SECURITY STANDARDS

PART I: Introductory Provisions and Definitions

1. Purpose and Scope

This Annex (hereinafter the "Annex") sets out binding security measures (hereinafter the "Security Measures") that the Supplier shall comply with in the performance of the Contract, to which this Annex forms an integral part.

The Security Measures are defined in view of the fact that the Customer is subject to extensive regulatory obligations. As a provider of regulated services, the Customer is subject to Act No. 264/2025 Sb., on Cybersecurity (hereinafter the "Cybersecurity Act"), and, as an organization operating in the civil aviation sector, also complies with the requirements of European regulations having direct effect on aviation security.

The objective of the Security Measures is to ensure the protection of the confidentiality, integrity, availability, authenticity, and resilience of the Customer's information and its information, communication, and industrial systems and services.

The Customer is required to implement and maintain, throughout the duration of the contractual relationship, appropriate technical and organizational cybersecurity measures commensurate with the nature, scope, and risk level of the services provided.

The Customer is obligated to fulfill these obligations in accordance with the requirements of Act No. 264/2025 Coll., on Cybersecurity, and related implementing regulations; or, in the case of a Supplier established outside the Czech Republic, in accordance with the regulations implementing Directive (EU) 2022/2555 (NIS2) in its home country, to the extent corresponding to the nature of the services provided.

The Customer may demonstrate compliance with this obligation, in particular, through valid certification of an information security management system, an independent security audit, a conformity assessment, or other equivalent evidence.

2. Legislative Framework

The Security Measures and requirements set out in this Annex are based on the legal framework of the Czech Republic and the European Union. The Customer is subject to statutory and regulatory duties under this framework. On the basis of these regulations, the Customer defines its security requirements, which are reflected in this Annex.

The Supplier shall comply with all Security Measures and duties set out in this Annex, thereby enabling the Customer to fulfil its regulatory obligations.

The legal regulations listed below constitute the key legal bases from which the Customer's requirements are derived:

a) Act No. 264/2025 Sb., on Cybersecurity (the Cybersecurity Act), in particular Section 13(5), which imposes the duty to incorporate requirements arising from security measures into contracts concluded with suppliers.

b) Implementing legal regulations to the Cybersecurity Act, in particular Decree No. 409/2025 Sb., on security measures for providers of regulated services under a regime of higher obligations (hereinafter the "Decree").

c) Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down requirements

for information security risk management with a potential impact on aviation security.

d) Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security.

e) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the "GDPR"), and Act No. 110/2019 Sb., on the processing of personal data, as amended, where the Supplier processes personal data for the Customer in the performance of the Contract.

f) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

g) Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

h) Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

Where more than one legal regulation applicable to the Customer applies to a particular area, the requirements set out in this Annex are defined to ensure the highest level of security and protection. This ensures that regulatory complexity does not result in a reduction of the security level but, on the contrary, leads to its strengthening, which is of fundamental importance for the Customer as a regulated entity.

3. Scope of Validity and Applicability

The Security Measures shall apply whenever the subject matter of performance for the Customer (whether provided exclusively or as part of other performance) includes any of the following activities:

a) Development, implementation, delivery, provision, support, or maintenance of software or hardware (hereinafter "Software" or "Hardware").

b) The Supplier's access to the Customer's information, communication, or industrial systems, in particular those designated as part of a regulated service within the meaning of the Cybersecurity Act.

c) Processing, transmission, storage, or archiving of the Customer's data and operational data of the Customer or its customers (hereinafter the "Customer Data").

The Supplier shall assess whether the individual Security Measures and duties set out in this Annex apply directly to the Supplier or to the manufacturer or provider of the performance supplied by the Supplier. Based on the outcome of such assessment, the Supplier shall ensure their proper performance by the relevant party, while remaining fully liable towards the Customer for compliance with all requirements.

3.1 Performance – Specific Provisions

The Supplier acknowledges that the subject matter of performance under the Contract, or any of its partial components, supports or interoperates with systems within the defined scope of the cybersecurity management framework of the Ostrava Airport.

