwise approved in writing by the Providing Party.

ARTICLE 4
Security Classifications and Markings

1. Classified Information to be provided under this Agreement shall be marked with one of the following Security Classifications:

For the Government of Japan, Classified Information is marked GOKUHI (KIMITSU) 極秘 (機密), TOKUTEI HIMITSU (KIMITSU) 特定秘密 (機密), GOKUHI 極秘, TOKUTEI HIMITSU 特定秘密, or HI 秘;

For the Government of Ukraine, Classified Information is marked Особливої важливості, Цілком таємно, or Таємно.

2. For Classified Information where a marking is not physically possible, the Providing Party shall inform the Receiving Party of the Security Classification. If the Receiving Party so requests, the Providing Party shall inform the Security Classification in writing.

3. The Receiving Party shall mark, where practicable, all Transmitted Classified Information with the name of the Providing Party and the corresponding Security Classification of the Receiving Party, as described in paragraph 4 of this Article.

4. The corresponding Security Classifications are:

In Japan	In Ukraine	Note: Equivalent in English
GOKUHI (KIMITSU) 極秘 (機密) or TOKUTEI HIMITSU (KIMITSU) 特定秘密(機密)	Особливої важливості	TOP SECRET
GOKUHI 極秘 or TOKUTEI HIMITSU 特定秘密	Цілком таємно	SECRET
HI 秘	Таємно	CONFIDENTIAL

ARTICLE 5

National Security Authorities and Competent Authorities

1. The National Security Authorities shall be:

In relation to Japan:

Ministry of Foreign Affairs;

In relation to Ukraine:

Security Service of Ukraine.

2. The National Security Authorities shall serve as a point of coordination and liaison with regard to the implementation and interpretation of this Agreement.

3. The National Security Authorities and the Competent Authorities shall monitor the implementation of this Agreement within their competence.

4. The Parties shall notify each other in writing of their respective Competent Authorities through diplomatic channels.

ARTICLE 6
Principles for Protecting Transmitted Classified Information

1. The Receiving Party shall not release Transmitted Classified Information to any Third Party without the prior written approval of the Providing Party.

2. The Receiving Party shall, in accordance with its national laws and regulations, afford Transmitted Classified Information a level of protection equal to that which it affords its own Classified Information at the corresponding level of Security Classification.

3. The Receiving Party shall not use Transmitted Classified Information for any purpose other than that for which it is provided without the prior written approval of the Providing Party.

4. The Receiving Party shall observe intellectual property rights such as patents, copyrights, or trade secrets applicable to Transmitted Classified Information, in accordance with its national laws and regulations.

5. Each Party shall maintain a register of individuals with a Personnel Security Clearance and who are authorized to have access to Classified Information and Transmitted Classified Information, in accordance with its national laws and regulations.

6. The Receiving Party shall establish procedures for the identification, location, inventory and control of Transmitted Classified Information to manage the dissemination of and access to Transmitted Classified Information.

7. The Providing Party shall inform the Receiving Party of any subsequent change in the Security Classification of the Classified Information which it has provided to the Receiving Party.

ARTICLE 7

Access to Transmitted Classified Information

1. No individual shall be entitled to have access to Transmitted Classified Information solely by virtue of rank, appointment, or a Personnel Security Clearance.

2. Access to Transmitted Classified Information shall be granted only to those individuals who have Need to Know and who have been granted a Personnel Security Clearance in accordance with the national laws, regulations and procedures of the Receiving Party.

3. The Receiving Party shall take appropriate measures to ensure that the determination on the granting of a Personnel Security Clearance to an individual is consistent with the interests of national security and based upon all relevant information indicating whether the individual is trustworthy and reliable in the handling of Transmitted Classified Information, in accordance with its national laws and regulations.

4. The Receiving Party shall take appropriate measures to ensure that the criteria referred to in the preceding paragraph have been met, in accordance with its national laws, regulations and procedures, in respect of any individual to be granted access to Transmitted Classified Information.

5. Before a representative of the Providing Party provides Classified Information to a representative of the Receiving Party, the Providing Party shall obtain an assurance from the relevant Competent Authority of the Receiving Party that the proposed recipient has Need to Know and holds the necessary level of Personnel Security Clearance appropriate to the corresponding level of Security Classification in accordance with Article 4.

