This Cybersecurity Agreement (the "**Agreement**")

PARTIES		
"Cargolux"		**"Service Provider"**
Legal Name	Cargolux Airlines International S.A.	Refers to the Company, including all its affiliates, subsidiaries, personnel, subcontractors that provide or support the delivery of IT Services to Cargolux under the relevant agreement(s)
Place of Incorporation	Grand-Duchy of Luxembourg	
Registered Office	L-2990 Sandweiler, Aéroport de Luxembourg, Grand-Duchy of Luxembourg	
Registration Number	B 8916	
Each party being referred to individually as the "**Party**" or collectively as the "**Parties**".		

WHEREAS

a) The Service Provider is a service provider performing critical IT Services (as defined below) to Cargolux in accordance with the respective service agreements entered into by and between the Parties.

b) Considering the recent regulatory developments on cybersecurity, the Parties wish to clarify cybersecurity aspects of all IT Services to ensure that they are performed in compliance with the terms and conditions of this Agreement.

c) Unless specified otherwise in writing, this Agreement covers all present and future IT Services performed by the Service Provider, no matter performed by the Service Provider in its own name or by its Affiliates, employees, representatives, agents or subcontractor, to the benefits of Cargolux or its Affiliates. Notwithstanding the foregoing, Cargolux may amend this Agreement at any time and will notify the Service Provider of such amendments. The amendments will become effective from the date indicated in the notice.

d) Cargolux has established three contractual Criticality Levels applicable depending on its relationship with the Service Provider, and considering the type of IT Services outsourced. The Service Provider hereby acknowledges and agrees that only the Criticality Level expressly designated in the Main Agreement shall be binding. Any Criticality Level not expressly identified shall not create any obligations for the Provider.

cargolux

Standard Terms

The following Standard Terms shall apply to this Agreement, the Main Agreement and standardly to all Criticality Levels:

1. DEFINITIONS

For the purposes of this Agreement the terms:

a) "**Affiliate**" shall mean any entity controlling, controlled by, or under common control with a Party. For the purposes of this clause, "control" shall mean holding directly or indirectly at least 50 % of the shares, or having the power, by way of voting rights or otherwise, to direct, manage or restrict the business of an entity.

b) "**Applicable Rules**" shall mean applicable information security laws, regulations and requirements, including but not limited to Regulation (EU) 2023/203 "Part-IS", Directive (EU) 2022/2555 (NIS2) and applicable national laws and regulations transposing NIS2, applicable aviation industry standards, regulatory requirements, and the terms of the Agreement between the Parties.

c) "**Confidential Information**" shall mean any and all confidential information regardless of form, whether oral, written, electronic or otherwise, disclosed or made available (directly or indirectly) by one Party or its Affiliates, agents, employees, officers, representatives or advisors (the "Discloser") to the other Party or its Affiliates, agents, employees, officers, representatives or advisors (the "Recipient") in connection with the performance of the IT Services, including, without limitation, any information (whether financial, technical, commercial, legal, scientific, personal or other), original ideas, assumptions, marketing plans, distribution channels, processes, research, trade secrets, services, customers, suppliers and other business partners, markets, personal data, and any statistics, reports, analyses, business projections or other studies relating to the Party or any of its Affiliates which contain or otherwise reflect such information.

d) "**Competent Authority**" shall mean any competent supervisory authority/ies relevant to the performance of the concerned IT Services.

e) "**Competent Personnel**" shall mean personnel assigned by the Service Provider in providing the IT Services.

f) "**Criticality Level**" shall mean any of the three contractual criticality levels defined under this Agreement, namely "Level 1", "Level 2" and "Level 3: Non-Critical", each with specific terms and conditions describing the Service Provider's obligations in relation to the performance of the IT Services.

g) "**Days**" shall mean calendar days, unless specified otherwise.

h) "**Information Security Event**" means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

i) "**IT Services**" shall mean any supply of hardware, software or any other IT services with or without access to Cargolux infrastructure or data performed by the Service Provider to Cargolux or its Affiliates.

j) "**Main Agreement**" shall mean the service agreement (s) entered into by and between the Parties concerning the provision of the IT Services.

2. CONFIDENTIALITY

Notwithstanding anything contrary agreed in the Main Agreement, the Parties agree to maintain in absolute confidence any Confidential Information and agree not to divulge such information to any third party without the prior written consent of the other Party for a period of not less than five (5) years following expiry or termination hereof.

3. TERM

This Agreement shall remain in full force effective as of March 27th, 2026 (the "**Effective Date**") and last for an indefinite period until the termination of each relevant Main Agreement.

4. GOVERNING LAW AND JURISDICTION

4.1 This Agreement is governed by and shall be construed in accordance with the Luxembourg law.

4.2 Any dispute arising out of or in connection with this Agreement shall be exclusively submitted to the Luxembourg jurisdiction with exclusion of conflicts of law principles.

5. MISCELLANEOUS

5.1. Neither Party hereto shall assign this Agreement or any part hereof or any benefit or interest herein without having first obtained the prior written consent of the other Party.

5.2. If any provision of this Agreement is held to be illegal, invalid or unenforceable, that provision shall (so far as it is illegal, invalid or unenforceable) be given no effect and shall be deemed not to be included in this Agreement, but that shall not affect the legality, validity or enforceability of any other provision of this Agreement.

5.3. Unless otherwise provided by the Main Agreement signed between the Parties regarding IT Services, neither this Agreement nor any disclosure of Confidential Information hereunder grants the Recipient any right, license, interest or title in, to or under the Confidential Information. No license is hereby granted to the Recipient under

any trademark, copyright, patent, trade secret or other proprietary right of the Discloser. Title to the Confidential Information shall remain solely with the Discloser.

5.4. No information which has been given by either Party is intended to form the basis of any invitation, offer or contract for the provision of services. Nothing in this Agreement shall operate to create a partnership, joint venture, agency or other business relationship between the Parties nor shall the Recipient have any authority to act in the name of or on behalf of the Information Provider.

5.5. Cargolux reserves the right to unilaterally amend and modify the terms and conditions contained in this Agreement in order to comply with any existing or future Applicable Rules. In the event of any such modifications, Cargolux will notify the Service Provider and the new terms and conditions will apply to all Main Agreements, effective as of the date indicated in the notice. Notwithstanding the foregoing, Cargolux will act in good faith and make all reasonable efforts to modify the terms and conditions only where deemed necessary.

5.6. This Agreement governs all the Cybersecurity obligations related to the IT Services. In case of any conflict with any clauses in the Main Agreement, the relevant clauses in this Agreement prevail.

Specific Terms

The following Specific Terms shall apply to this Agreement, the Main Agreement and specifically and independently to each of the relevant Criticality Level:

LEVEL 1

1. UNDERTAKINGS

1.1 Cargolux has developed its information security system to adhere to the requirements as specified in the Applicable Rules. The Service Provider shall cooperate with Cargolux in maintaining its adherence to these requirements, and the Service Provider shall not, through its performance under its commitments to Cargolux, negatively impact this information security system established by Cargolux.

1.2 When performing the IT Services, the Service Provider shall comply with the Applicable Rules, implement and maintain appropriate physical and logical security measures, internal controls intended to protect Cargolux's data, services and infrastructure in its environments against accidental, unauthorized alteration, dissemination or access, as well as unlawful process.

1.3 The Service Provider shall provide timely notice of any changes regarding (i) its networks (including enhancement); (ii) the use of new technologies; (iii) the adoption of new products or newer versions or releases; (iv) the development of new tools and environments; (v) any change to physical location of service facilities; (vi) any change of sub-suppliers; (vii) any sub-contracting to another supplier; or (viii) any change to its policies and procedures that may affect the information security of either Party or the delivery of the IT Services. Following such notice, the Parties shall review and will equitably adjust the terms of their commitment as necessary to appropriately address risk.

2. PERSONAL REQUIREMENTS *(in case of consultancy IT Services)*

2.1 The Service Provider ensures that the Competent Personnel must:

a) successfully complete the Cargolux Information Security and Data related training at the beginning of the concerned IT Services;
b) successfully perform an enhanced background check as required by the regulation when being granted with unsupervised administrative rights;

c) exclusively carry out the mission within the assets to which they have been granted access and shall report any access that is not necessary for the completion of the mission;

d) refrain from any attempt, on its own or through unauthorized third parties, to retrieve or interfere with any information or data without the prior authorization of Cargolux.

2.2 The Service Provider undertakes to ensure compliance by its Competent Personnel of the Service Provider's undertakings hereunder.

3. BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

3.1 The Service Provider shall design, implement and maintain a Business Continuity Plan ("BCP") and Disaster Recovery Plan ("DRP") that meet Cargolux's response time and recovery capabilities for the provision of the IT Services, defined in the table below. This includes without limitation: i) high availability solutions to mitigate hardware failures, single point of failure, availability zone outage, redundant infrastructure and automated failover mechanisms, ii) data redundancy and backup strategies to protect against data loss or extorsion, performed regularly and retained for a minimum of 30 days aligned with RPO, iii) a DR testing program including annual full scale tests, tabletop exercises, with documented results and corrective actions shared with Cargolux.

Recovery Time Objective (RTO) The maximum acceptable time allowed for the recovery of the IT Service after a crisis situation	4h
Recovery Point Objective (RPO) Point to which information and data used by an IT Service is restored to enable the IT Service to operate on resumption	4h

In the event of any inconsistency or conflict between the response time defined in this Agreement and the Main Agreement, the RTO and RPO already defined in the Main Agreement shall prevail.

3.2 Where a risk would have been identified during the implementation, maintenance or testing of the BCP and DRP, the Parties shall promptly inform each other of such risk without undue delay. The risks identified should be addressed through a risk treatment plan to be executed within the timeframe as requested by Cargolux.

3.3 The Service Provider shall proactively manage third-party dependencies and continuously improve BC and DR capabilities by identifying critical suppliers, ensuring their BC and DR plans meet defined RTO and RPO standards, and conducting annual risk reassessments to address evolving threats. Lessons learned from testing and incidents shall be documented and their summaries must be shared with Cargolux upon request.

4. REQUEST FOR INFORMATION

4.1 Cargolux reserves the right to request information on information security matters and consult with the Competent Personnel within the scope of the IT Services reasonably necessary to ascertain compliance with the Applicable Rules. Such requests, which shall be included in the provision of the IT Services, may be conducted by Cargolux or an agreed independent third party bound by a confidentiality agreement and shall be scheduled with a minimum prior notice period of thirty (30) Days.

4.2 The Service Provider agrees to provide access to all relevant areas, documentation, logs, and personnel necessary to facilitate the information assessment. The scope and objectives should be limited to processes, resources and data used for the provision of IT Services. The Service Provider shall cooperate fully and provide all necessary assistance to Cargolux during the process. Any findings identified during the information assessment shall be promptly addressed through a remediation plan.

4.3 Cargolux reserves the right to make the information referred to in this Clause available to the Competent Authority upon its request.

4.4 In the event of an on-site information assessment request from the Competent Authority, the Service Provider commits to (i) duly cooperate with the Competent Authority and attend any meeting requested and (ii) give all relevant access to the Competent Authority within the timeframe as requested by the Competent Authority, such as access to information and data related to the concerned IT Services.

5. INCIDENT NOTIFICATION

5.1 In the event the Service Provider becomes aware of any Information Security Event in relation to the performance of the IT services affecting Cargolux or its Affiliates, the Service Provider must notify Cargolux without any undue delay and in any **case no later than 24 hours** after its discovery at the following email address: cybersec@cargolux.com.

5.2 Such notification shall be made in writing and include relevant details of the Information Security Event (including but not limited to the starting date, nature, location, types of data involved), the potential impact on the contracted IT Service or data, and any remediation actions taken or planned. The Parties agree to cooperate in a timely manner to manage the Information Security Event, mitigate damages, and provide any necessary support to restore the affected systems or data. Additionally, both Parties shall maintain open and transparent communication throughout the process of response, keeping each other informed of significant developments, progress, and resolution status.

5.3 Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay until the Information Security Event is considered as closed by Cargolux. Once the Information Security Event is closed, the Service Provider shall send a report regarding the management of the incident.

5.4	The Service Provider is prohibited from disclosing any information related to the Information Security Event in an unauthorized way and/or access to information and data outside of the scope of this Agreement and the IT Services. Cargolux remains the Party responsible for reporting the Information Security Event to the Competent Authority, where required.

6. TERMINATION

6.1	In the event that the Service Provider breaches any of its contractual obligations under the Main Agreement or this Agreement and fails to remedy such breach within 15 Days from the date of receipt of the official notification requiring the correction of such breach, Cargolux shall be entitled to terminate the Main Agreement with immediate effect, without prejudice to any other rights or remedies available under the Main Agreement or any applicable laws.
6.2	Within 90 Days after the Main Agreement's termination, the Service Provider shall, at Cargolux's discretion, provide any existing copies of the data and delete the processed data certifying it has done so, or, return all data and delete existing copies and provide a declaration regarding compliance with this clause and, whether applicable, the list of data retained by the Service Provider in compliance with applicable regulations. Until the data is deleted or returned, the Service Provider shall continue to ensure compliance with this Agreement.

LEVEL 2

1. CYBERSECURITY

The Service Provider shall implement security measures to keep its IT systems and data secure, reliable, and operational. These measures shall comply with applicable information security regulations and align with industry standards. If the Service Provider detects any risk, vulnerability, or incident that could affect the IT Service or Cargolux's information security (hence "IS Event"), it shall notify Cargolux at: cybersec@cargolux.com.

An IS Event shall be considered significant (the "Significant Information Security Event") if:

(a) It has disrupted or capable of disrupting the continuity of Cargolux's flight operations, continuing airworthiness, or aviation safety;

(b) It has caused or is capable of causing severe operational disruption of the services or financial loss of the entity concerned; or

(c) It has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

The notification shall be sent:

a. **no later than 72 hours** - from the date when the Service Provider becomes aware of it - in case of an IS Event other than the Significant Information Security Event.

b. **no later than 24 hours** - from the date when the Service Provider becomes aware of it - in case of the Significant Information Security Event. In this case, the Service Provider shall indicate in the first notification its existing business continuity plan and backup procedures.

If the first notification does not contain all information concerning the management of an IS Event, the Service Provider shall provide further details until the IS Event is considered as closed by Cargolux.

The Service Provider shall provide timely notice of any changes regarding (i) its networks (including enhancement); (ii) the use of new technologies; (iii) the adoption of new products or newer versions or releases; (iv) the development of new tools and environments; (v) any change to physical location of service facilities; (vi) any change of sub-suppliers; (vii) any sub-contracting to another supplier; or (viii) any change to its policies and procedures that affect the information security of either Party or the delivery of the IT Services. Following such notice, the Parties shall review and will equitably adjust the terms of their commitment as necessary to appropriately address risk.

2. COOPERATION

Cargolux reserves the right to make any information available to the competent supervisory authority upon its request. Upon request, the Service Provider further agrees:

(i) to provide within 7 Days the documentation concerning the execution of the obligations under these clauses;

(ii) to grant access to its premises for on-site information assessment; and

(iii) to promptly address any identified non-compliance findings and to show proof of their remediation resolutions.

3. TERMINATION

In the event that the Service Provider breaches any of its contractual obligations under the Main Agreement or this Agreement and fails to remedy such breach within 30 Days from the date of receipt of the official notification requiring the correction of such breach, Cargolux shall be entitled to terminate the Main Agreement with immediate effect, without prejudice to any other rights or remedies available under the Main Agreement or any applicable laws.

Within 90 Days after the Main Agreement's termination, the Service Provider shall, at Cargolux's discretion, provide any existing copies of the data and delete the processed data certifying it has done so, or, return all data and delete existing copies and provide a declaration regarding compliance with this clause and, whether applicable, the list of data retained by the Service Provider in compliance with applicable regulations. Until the data is deleted or returned, the Service Provider shall continue to ensure compliance with this Agreement.

4. PERSONNEL REQUIREMENTS *(in case of consultancy IT Services)*

The Service Provider ensures that the personnel assigned to any consultancy IT Services (the "Consultant") must:

a) successfully complete Cargolux's Information Security and Data related training at the beginning of the concerned IT Services;
b) exclusively carry out the mission within the assets to which they have been granted access to and shall report any access that is not necessary for the completion of the mission;
c) refrain from any attempt, on its own or through unauthorized third parties, to retrieve or interfere with any information or data without the prior authorization of Cargolux; and
d) successfully perform an enhanced background check as required per the regulation when being granted with unsupervised administrative rights.

The Service Provider undertakes to ensure compliance by its Consultant's undertakings hereunder.

LEVEL 3: Non-Critical
The Service Provider shall implement security measures to keep its IT systems and data secure, reliable, and operational. These measures shall comply with applicable information security regulations and align with industry standards. If the Service Provider detects any risk, vulnerability, or incident that could affect the IT Services or Cargolux's information security ("IS Events"), it shall notify Cargolux **no later than 72 hours** from the date in which becomes aware of it - at: cybersec@cargolux.com. Upon request, after the first notification, the Service Provider shall provide follow-ups until the management of the IS Event.