4. Definitions

For the purposes of this Annex, the following terms shall have the meaning set out below:

- Confidential Information: Any and all information, personal data, data, or communications that the Supplier becomes aware of in connection with the preparation or performance of the Contract, including, without limitation, the subject matter of the Contract, facts constituting trade secrets, and the internal affairs of the Customer.
- Cybersecurity Incident: A breach of information security in cyberspace originating in cyberspace that has a significant impact on the provision of a regulated service. For the purposes of this Annex, a Cybersecurity Incident shall include any event that compromises or threatens the confidentiality, integrity, or availability of the Customer Data or of the systems in which such data are processed.
- Cybersecurity Event: An event in cyberspace that may lead to the occurrence of a Cybersecurity Incident.
- Subcontractor: Any third party engaged by the Supplier in the performance of the Contract.
- Vulnerability: A weakness of an asset that may be exploited by one or more threats.
- Information Classification: The Customer's system for classifying information (e.g. Public, Internal, Sensitive, Strategic), which defines the required level of protection. Unless the Customer provides otherwise, the Supplier shall handle all Customer Data and Confidential Information at least as "Internal".

PART II: Rights and Obligations

5. General Obligations

5.1 Compliance with Applicable Laws and the Customer´s Policies

a) The Supplier shall comply with the relevant provisions of the Customer's internal security policies, methodologies, and procedures applicable to the subject matter of performance, provided

that the Supplier has been duly informed of them.

b) The Customer undertakes to provide the Supplier with access to the relevant documentation to the extent necessary.

c) The subject matter of performance shall not infringe any copyright or licensing rights of any third party.

d) The Customer may, with due justification, reject the subject matter of performance or any part thereof when it is subject to warnings issued by the National Cyber and Information Security Authority.

5.2 Contact Person and Responsibility

a) No later than 15 days after the conclusion of the Contract, the Supplier shall designate a responsible contact person for the area of cybersecurity and for the performance of obligations arising from this Annex.

b) The Supplier shall notify the Customer of the contact details of such person in writing within the same time limit.

c) Any change of the contact person shall be notified by the Supplier to the Customer within 5 business days.

d) No later than 30 days after the conclusion of the Contract, the Supplier shall ensure that the designated contact person confirms to the Customer in writing that all persons involved in the performance of the Contract (including employees of Subcontractors) have been duly informed of the documentation provided by the Customer and of the content of this Annex, and have undertaken to comply with the requirements set out therein.

6. Notification Obligation

The Supplier shall notify the Customer in writing without undue delay of the following circumstances:

a) Any material change in the control of the Supplier within the meaning of Act No. 90/2012 Sb., on Business Corporations.

b) Any change in the ownership of key assets used for the performance of the subject matter of the Contract.

c) Any request by a foreign authority for access to or transfer of data processed in the territory of a foreign state, except where such notification would be contrary to the applicable legislation under which the data are processed or under which the request was made.

7. Personnel Security and Access Management

7.1 Personnel Requirements and Awareness of the Measures

a) The Supplier shall ensure that all its personnel (including employees and external contractors) and the personnel of its Subcontractors who come into contact with the Customer Data or have access to the Customer’s systems are bound by confidentiality obligations at least equivalent in scope to those set out in the Contract and this Annex.

b) In accordance with the Customer’s requirements and instructions, the Supplier shall ensure that its employees and third-party personnel receive appropriate instruction and training.

7.2 Identity Verification

a) The Customer is entitled to verify the identity of all personnel of the Supplier and approved Subcontractors who access the Customer’s systems and the data or services processed therein.

Any exceptions to this requirement may be granted by the Customer on a case-by-case basis.

b) The Supplier shall provide the contact details of the personnel granted access without prior request.

7.3 Identity Management and Access Control

a) The Supplier shall apply the principles of least privilege and need-to-know.

b) The Supplier shall grant access rights to the Customer's systems and data on the basis of a documented business need, shall review such access rights on a regular basis (at least once per year), and shall remove them without undue delay upon termination of employment, change of job position, or end of the need for access.

c) The Supplier shall strictly separate user accounts from administrative (privileged) accounts.

d) Where an application or system forming part of the subject matter of performance uses technical, application, or database accounts authenticated by means of a password, the Supplier shall ensure that, for such accounts, an immediate and free-of-charge password change by an administrator on the Customer's side is provided.

7.4 Authentication Security

a) The Supplier shall never store authentication credentials, in particular passwords, in a readable or plain-text form. The Supplier shall protect such credentials using sufficiently strong and up-to-date cryptographic measures in accordance with the applicable recommendations of the National Cyber and Information Security Authority. Such recommendations may be provided to the Supplier upon request.

b) For all remote access to the Customer's network infrastructure and for all access to the interfaces of systems managing the Customer Data, the Supplier shall enforce the use of multi-factor authentication.

8. Security Throughout the Lifecycle of Systems and Services

8.1 Secure Design and Development

a) The Supplier represents and warrants that all software or hardware that he supplies, has been developed in accordance with secure development principles.

b) The subject matter of performance shall not contain any unnecessary components, services, libraries, or user accounts that are not objectively required for its proper operation (principle of minimisation).

c) The Supplier undertakes not to intentionally integrate into the subject matter of performance any vulnerabilities, backdoors, Trojan horses, keyloggers, sniffers, or any other form of malicious code, and shall not take any action that would enable such integration.

d) Upon the Customer's request, the Supplier shall provide accurate information on the origin and composition of the supplied components (Bill of Materials – BoM).

8.2 Vulnerability and Security Update Management

a) The Supplier shall continuously monitor for and identify technical vulnerabilities and configuration non-compliances in the subject matter of performance and its third-party components. The Supplier shall notify the Customer without undue delay of all identified findings, in particular newly discovered vulnerabilities.

b) The Supplier shall continuously inform the Customer of the release of security updates (patches) for the subject matter of performance or any part thereof.

c) Where the performance includes the installation of an operating system or third-party software, the Supplier shall install only the latest stable version fully supported by the manufacturer.

d) The Supplier shall be responsible for ensuring that, at the time of handover, the systems provided include the latest, stable, and properly tested security updates.

8.3 Security Testing and Assessment

a) The Customer reserves the right, at any time during the term of the Contract, including prior to its conclusion, to carry out or to have carried out by a third party penetration testing or vulnerability testing of the solution supplied.

b) The Supplier undertakes to provide the Customer with all necessary cooperation required for the performance of such testing.

c) When the results of the testing reveal critical or high-severity findings, the Supplier shall, without undue delay and at its own expense, adopt effective remedial measures to eliminate the identified vulnerabilities.

d) The remediation plan shall be subject to the Customer's approval.

e) The results of the testing shall be disclosed exclusively to authorised persons of the Supplier and the Customer.

8.4 Secure Configuration

a) The Supplier shall be responsible for the secure configuration of all systems that he supplies, in accordance with recognised standards (e.g. CIS Benchmarks) and the Customer's specific requirements, where such requirements have been defined.

b) The Supplier shall provide the Customer with documentation describing the configuration measures and settings implemented.

8.5 Change Management

a) The Supplier shall notify the Customer of any planned changes to the solution supplied sufficiently in advance. The Customer shall assess the significance and impact of such changes and, where appropriate, carry out a related risk analysis and propose measures to mitigate any adverse effects. The significance of a change shall be assessed by the Customer.

b) The Supplier shall provide the Customer with all necessary cooperation in the risk analysis, the update of security documentation, and the related testing.

c) For each significant change, the Supplier shall ensure the possibility to revert to the original state (rollback).

9. Data and Information Protection

9.1 Use of the Customer Data

a) The Supplier shall use the Customer Data exclusively for the purpose of the due performance of the subject matter of the Contract and only to the extent strictly necessary.

b) Any other use, copying, modification, or disclosure to third parties shall be strictly prohibited without the Customer's prior written consent.

c) The Supplier undertakes to use the Customer Data in accordance with the Contract and the applicable legislation.

9.2 Cryptographic Protection

a) The Supplier shall store and transfer all Confidential Information (e.g. certificate identifiers, passwords, access rights, configuration files) provided by the Customer or generated during the performance exclusively in encrypted form and shall protect such information against unauthorised access.

b) The cryptographic algorithms used and key lengths shall comply with the applicable recommendations of the National Cyber and Information Security Authority. Such recommendations may be provided to the Supplier upon request.

9.3 Network Communication Security

a) The Supplier shall secure all transfer of the Customer Data via public and private networks using strong and currently resilient cryptographic protocols.

b) The Supplier shall protect online transactions carried out through web technologies by means of valid SSL/TLS certificates issued by a trusted certification authority.

c) The Supplier shall protect all Supplier's information systems connecting to the Customer's network infrastructure by means of up-to-date and properly configured solutions for the detection and removal of malicious code.

9.4 Data and Media Disposal

a) Where, in the performance of the Contract, the Supplier is required to erase the Customer Data or to dispose of technical storage media, the Supplier shall always proceed in accordance with recognised standards for secure data disposal.

b) Where the information classification has not been determined, the disposal method applicable to the highest level of asset criticality shall be applied.

c) The disposal methods allowed shall include secure overwriting, degaussing, or physical destruction of the storage media.

d) The Supplier shall prepare a record of the disposal carried out and shall provide it to the Customer.

10. Monitoring and Handling of Cybersecurity Incidents

10.1 Activity Logging

a) Where the subject matter of performance takes the form of a software-based or combined solution, it shall provide audit logs of activities performed therein, to an extent that enables the clear and reliable identification of the user, the time, and the action performed.

b) The Supplier undertakes to enable the Customer to access the audit logs in a form that allows their centralised processing by a Security Information and Event Management (SIEM) tool.

10.2 Detection and Reporting of Cybersecurity Events and Incidents

a) The Supplier shall notify the Customer without undue delay, and no later than three (3) hours after becoming aware, of any cybersecurity events or incidents related to the performance of the subject matter of the Contract.

b) The Supplier shall make such notification by telephone to the Customer's contact line, namely the Security Operations Desk (+420 602 238 151), and at the same time in writing to the following email address: bd@airport-ostrava.cz.

c) The notification shall include a description of the nature of the event or incident, the affected assets, the anticipated impact, and information on the measures already taken by the Supplier in relation to the relevant event or incident.

10.3 Cooperation in Incident Handling

a) In assessing the causes and impacts of a cybersecurity incident related to the subject matter of the Contract, the Supplier shall provide the Customer with full and immediate cooperation.

b) Such cooperation shall include, in particular, the provision of logs, identification data (e.g. IP address, MAC address), the provision of memory or disk images for forensic analysis, and the implementation of remedial and mitigation measures required by the Customer.

c) Where the Supplier has caused or contributed to the occurrence of a cybersecurity incident, the Supplier shall, at its own expense, perform a Root Cause Analysis and submit to the Customer for approval a set of technical and organisational measures aimed at preventing the recurrence of the incident.

d) In the event of a serious cyber incident, the Customer may contact NÚKIB if the Supplier refuses or fails to respond to the Customer's requests for data. The Supplier must provide the data immediately (the Supplier is also entitled to reimbursement of costs incurred after providing the data—so-called reasonable costs).

11. Business Continuity Management

a) The Customer may involve the Supplier in its business continuity management system. This shall include, in particular, the right to include the Supplier and the services provided by the Supplier in the Customer's business continuity plans and emergency plans.

b) The Supplier undertakes to provide the necessary cooperation during scheduled outages, in the event of an extraordinary incident, or during the testing of the Customer's business continuity and recovery plans.

12. System and Operational Documentation

a) No later than upon handover and acceptance of the performance, the Supplier shall deliver complete system and operational security documentation. Failure to deliver such documentation shall be deemed a material defect preventing acceptance of the performance.

b) The system documentation shall include a description of the functions and activities necessary for the administration and use of the delivered solution, including user and administrator manuals.

c) The operational security documentation shall include a description of the necessary security functions (e.g. update procedures, logging capabilities, backup and recovery procedures, installation and configuration procedures).

13. Supply Chain Management

13.1 Approval and Management of Subcontractors

a) The Supplier shall not engage any additional Subcontractor in the performance of the Contract without the Customer's prior, specific, and written consent or instruction.

b) Prior to granting such consent, the Customer may request from the Supplier any information necessary to carry out its own risk assessment in relation to the proposed Subcontractor.

c) The Customer undertakes that Subcontractors who do not provide key parts of the performance shall not be granted access to the Customer Data.

13.2 Flow-Down and Enforcement of Security Obligations

a) The Supplier shall contractually bind each of its Subcontractors to comply with all obligations set out in this Annex, either in full or to a reduced extent corresponding to the Subcontractor's involvement. Upon the Customer's written request, the Supplier shall submit, for the purpose of demonstrating compliance with this obligation, an appropriately anonymised agreement concluded with the relevant Subcontractor.

b) The Supplier shall be fully and exclusively liable for any acts or omissions of its Subcontractors as if they were his own acts or omissions.

c) Any breach of this Annex by a Subcontractor shall be deemed a direct breach of the Contract by the Supplier.

PART III: Audit, sanctions and termination

14. Audit

14.1 Customer´s Right to Audit

a) The Customer is entitled to carry out audits for the purpose of verifying that the Supplier complies with the obligations arising from this Annex. The number and frequency of such audits shall not be limited.

b) The Customer shall notify the Supplier of its intention to carry out an audit in writing at least fourteen (14) days in advance, unless a serious cybersecurity incident or a suspicion thereof justifies the immediate conduct of an audit.

14.2 Duty to Cooperate and Remedy Findings

a) The Supplier shall provide the Customer with all necessary cooperation during the audit, in particular by making all relevant documentation available, granting access to premises and information systems, and ensuring the presence of its responsible representatives.

b) The Customer shall inform the Supplier of the results of the audit by means of an audit report and shall grant the Supplier a reasonable period to submit its comments.

c) The Supplier shall, without undue delay, adopt remedial measures to eliminate all identified deficiencies within the time limit agreed with the Customer.

d) Failure to comply with this obligation shall be deemed a material breach of the Contract.

15. Obligations upon Termination of the Contract

15.1 Exit Plan

a) The Supplier undertakes, in cooperation with the Customer, to prepare and, throughout the term of the Contract, regularly update an Exit Plan (the "Plan").

b) The Plan shall describe in detail the procedures, responsibilities, and timeline for the orderly transition of all activities related to the performance of the Contract to the Customer or to a new

supplier.

c) The Plan shall in particular include procedures for data migration, handover of documentation, knowledge transfer, and the secure disposal of all Customer Data from the Supplier's systems.

15.2 Cooperation during Transition

The Supplier shall provide all necessary cooperation for the implementation of an orderly termination of the cooperation and transition of activities, including after the expiry or termination of the Contract, for the period strictly necessary to ensure the continuity of services.

15.3 Right to Extraordinary Termination

The Customer may terminate the Contract unilaterally and with immediate effect, without any notice period, in the event of a material change of control over the Supplier or its key assets, where such change, based on the Customer's duly reasoned assessment, constitutes an unacceptable security risk.

16. Final Provisions

16.1 Validity and Enforceability

a) If any provision of this Annex becomes invalid or unenforceable, such invalidity or unenforceability shall not affect the validity or enforceability of the remaining provisions.

b) The Contracting Parties undertake to replace any invalid or unenforceable provision with a new provision whose meaning and purpose shall be as close as possible to the original intent.

c) The Supplier shall not be entitled to any additional remuneration for the performance of obligations under this Annex beyond the price agreed in the Contract, as the costs of ensuring security form an integral part of the due performance of the Contract.

16.2 Amendments

The Contracting Parties may amend or supplement this Annex only by written, consecutively numbered amendments signed by duly authorised representatives of both Contracting Parties.