ARTICLE 8

Visit Procedures

1. Visits that involve access by individuals of the Competent Authority of one Party to Classified Information held by the Competent Authority of the other Party shall be undertaken only with the prior approval of the Competent Authority of the other Party. Approval for such visits may be granted only to those individuals who have Need to Know and hold the necessary level of Personnel Security Clearance pursuant to Article 7.

2. Requests for visits shall be submitted by the relevant Competent Authority of the visiting Party through Government to Government channels to the relevant Competent Authority of the other Party and shall include verification of the fact that the visiting individuals have Need to Know and hold the necessary level of Personnel Security Clearance pursuant to Article 7.

ARTICLE 9
Transmission of Classified Information

Classified Information shall be transmitted between the Parties through Government to Government channels. The Providing Party shall be responsible for custody, control, and security of all Classified Information until its receipt by the Receiving Party, subject to the national laws and regulations of the Providing Party.

ARTICLE 10
Security Requirements during Transmission

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

a. Classified Information in the form of documents or other media:

(i) Classified Information shall be transmitted in a sealed or tamper-indicating envelope enclosed within another sealed or tamper-indicating envelope or within a security pouch, the innermost envelope bearing only the Security Classification of the documents or other media and the organizational address of the intended recipient, the outer envelope or the security pouch bearing the organizational address of the recipient, the organizational address of the sender, and the registration number, if applicable.

(ii) No indication of the Security Classification of the enclosed documents or other media shall be shown on the outer envelope or the security pouch.

(iii) Receipts shall be prepared for packages containing Classified Information. A receipt for the enclosed Classified Information shall be signed by the Receiving Party's final recipient and returned to the Providing Party's sender.

b. Classified Information in the form of, or which is contained in, equipment:

(i) Classified Information shall be transmitted in sealed and covered vehicles, or be securely packaged or protected, in order to prevent identification of its contents and kept under continuous control to prevent access by unauthorized individuals.

(ii) Classified Information that is awaiting shipment shall be placed in protected storage areas that provide protection commensurate with the level of Security Classification of the Classified Information. Only authorized individuals with the necessary level of Personnel Security Clearance shall have access to the equipment.

(iii) Receipts shall be obtained on every occasion when Classified Information changes hands en route and is delivered to the Receiving Party's final recipient. All receipts shall be returned to the Providing Party's sender.

c. Electronic Transmissions:

Classified Information shall be protected during transmission using encryption appropriate for the relevant level of Security Classification. Information systems' standards for processing or storing Transmitted Classified Information or conveying Classified Information shall receive security accreditation by the appropriate authority of the Party employing the system.

ARTICLE 11
Security of Facilities

Each Party shall be responsible for the security of all facilities of the Competent Authorities where Transmitted Classified Information is kept and shall ensure that for each such facility officials are appointed who shall have the responsibility and authority for the control and protection of Transmitted Classified Information.

ARTICLE 12
Storage of Transmitted Classified Information

The Receiving Party shall store Transmitted Classified Information in a manner that ensures access is limited to authorized individuals pursuant to Article 7.

ARTICLE 13
Destruction of Transmitted Classified Information

Destruction of Transmitted Classified Information shall be done so in a manner that prevents its reconstruction in whole or in part in accordance with the national laws and regulations of the Receiving Party.

ARTICLE 14
Reproduction of Transmitted Classified Information

When the Receiving Party reproduces Transmitted Classified Information in the form of documents or other media, it shall also reproduce all original Security Classification markings thereon or mark them on each copy. The Receiving Party shall place such reproduced Transmitted Classified Information under the same controls as the original Transmitted Classified Information. The Receiving Party shall limit the number of copies to that required for official purposes.

ARTICLE 15

Translation of Transmitted Classified Information

The Receiving Party shall ensure that any translation of Transmitted Classified Information is carried out by individuals who have Need to Know and hold the necessary level of Personnel Security Clearance pursuant to Article 7. The Receiving Party shall keep the number of copies of a translation to a minimum and control any distribution. Such translations shall bear markings of the Security Classification of the Receiving Party equivalent to the Security Classification of the Providing Party and suitable notation in the language into which such translation was made indicating that such translation contains Transmitted Classified Information. The Receiving Party shall place such translations under the same controls as the original Transmitted Classified Information.

ARTICLE 16

Release of Transmitted Classified Information to Contractors

Prior to the release to a Contractor of any Transmitted Classified Information, the Receiving Party shall, subject to its national laws and regulations, take appropriate measures to ensure that:

a. the Contractor's facilities have the capability to protect Transmitted Classified Information at the relevant level of Security Classification;

b. all individuals having access to Transmitted Classified Information are informed of their responsibilities to protect Transmitted Classified Information;

c. information generated by Contractors using Transmitted Classified Information is marked with the comparable level of Security Classification of the Receiving Party and receives comparable protection to the original Transmitted Classified Information;

d. initial and periodic security inspections are carried out by the Receiving Party at each Contractor's facility where Transmitted Classified Information is stored or accessed to ensure that it is protected in the same manner as required in relevant provisions of this Agreement;

e. a register of individuals with a Personnel Security Clearance and who are authorized to have access to Transmitted Classified Information is maintained at each Contractor's facility;

f. individuals are appointed at each Contractor's facility who shall have the responsibility and authority for the control and protection of Transmitted Classified Information; and

g. Contractors apply and maintain measures for the protection of Transmitted Classified Information in the same manner as required in the relevant provisions of this Agreement.

ARTICLE 17
Loss or Compromise of Transmitted Classified Information

1. The Providing Party shall be informed immediately of all losses or compromises, as well as suspected losses or compromises, of Transmitted Classified Information, and the Receiving Party shall investigate to determine the circumstances.

2. The results of the investigation and information regarding measures taken to prevent recurrence shall be provided in writing to the Providing Party.

ARTICLE 18
Implementing Arrangements

Competent Authorities, within their competence, may mutually determine Implementing Arrangements, which are subordinate to this Agreement and which shall specify supplementary provisions.

ARTICLE 19
Disputes and Consultation

1. The Parties shall consult each other regarding the implementation of this Agreement.

2. Any matter relating to the interpretation or application of this Agreement and any Implementing Arrangements shall be resolved solely through consultation between the Parties.

3. The Competent Authorities of the Parties shall settle disputes that may arise concerning the implementation of any Implementing Arrangements through consultation.

4. Where a dispute cannot be settled under the provisions of paragraph 3 of this Article, the dispute shall be settled in accordance with the provisions of paragraph 2 of this Article.

ARTICLE 20
Visits by Security Representatives

Implementation of the foregoing security requirements can be promoted through reciprocal visits by security representatives of the Parties. Accordingly, with the mutual consent of the Parties, security representatives of each Party may be permitted to make visits to facilities of the other Party to discuss their respective security procedures and observe their implementation in the interests of achieving reasonable comparability of their respective security systems.

ARTICLE 21
Costs

Each Party shall bear its own costs incurred in the course of implementing its obligations under this Agreement, in accordance with its national laws and regulations and within the limit of its annual budgetary appropriations.

ARTICLE 22
Entry into Force, Amendment, Duration and Termination

1. Each Party shall send in writing through diplomatic channels to the other Party the notification confirming that its internal procedures necessary for the entry into force of this Agreement have been completed. This Agreement shall enter into force on the thirtieth day after the date of receipt of the latter notification.

2. This Agreement may be amended by written agreement between the Parties.

3. This Agreement shall remain in force for a period of one year and shall be automatically extended annually thereafter unless either Party notifies the other Party in writing through diplomatic channels at least ninety days in advance of its intention to terminate this Agreement.

4. Notwithstanding the termination of this Agreement, all Transmitted Classified Information provided pursuant to this Agreement shall continue to be protected according to the terms set forth in this Agreement.

Done at Kyiv this sixteenth day of November 2024 year in duplicate, in the Japanese, Ukrainian, and English languages, all three texts being equally authentic. In case of any divergence of interpretation of the provisions of this Agreement, the English text shall prevail.

For the Government of Japan:	For the Government of Ukraine: