CONTRACT FOR WORK

Letiště Praha, a. s. (in English Prague Airport)

as the Customer

and

Simpleway Europe a. s.

as the Contractor

Customer's contract number	Contractor's contract number
0122002838	SWPRG100

Parties:

Letiště Praha, a. s. (in English Prague Airport),

with registered office: K letišti 1019/6, Praha 6, postal code 161 00
incorporated in the Companies Register kept by the Municipal Court in Prague, Section B, Insert 14003
Business Identification Number: 282 44 532
VAT ID: CZ699003361
represented by: Mr. Jiří Kraus, Vice-Chairman of the Board of Directors and Mr. Jiří Černík, Member of the Board of Directors

(hereinafter only as "**Customer**" or **"LP"**)

and

Simpleway Europe a. s.

with registered office: Na okraji 335/42, Praha 6, postal code 162 00,
incorporated in the Company Register kept by Municipal Court in Prague, Section B, Insert 20925,
Business Identification Number: 04377028,
VAT ID: CZ04377028,
Bank details: Fio banka, a.s,
Account number (CZK): 2000938639 / 2010,
represented by: Mr. Jakub Maléř, member of Board of Directors and by Mr. Petr Otoupal, member of Board of Directors ,
(hereinafter only "**Contractor**")

(The Customer and the Contractor shall be hereinafter jointly referred to also as "**Parties**" or individually as "**Party**")

have concluded

in accordance with the provisions of Section 2586 et seq. of the Act No. 89/2012 Coll., the Civil Code, as amended, and in accordance with the Act No. 121/2000 Coll., on the Copyright, on the Rights Related to Copyright and on the Amendment to Certain Acts (Copyright Act), as amended, the following Contract for Work (hereinafter only as "Contract").

1. DEFINITIONS AND INTERPRETATIONS

1.1 The terms referred to herein shall have the meaning defined in this clause 1.1 and in the text of this Contract the first letter of such term shall be capitalized:

1.1.1 **"Administrator"** is an administrator of the System on the Customer's part who is responsible for administration and configuration of the System in the Customer's environment.

1.1.2 "**AODB**" means Airport Operation Data Base.

1.1.3 "**Backup Platform"** means platform which has same functionalities as Production Platform. In case of failover of the Sytem, operation of System shall be switched manualy by Customer on to Backup Platform within 20 minutes.

1.1.4 **"Copyright Act"** means the Act No. 121/2000 Coll., on the Copyright, on the Rights Related to Copyright and on the Amendment to Certain Acts (Copyright Act), as amended, or any legal regulation that will supersede it, whether in full or in part.

1.1.5 **"Production AODB"** means AODB for the exchange and processing of up-to-date operationl AODB data.

1.1.6 "**Current Hardware**" means graphic controllers mentioned in Annex 5 hereto

1.1.7 "**Hardware"** means graphic controllers delivered within Work, described in Annex 6 hereto.

1.1.8 **"Price of the Work"** has a meaning as set forth in art. 8.1 hereof.

1.1.9 **"Customization"** means a process of customizing the System to the Customer's specific needs, by setting customer parameters or other moderations of the System in accordance with the Annex No. 1 hereto.

1.1.10 **"Work"** means

1.1.10.1 Completion and/or delivery of the System;

1.1.10.2 completing Customization, Installation and Integration of the System, in accordance with the technical and functional specification which form the Annex No. 1 hereto;

1.1.10.3 Creation of Production, Test and Backup Platform.

1.1.10.4 Delivery and Installation of Hardware

1.1.10.5 Reinstallation and prophylaxis of Current Hardware (if it is proposed)

1.1.10.6 Documents preparation;

1.1.10.1 Provide Customer with cooperation for Penetration test

1.1.10.2 organisation of trainings for Users and Administrators.

1.1.10.3 Post-implementation adjustments (25 ManDays)

1.1.11 **"Documents"** mean (i) user manual, (ii) administrator's manual and (iii) other documents describing in detail functionality, operating parameters, technical parameters and user or administrator parameters of the System in Czech or English language and in electronic form as docx, or pdf.

1.1.12 **"Confidential Information"** is information which is obtained by the Party by entering into this Contract or in connection with performance hereof, it is related to the other Party or its representatives, Controlled entities, CAH (Czech aeroholding) entities and their relations, relationships and business or other activities, including information contained in the System, namely information of a commercial character and information related to the operation of Václav Havel Airport Prague.

1.1.13 **"Invoice"** means a tax document issued by the Contractor for the purpose of payment of the Price of the Work the essential elements of which are set forth in the Act No. 235/2004 Coll., on Value Added Tax, as amended.

1.1.14 **"Implementation"** means a process of Installation, Customization and System Integration in accordance with the Annexes No. 1 and No. 4 hereto.

1.1.15 **"Installation"**

1.1.15.1 with respect to Hardware or Current Hardware, the performance of any and all activities required to put the hardware into operation, including without limitation, remove of old hardware its plugging in into the electrical network at points designated by the Customer, and interconnection of hardware elements with other hardware elements within the System,

1.1.15.2 with respect to System means performance of all activities necessary for putting the System into operation**,** including without limitation, the implementation of the System **and** the components thereof in the Customer's environment.

1.1.16 **"Integration"** means physical and functional interconnection of the System with other elements and/or software and/or hardware equipment of the Customer.

1.1.17 **"Insolvency Act"** means the Act No. 182/2006 Coll., on Insolvency and Its Resolution (Insolvency Act), as amended, or any other legal act which results in insolvency or bankruptcy of any party to this Contract.

1.1.18 **"Response Time"** means a time period set obligatorily in this Contract during which the Contractor is obliged to inform using a telephone line [redacted] (or another number notified for this purpose by the Customer to the Contractor) and using an electronic mail at the address [redacted] (or another email notified for this purpose by the Customer to the Contractor) the Customer of the manner in which the reported Defect will be removed and by which Contractor's employees. The Response Time starts from the moment the Defect is reported by the Customer to the Contractor's contacts set forth in the Annex No. 3 hereto.

1.1.19 **"Time for Defect Removal"** means a time period mentioned in table in art. 7.4 hereof set forth obligatorily in this Contract during which the Contractor is obliged to remove the reported Defect. The Time for Defect Removal starts from the moment the Defect is reported by the Customer to the Contractor's contacts set forth in the Annex No. 3 hereto.

1.1.20 **"Test Plaform"** means plaform for System which must be run in parallel with Production Platform. Test Platform has the same functionalities as Production Platform and contains its interface for AODB data transfer.

1.1.21 **"Licence"** means a right to use the Work pursuant to the provisions of Section 2358 et seq. of the Civil Code, as amended, in the scope specified in article 6. hereof.

1.1.22 **"Delivery Place"** means the places pursuant to art. 3.2 hereof where the Contractor is obliged to supply the Work for the Pilot Operation.

1.1.23 **"Civil Code"** means the Act No. 89/2012 Coll., the Civil Code, as amended or any legal regulation that will supersede it, whether in full or in part.

1.1.24 **"Personal Data"** means personal data of natural persons, namely employees of the Customer and CAH entities, the protection and processing of which is subject to the Personal Data Protection Act;

1.1.25 **"Production Platform"** means platform for System optimized for 24/7 operation, fulfilling all requirements specified in Annex No. 1 – Technical and Functional Specification of the System.

1.1.26 **"CAH entities"** mean commercial corporations which form a group with the Customer pursuant to the provisions of Section 79 et seq. of the Act No. 90/2012 Coll., on Commercial Corporations and Cooperatives, as amended (**"Act on Commercial Corporations"**).

1.1.27 **"Controlled Entity"** means a legal person controlled by the Customer of by its affiliates pursuant to the Act on Commercial Corporations.

1.1.28 **„Penetration test"** means a special method of verification whether the System interface accessible from the Internet is provided with sufficient protection against an attack looking for private or non-public data, or taking control of the System and its features. Penetration tests will be carried out using the OWASP method (The Open WebAplication Security Project – a set of recognized security methods which are necessary for the erection of a safe web application [redacted]).

1.1.29 **"Report"** means a report made by the Customer by a telephone to the Contractor's Support Centre regarding the existence of a Defect. Each telephone report must be confirmed by the Customer also by sending an email message to the Contractor to the email prg-support@simpleway.cz, by the end of the following Business Day.

1.1.30 **"Ongoing Information Period"** means a frequency of ongoing information about removal of Defects which must be delivered by the Contractor to the Customer.

1.1.31 **"Support Centre"** means the Contractor's Service Support Centre at telephone line: [redacted], e-mail: [redacted]

1.1.32 "**Business Day**" means any calendar day, with the exception of Saturday, Sunday, day of rest or holiday pursuant to the applicable legal regulations of the Czech Republic.

1.1.33 **"Intellectual Property Rights"** mean all patents, copyrights, rights to utility designs, trademarks, trade names and commercial names, protected designation of origin, rights related to copyrights, special rights of database makers, trade secret, know-how and any other intellectual property rights of any character (whether or not registered), including any registration applications and exclusive rights to register for protection anything from the aforesaid rights at any place in the world.

1.1.34 "**Handover**" means the day when the Parties sign the Handover Protocol.

1.1.35 **"Handover Protocol"** means a protocol of handover and takeover of the Work signed by both Parties.

1.1.36 **"Service Period"** means 24 hours, 7 days a week.

1.1.37 **"Service Request"** means a record on reported error status and/or request for a change requested by the User.

1.1.38 **"Services"** means all activities to be provided by the Contractor in the course of performance of the Contract that are necessary for fulfilment of the contractual obligations.

1.1.39 **"Service Level Agreement"** means agreement for the Contractor's obligation to provide Customer with support services related to the Work to ensure the functionality, availability, response and provision of the support for Work and the Customers obligation to pay to the Contractor for a monthy fee for these services.

1.1.40 **"System"** means the flight information display system. Technical and functional requirements of the system are specified in the Annex No. 1 hereto.

1.1.41 **"Customer's System"** means the applications or systems that contain Customer's data.

1.1.42 **"Model Technical Description"** means technical and functional specification of the System as described in the Annex No. 1 hereto,

1.1.43 **"Verification Operation"** means a period of maximum 2 months after Installation of System on Production platform during which the properties of the System with Hardware are verified and functionality of the System is tested in non – public area with data from Production AODB data.

1.1.44 **"Pilot Operation"** means a period of maximum 6 months after succesfull completion of Verification Opeartion during which will be all Hardware Installed and during which the properties of the System are verified and functionality of the System is tested with datas from Production AODB data.

1.1.45 **"User"** is any person who uses and/or is authorised to use services provided by the Customer.

1.1.46 **"Defect"** means (i) defects in title of the Work or Hardware/Current Hardware or (ii) conflict between actual properties of the Work or Hardware/Current Hardware and the properties that are set in this Contract or in the Documents or (iii) any functional deviation of the Work or Hardware/Current Hardware from standard functionalities described herein, namely in the Annex No. 1 Technical and Functional Specification of the System, or Documents that adversely affects its activities or functioning.

1.1.47 **"Category A Defect"** means the most severe Defect, such as when:

1.1.47.1 the supplied Work or Hardware/Current Hardware has defects in title, or

1.1.47.2 the supplied Work or Hardware/Current Hardware or any part thereof lacks the properties explicitly described in this Contract or in the Documents, or

1.1.47.3 the supplied Work or Hardware/Current Hardware or any part thereof is completely dysfunctional or the Customer cannot use the Work or a substantial part thereof.

1.1.48 **"Category B Defect"** means a Defect which can be described as a Defect which limits the use or functionality of the Work or Hardware/Current Hardware or any part thereof, thus substantially affecting processes and increasing labour requirements at the Customer and/or in consequence of which the data and/or work of the User is lost.

1.1.49 **"Category C Defect"** means a Defect which is not categorized by the Customer as a Category A Defect or a Category B Defect and which

1.1.49.1 does not prevent or has an absolutely minimum influence on proper use or functionality of the Work or Hardware/Current Hardware or any part thereof by the Customer, and

1.1.49.2 has a minimum influence on disruption of processes and increase in labour requirements at the Customer.

1.1.50 "**Act on Personal Data Protection**" means the Act No. 101/2000 Coll., on Personal Data Protection, as amended.

1.2 Other terms may be defined directly in the text of the Contract which definition shall be in bold letters with the phrase "hereinafter only as" before it and further in the text hereof shall be capitalized.

1.3 Terms in singular number includes the plural number and vice versa; any word which denotes the masculine gender shall include the feminine and/or the neuter genders and vice versa; any reference to a person includes natural and legal person and vice versa.

2. SUBJECT

2.1 Subject to the conditions stipulated hereunder

2.1.1 The Contractor undertakes to create for the Customer the Work and deliver it to the Customer in accordance with this Contract and the annexes hereto which are integrally incorporated herein and supply to the Customer the works and supplies in accordance herewith,

2.1.2 the Customer undertakes to pay the Contractor for the properly completed Work the agreed Price of the Work and properly accept the Work from the Contractor in accordance with this Contract and the annexes hereto.

3. TIME AND DELIVERY PLACE

3.1 The Contractor will successfully finish the Pilot Operation no later than within 300 calendar days from the day of this Contract becomes effective and in accordance with the detailed time schedule of the Implementation which forms the Annex No. 4 hereto (hereinafter only as **"Time Schedule"**).

3.2 The Delivery Place of the Work will be: the premises at the addresses (i) K Letišti 6/1019, Prague 6 so-called "Bílý dům" (White House) and (ii) Jana Kašpara 1069/1, Prague 6, APC building or other places within the compounds of the International Airport Prague/Ruzyně designated by the Customer. The Contractor has the right to perform the works on the Work even outside the Delivery Place, however, only subject to a previous written consent of the Customer.

4. RIGHTS AND OBLIGATIONS OF CONTRACTING PARTIES

4.1 The Customer has the right to print out, use and supplement the Documents related to the System in an unlimited number of copies for own needs and in own favour, as well as for the needs and in favour of CAH entities and to handover the Documents to CAH entities for use. The Contractor hereby agrees explicitly with the use of such Documents by the Customer and CAH entities. Any further distribution of the Documents to third parties shall be subject to art. 11 hereof.

4.2 The Contractor undertakes to:

4.2.1 complete the Work at own costs and risk in accordance herewith and the annexes hereto, with the instructions of the Customer's authorised employees and remove all Defects rebuked in the course of Handover or during the warranty period pursuant to article 7.4 hereof;

4.2.2 complete the Work (or any part hereof) personally in accordance herewith. The Contractor is not authorised to perform the Work (or any part thereof) via a subcontractor, without obtaining a previous written consent of the Customer. In case the Customer grants a previous written consent to the Contractor to perform the Work (or any part thereof) in accordance with this Contract via a subcontractor, the Contractor will be liable to the Customer for the completion of the Work (or the respective part thereof) in accordance with this Contract in the same scope as if he performs the Work himself. The appointment of the subcontractor will not affect the Contractor's obligation to complete the Work in accordance herewith and this obligation stays with the Contractor during the whole term of this Contract;

4.2.3 comply with all generally binding legal regulations and the Customer's regulations in the field of waste management and remove all waste generated during performance of the Work in accordance with the applicable legislation at own costs;

4.2.4 report immediately by email or by fax to the security division (BZP) of Letiště Praha, a. s. any loss, theft, damage of an ID card (including visitor cards) or other permit issued by the Customer or any CAH entity to the Contractor or the Contractor's employees. Similarly, the Contractor is obliged to return any permits or other cards issued for him or for his employees upon the end of their validity period;

4.2.5 make sure that his employees or employees of his subcontractors pursuant to article 4.2.2 hereof complied with the ban on consumption of alcoholic beverages or misuse of other addictive substances. In case of a breach of this ban the Customer has the right to prohibit to such Contractor's employee an entry to the Delivery Place. In case that such a breach results in a delay in completing the subject of the Contract, the liability will reside with the Contractor. The parties have agreed that the same procedure will apply

also if any employee of the Contractor and of the Contractor's subcontractor pursuant to 4.2.2 hereof commits a crime at the Delivery Place, if obligations pursuant to article 11 and/or 12 hereof are breached or in case of a violent behaviour to the Customer's employees or other persons at the Delivery Place;

4.2.6 make sure that his employees or employees of his subcontractor pursuant to art. 4.2.2 hereof engaged in performance hereof complied during their stay at the Delivery Place with internal regulations, instructions and directives, regulations governing movement of persons, vehicles, materials, fire safety, occupational health and safety and other regulations with which they will be familiarised by the Customer. Training shall take place before the Pilot Operation.

4.2.7 train Customer's employees, or employees of CAH entities in use, management and administration of the System, in the scope pursuant to the Annex No. 1 hereto (hereinafter only as the "Training"). The price for training in the scope stipulated hereunder is included in the Price of the Work. The price for employee training will be stated in the invoice for the Work separately;

4.2.8 handover to the Customer all necessary created source codes/installation files created as a part of the Work on a tangible data carrier or on a substitute data storage device on or before the day of handover of the Work for testing performed in accordance with the Time Schedule.

4.2.9 perform the Work in compliance with requirements stipulated in Annex No. 7 hereto.

4.3 The Contractor will inform the Customer of any outstanding overdue debts arisen out of this Contract no later than within three (3) Business Days so as the Customer could pay them without undue delay.

4.4 The Customer will provide the Contractor with all necessary cooperation consisting in:

4.4.1 providing an access to the Delivery Place,

4.4.2 providing the Contractor with all information, materials and cooperation in the scope and time necessary for performance of the subject hereof,

4.4.3 ensuring the operation of all technical (SW and HW) infrastructure of the surrounding systems associated with the subject hereof.

5. HANDOVER AND TAKEOVER OF THE WORK

5.1 Handover and takeover of the Work will take place on the basis of the acceptance procedure which has five (5) stages:

5.1.1 Installation, Implementation and Customization

5.1.2 Verification Operation,

5.1.3 Penetration test,

5.1.4 Pilot Operation,

5.1.5 Documents handover,

5.1.6 Handover Protocol signing.

5.2 The time period for starting the Verification Operation is three (3) Business Days from the Contractor's request delivered to the Customer after Implementation, unless otherwise agreed by the parties.

5.3 In case the Customer fails to appear on the date specified for performance of the Verification Operation, and does not appear even in the additionally provided time period of three (3) Business Days from after the Contractor's repeated request, the Verificaton Operation will be considered finished without Defects.

5.4 The Parties will sign a record of the completed VerificationOperation.

5.5 If it is established during the Verification Operation that the number of Defects does not exceed the following values:

(a) Category A Defects…….. 0

(b) Category B Defects…….. 0

(c) Category C Defects…….. 10

the Contractor will start performing the Pilot Operation

5.6 If the record of the completed Vefificaton Operation implies that the Work does not meet the criteria stated in art. 5.5 hereof, the Contractor will remove the detected Defects and, after they are removed, the Contractor will call the Customer to start the Verificaton Operation with the art. 5.2 through 5.5 hereof being applied as appropriate. The procedure of testing and subsequent defect removal will repeat until the Contractor meets the acceptance criteria stated in art. 5.5 hereof, however, no more than twice (2x) and no later than by 2 month from the first round of Verification Operation.

Penetration test

5.7 After the successful completion of the Verificaton Operation and meeting the requirements as set forth in art 5.5 hereof, the Customer will carry out a Penetration test, within ten (10) Business days from the signature of the record of the Verification Operation as set forth in art. 5.6 hereof. The performance of the Penetration test will be supplied by a third party at the Customer's expense. The Contractor is obliged to provide all necessary cooperation for the performance of the Penetration test.

5.8 Provider of Pentration test will perform the penetration test report, which could be presented to the Contractor (hereinafter as „P**enetration test Report**").

5.9 In the event that the Penetration test Report does not uncover any security issues in Categories Medium, High, Critical or higher (or their equivalents in meaning), the Contractor is entitled to invite the Customer to take over the Work in writing. Parties have expressly agreed that in case of discrepancies in classification of the security issue the Customer shall determine the category of the security issue. The indicative meaning of the above security issue Categories is listed below:

5.9.1 Security issue Category "Critical" – uncovered vulnerability of the System may be used immediately to compromise the System (gaining access to unprivileged folders, gaining access to the domain/local administrator account, gaining access to other user accounts, potential permanent putting the System out of service, etc.).

5.9.2 Security issue "High" – uncovered vulnerability of the System which, combined with other vulnerabilities or practices, poses a high risk.

5.9.3 Security issue "Medium" – special conditions must be met to misuse the above vulnerabilities or the potential misuse thereof has a limited impact.

5.10 In the event that the Penetration test Report uncovers that the Work shows any security issues of the Categories listed in art. 5.8 hereof, the Contractor undertakes to remedy the uncovered deficiencies and, after the removal thereof, to invite the Customer to initiate the Penetration test again, with art. 5.4 and 5.5 hereof being applied as appropriate. This process and subsequent troubleshooting will be repeated until the Contractor meets the acceptance criteria as set forth in

art. 5.8 hereof, however, no more than twice (2x) and no later than twenty (20) days after the initiation of the first Penetration test. Any repeated Penetration tests will be performed at the Contractor's expense.

Pilot Operation

5.11 The time period for starting the Pilot Operation is three (3) Business Days from the Contractor's request delivered to the Customer after Penetration Test completiton, unless otherwise agreed by the Parties.

5.12 In case the Customer fails to appear on the date specified for performance of the Pilot Operation, and does not appear even in the additionally provided time period of three (3) Business Days from after the Contractor's repeated request, the Pilot Operation will be considered finished without Defects.

5.13 The Parties will sign a record of the completed Pilot Operation.

5.14 If it is established during the Pilot Operation that the number of Defects does not exceed the following values:

(d) Category A Defects…….. 0

(e) Category B Defects…….. 0

(f) Category C Defects…….. 10

the Customer will start performing the Penetration test

5.15 If the record of the completed Pilot Operation implies that the Work does not meet the criteria stated in art. 5.511 hereof, the Contractor will remove the detected Defects and, after they are removed, the Contractor will call the Customer to start the Pilot Operation with the art. 5.8 through 5.11 hereof being applied as appropriate. The procedure of testing and subsequent defect removal will repeat until the Contractor meets the acceptance criteria stated in art. 5.511 hereof, however, no more than twice (2x) and no later than by date set in art. 3.1. hereof.

5.16 After the Pilot Operation is successfully completed and the acceptance criteria are met pursuant to article 5.14 hereof, the Customer will check and confirm the completeness of the Documents and the Contractor will perform the Training and the obligation pursuant to subparagraph 4.2.8 will be fulfilled, and the Parties will sign the Handover Protocol. The Handover Protocol will contain a list of the remaining Defects and security issues detected during the Penetration Test and/or Pilost Operation with the time period set for removal thereof; in the absence of such time period for defect removal, the time period is assumed to be twenty (20) Business Days from the day of signing of the Handover Protocol.

6. LICENSES

6.1 In accordance with the Copyright Act, as amended, and with the Civil Code, as amended, the Parties have agreed that the Contractor grants to the Customer to the Work, software applications created by the Contractor during performance of the Work, as well as to all other Contractor's outputs created hereunder during performance of the Work which are subject to the protection under the Copyright Act a licence with a limited territorial validity in the Czech Republic, in the quantity necessary for operation of the Work as per the Annex No.1 hereto, without any restrictions as regards the manner of use, for the time of duration of the proprietary copyrights to the Work (hereinafter only as "**Licence to the Work**"). The Contractor grants to the Customer the Licence to the Work as a non-exclusive licence. The Parties have agreed that the Customer is not obliged to make use of the Licence to the Work. The Parties have agreed that the Customer has the right to moderate or otherwise change the Work, name of the Work, or combine the Work with other works or include it in a collection of works and subsequently use the Work in this form, use the Work also in the form processed by a third person or in otherwise moderated form, separately

or in a group or in combination with other work or components, in the scope of the Licence to the Work stated in this article 6 hereof. The Customer has also the right to adjust the Work during the term of the Licence to the Work, both by himself or through any third party (namely his subcontractor) and the Contractor grants to the Customer by attaching his signature to the Contract a consent to making the Work available to any third person for the purpose of such adjustments or interventions into the Work pursuant to this article.

6.2 The Contractor agrees that the Customer may use the Work in the scope set forth in article 6.1 hereof in own benefit and for own needs, as well as for the benefit and needs of CAH entities. The Customer has the right to grant the rights which are a part of the Licence to the Work in full or in part to CAH entities (sublicence).

6.3 A fee for the Licence to the Work pursuant to this article 6 is included in the Price of the Work pursuant to article 8 hereof.

6.4 For the avoidance of doubt the Parties expressly state that the Contractor is also obliged to secure for the Customer all Licences or sublicences of the third parties, necessary for the quiet enjoyment of the System.

7. WARRANTIES

7.1 The Contractor hereby warrants that the System will operate in accordance with this Contract and the Documents related to the System and that it will properly process data from all its interfaces, i.e. both data and user interfaces.

7.2 The Contractor hereby warrants that the Work in the supplied form will be free from any viruses which could prevent the Customer on the basis of a pre-defined fact or otherwise from using the Work or its operation could be limited or otherwise adversely affected, or that it will not adversely affect or damage the Systems of the Customer and/or of CAH entities.

7.3 The Contractor represents that he has the right to grant to the Customer the Licence to the Work in accordance with article 6 hereof. The Contractor hereby warrants that the Work or other deliverables of the Contractor delivered hereunder or the use of the Work by the Customer in accordance herewith does not infringe and will not result in any infringement of any third party intellectual property rights. Should the Contractor breach his obligation arising out of the warranty stated in this subparagraph, the Contractor will be liable for all and any consequences resulting from such a breach, including, without limitation, the obligation to immediately and at own costs ensure the right for the Customer to use the Work which will not infringe any third party intellectual property rights and to indemnify the Customer for any damage which may be caused to the Customer, including non-material loss.

7.4 The warranty provided by the Contractor pursuant to art. 7.1 and 7.2 hereof will remain valid for the period of forty twelve (12) months from signing of the Handover Protocol pursuant to article 5.16 hereof. Should it appear in the course of the time period stated in the previous sentence that any of the warranties and assurances pursuant to art. 7.1 or 7.2 hereof is untrue, the Work has Defects and the Contractor agrees to remove them at own costs. The Contractor will start with removal of such Defects, unless the Parties agree on a longer time period, within the following time periods that will start after the Defect is reported to the Contractor's contact data stated in the Annex No. 3 hereto. The time periods stated in the table in this article 7.4 run during the Service Period.

item (Defect category)	Response Time/Start of Defect Removal	Time for Defect Removal	Information frequency (Frequency of ongoing information)

A Category of the Defect of the Work	within 30 minutes	Up to 4 hours	Every 1 hour until the Defect is removed
B Category of the Defect of the Work	Up to 4 hours	Up to 24 hours	Every 6 hours until the Defect is removed
C Category of the Defect of the Work	by the next Business Day	Up to 14 Calendar days	Every 24 hours until the Defect is removed

7.5 The Parties have agreed that the warranty provided by the Contractor under art. 7.1 and 7.2 hereof shall be provided to the Customer only if the Service Level Agreement will be termitade for whatoeverc reason.

7.6 For the avoidance of doubt, the Parties note that regardless of whether the Contractor provides the Customer with a warranty in accordance with art. 7.1 and 7.2 hereof, the Contractor's statutory rights of misconduct are always unaffected, with the Contractor committing to initiate removal of defects (and Defects), unless the Parties agree for a longer period of time, within the time limits specified in art.7.4 hereof from notification Defects on contractor's contact details listed in Attachment 2 to this Contract. The deadlines listed in the table in art 7.4 are done in Service Period. The Contracting Parties hereby agree that the application of the provisions of aro. 13 (13.3) and (13.4) of the Treaty is only possible in the cases referred to in Article 7.5 hereof.

7.7 Warranty for Hardware and Current Hardware

7.7.1 The Contractor hereby grants the Customer a warranty for the quality of the Hardware in the duration of 4 (four) years (“HW warranty”). HW warranty shall commence running from the day following the signing of Handover Protocol.

7.7.2 The Customer shall be obliged to notify any Defect of Hardware occurred during the HW warranty to the Support Center, such notification to be made within such period of time upon discovery of the Defect, as can be reasonable required from the Customer.

7.7.3 The Contractor undertakes to rectifiy a Notified Defect of Hardware as follows:

7.7.3.1 In case of Category A Defect, within 2 (two) Business Days from receipt of the Customer’s Report containing the Defect Notice, unless the Parties agree otherwise in writing.

7.7.3.2 In case of Category B Defect, within 10 (ten) Business Days from receipt of the Customer’s Report containing the Defect Notice, unless the Parties agree otherwise in writing.

7.7.3.3 In case of Category C Defect, within 20 (twenty) Business Days from receipt of the Customer’s Report containing the Defect Notice, unless the Parties agree otherwise in writing.

7.7.4 The Parties hereby agrees on the following Defect of Hardware rectification methods:

7.7.4.1 Replacement of the defective Hardware with defect- free Hardware, or

7.7.4.2 Repair of the defective Hardware, provide that a similar Defect was not claimed more tha three times during HW warranty.

7.7.4.3 Agreement between Parties on a Defect rectification method other than that describet in text above. In such case the Parties shall enter into a written agreement on such other Defect rectification method.

7.7.5 The Contractor grants to the Customer a 6 month warranty period with respect to the quality of any repairs made, provided that such warranty period shall not end earlier than the original HW warranty.

7.7.6 The Contractor grants to the Customer a 6 months warranty for for all services related to the Current Hardware (reinstallation, prophylaxis etc.)

8. PRICE AND PAYMENT TERMS

8.1 The Price of the Work in accordance with this Contract amounts to **42 575 000,00 CZK** (in words: fortytwomillionfivehunderedseventyfivethousands Czech crowns) **without VAT** (hereinafter only as **"Price of the Work"**). The price includes all Contractor's costs of completion of the Work and all supplies of the Contractor hereunder and the detailed breakdown of the price is contained in the Annex No. 2 hereto. The Price of the Work includes the fee for the Licence to the Work pursuant to article 6 hereof.

8.2 The Contractor has the right to invoice the Price of the Work after the Handover Protocol is signed pursuant to art. 5.16 hereof by both Parties. The day of signing of the Handover Protocol is also the day of taxable transaction.

8.3 The Parties have agreed that tax documents issued hereunder may be both in printed and electronic form as pdf.

8.4 The maturity period of an Invoice issued by the Contractor will be thirty (30) days from the day of delivery thereof to the Customer. The Handover Protocol signed by both Parties will be an integral part of the Invoice. Should the due day fall on Saturday, Sunday, or other day of rest, 31st December or other day which is not a business day pursuant to the Act 370/2017 Coll., on Payment System, as amended, the maturity shall be extended to the nearest business day. The Customer's obligation is settled when the due amount is deducted from the Customer's account.

8.5 The received Invoice must comply with all requirements set for a tax document pursuant to the applicable legal regulations of the CR, namely the Act No. 235/2004 Coll., on Value Added Tax, as amended, and must contain objectively correct data in relation to the supply. After the Customer receives the invoice, he has fifteen (15) days to assess whether or not it is correct or return it, if it contains errors. After the incorrectly issued Invoice is returned, the maturity period is interrupted and a new maturity period starts again after delivery of the correctly issued Invoice to the Customer.

8.6 The Price of the Work will be paid directly to the Contractor's bank account with a bank in the Czech Republic and specified in this Contract the number of which is published by the tax administrator in the manner enabling a remote access (in accordance with the applicable version of the Act No. 235/2004 Coll., on Value Added Tax), unless the Invoice states other bank account the number of which is published by the tax administrator in the manner enabling a remote access (in accordance with the applicable version of the Act No. 235/2004 Coll., on Value Added Tax).

8.7 If the Contractor in accordance with the Act No. 235/2004 Coll., on Value Added Tax:

8.7.1 is appointed by a decision of the tax administrator an unreliable payer, or

8.7.2 demands payment for a taxable supply provided hereunder to the bank account which is not published by the tax administrator in the manner enabling a remote access, or to the bank account kept by the payment service provider outside the territory of CR,

the Customer has the right to pay to the Contractor's bank account only the Price of the Work for the provided taxable supply without a value added tax (hereinafter only as "**VAT**"). The Customer

may pay VAT, if chargeable and if it is according to the Contract included in payment by the Customer, directly to the account of the relevant tax administrator. In such case the amount corresponding to VAT is not considered an amount due to the Contractor and the Contractor is not entitled to demand payment of VAT or impose any contractual sanctions, default interest or penalties. The Customer will inform the Contractor of such procedure on or before the date of payment of the Price of the Work.

8.8 The mailing address for delivery of Invoices is:

In electronic form as pdf. to the mailbox:

[redacted]

or in a printed form to the address:

Letiště Praha, a. s.
Register of invoices
Jana Kašpara 1069/1
160 08 Praha 6

8.9 The Customer is authorized to lower the paid Price by the paid withholding tax or other similar tax in the case when payment of the Price shall be in, accordance with Czech tax regulations, subject to withholding tax or other similar tax. In such case the sum amounting to withholding tax or other similar tax shall not be considered as an unpaid liability of the Customer against the Contractor.

9. LIST OF PERSONS

9.1 The employees or authorised persons named in the Annex No. 3 hereto are authorised to act in organisational-technical matters.

9.2 The Parties may replace the employees or authorised persons named in the Annex No. 3 hereto upon a written notice to the other Party.

10. CONTRACT TERM

10.1 This Contract will come into force and effectivity as of the day of its signing by both Parties, However, if a special legal provision stipulates that this Contract may enter into force at the earliest on a certain day which is later than the date of signature of this Contractt by the last Party, this Contract shall become effective only on the date on which this Contract may become effective in the first instance (hereinafter only as "**Effective Date**")The effectiveness and force of this Contract terminates:

10.1.1 by a written agreement of the Parties;

10.1.2 by a notice of withdrawal pursuant to this art. 10 hereof;

10.1.3 upon fulfilment of all obligations under this Contract, except for the obligations which survive the termination hereof (namely art. 4.1, 6 and 7 hereof).

10.2 The Parties have agreed that the Customer has the right to withdraw from this Contract, in addition to the cases stated in the applicable legal regulations, also when:

10.2.1 the Contractor fails to meet the acceptance criteria for completion of the Pilot Operation, not even after two Pilot Operations pursuant to art. 5.11 and following., or

10.2.2 the Contractor fails to meet the acceptance criteria for completion of the Penetration Test, not even after two Penetration Tests pursuant to art. 5.9 hereof, or

10.2.3 the Contractor fails to fulfil his obligation stated in article 3.1 hereof;

10.2.4 the Contractor enters into a contract or contracts with a subcontractor for performance of the Work or any part thereof without the Customer's previous consent, or

10.2.5 the Contractor breaches any of the obligations pursuant to art. 4.2 hereof and fails to remedy the breach not even within twenty (20) Business Days from delivery of the Customer's written request,

10.2.6 the Contractor finds himself in the situation when (i) the court has initiated insolvency proceedings in accordance with the valid and effective legal act governing insolvency, bankruptcy and the methods of resolving it (hereinafter only as "**Insolvency Act**") or (ii) the court has decided on bankruptcy in accordance with the Insolvency Act, or (iii) the court has decided on the annulment of bankruptcy because of the lack of the debtor's assets to settle the creditors' claims, or (iv) the Contractor filed an insolvency motion against himself in accordance with the Insolvency Act, or (v) a resolution has been adopted on mandatory or voluntary dissolution of the Contractor (except for mergers, amalgamation or other case of legal succession).

10.3 The Contractor has the right to withdraw from this Contract also if

10.3.1 the Customer is late with payment of any amount legitimately invoiced by the Contractor and such delay continues more than thirty (30) days from the Contractor's written notice delivered to the Customer.

10.4 Withdrawal comes into effect from the day of delivery of the notice to the other party.

10.5 The Parties have agreed that even after the termination hereof in any of the manners stated herein or in the applicable legal regulations, the force and effect of the provisions governing contractual sanctions, art. 11. and art. 12 hereof will survive.

11. CONFIDENTIAL INFORMATION

11.1 The Parties have agreed that all and any Confidential Information which they have exchanged in the course of concluding and performing this Contract, as well as any information which forms the contents hereof and information which they may exchange or which may otherwise arise out of performance of this Contract will remain confidential according to their will.

11.2 The Parties have agreed that they will not disclose the Confidential Information to any third parties and they will adopt such measures which will prevent disclosure of such information to third parties. The provisions of the previous sentence will not apply to the cases when:

11.2.1 the Parties have an opposite obligation stipulated by law; and/or

11.2.2 they disclose such information:

11.2.2.1 to persons who have a confidentiality obligation by the operation of law; and/or

11.2.2.2 to subcontractors, or other advisers, employees providing that (i) the relevant Party will be informed of such disclosure in good time, and that (ii) the relevant persons to whom the Confidential Information is disclosed will accept a written obligation to keep secrecy and confidentiality of the information received, at least in the scope stipulated hereunder, and/or

11.2.2.3 the Customer to the CAH entities and/or to the Controlled Persons, including the company Letiště Praha, a. s.; and/or

11.2.3 such information becomes a public domain or available to public otherwise then through a breach of obligations arising out of this article; and/or

11.2.4 one Party grants a written consent to the other Party to disclose the information to a third party.

11.3 The Contractor will make sure that the obligations stipulated in this article 11 were observed by all his employees and subcontractors who are in any manner engaged in performance of the subject hereof and any third parties to whom the Customer's Confidential Information was disclosed by the Contractor in any form. For the avoidance of any doubts the Contractor represents and agrees that he will be liable in full for any violation of the obligations stipulated in this article 11 by his employees and/or subcontractors and/or third parties to whom the Confidential Information of the Customer was disclosed by the Contractor in any form and he will indemnify the Customer in full for any damage caused by such a violation, including a non-material damage.

11.4 The Customer will make sure that the obligations stipulated in this article 11 were observed by all his employees and any third parties to whom the Contractor's Confidential Information was disclosed by the Customer in any form. For the avoidance of any doubts the Customer represents and agrees that he will be liable in full for any violation of the obligations stipulated in this article 11 by his employees and/or third parties to whom the Confidential Information of the Contractor was disclosed by the Customer in any form and he will indemnify the Contractor in full for any damage caused by such a violation, including a non-material damage.

11.5 The obligations contained in this subparagraph related to keeping a confidential character of information will remain in full force and effect regardless of the termination hereof.

12. PERSONAL DATA PROTECTION

12.1 Should the Contractor come during fulfilment of his obligations hereunder into contact with Personal Data, he agrees to comply with all applicable legal regulations, namely the Act on Personal Data Protection.

12.2 The Contractor further agrees to technically and organisationally provide his supplies hereunder so that Personal Data was appropriately protected and treated in accordance with the Act on Personal Data Protection. The Contractor agrees to prevent any unauthorised or incidental access to Personal Data, or unauthorised change, destruction or other misuse thereof.

13. CONTRACTUAL PENALTIES AND INDEMNIFICATION

13.1 Should the Contractor fail to comply with the deadline set for delivery of the Work stated in art. 3.1 hereof, the Customer is entitled to claim from the Contractor a contractual penalty in the amount of 0.05% of the Price of the Work according to article 8 hereof for each, even commenced, day of such delay.

13.2 Should the Contractor fail to remove the Defects or security issues detected during the Penetration Test stated in the Handover Protocol by the date stated in art. 5.16 hereof, the Customer is entitled to claim from the Contractor a contractual penalty in the amount of CZK 10,000 for each, even commenced, day of such delay.

13.3 Should the Contractor fail to start with removal of the Defects stated in article 7.4 hereof, the Customer is entitled to claim from the Contractor a contractual penalty in the amount of CZK 1,000 for each, even commenced, day of such delay.

13.4 Should the Contractor fail to remove the Defects within the time limit stated in 7.4 hereof, the Customer is entitled to claim from the Contractor a contractual penalty in the amount of 10,000 for each, even commenced, 24 consecutive hours, or for each commenced day of such delay, if applicable.

13.5 Should the Contractor breach the obligation pursuant to article 11 and/or article 12 hereof, the Customer is entitled to claim from the Contractor a contractual penalty in the amount of CZK 100,000 for each such breach.

13.6 Should the Contractor breach the warranty pursuant to article 7.3 hereof, the Customer is entitled to claim from the Contractor a contractual penalty in the amount of CZK 100,000 for each such breach.

13.7 Payment of the relevant contractual penalty will be without prejudice to the Customer's right to claim the compensation for damages caused to the Customer in consequence of a breach of any obligations of the Contractor secured by the contractual penalty pursuant to this Contract. In case the contractual penalty is reduced by a court ruling, the Customer's right to claim damages in full remains unaffected. If any legal regulation sets a penalty for a breach of the contractual obligation (at any time during the term hereof), the Customer's right to claim damages in full will not be affected by such a claim.

13.8 The contractual penalty is payable within fourteen (14) days from the day of delivery of a written payment request served by the Customer to the Contractor.

13.9 The Contractor hereby explicitly agrees to indemnify the Customer for any non-material damage caused to the Customer as a result of a breach of the Contractor's obligation in accordance with this Contract and/or in connection herewith.

13.10 The Parties have agreed that the Customer's obligation to indemnify the Contractor for damages caused to the Contractor as a result of a breach of the Customer's obligation in accordance with this Contract and/or in connection herewith is excluded in a maximum scope permitted by the applicable legal regulations.

13.11 If any financial amount is to be paid by the Contractor to the Customer which yields interest, the Parties have agreed explicitly that in such case the default interest may be requested.

13.12 If one fact results in a breach of more articles hereof and therefore the Contractor's obligation to pay the contractual penalty should be constituted pursuant to two or more provisions of art. 13. hereof, the Contractor will pay to the Customer the contractual penalty only according to the provision of art. 13 hereof which constitutes the obligation to pay higher contractual penalty.

14. CONTRACT DATA AND NOTICES

14.1 All and any notices or documents which are to be made in writing in accordance with this Contract, must be, unless the Contract states otherwise, delivered personally or mailed as a registered mail or by a courier to the contact data of the other Party. Contact data of the Parties are contained in the Annex No. 3 hereto.

14.2 The communication other than stated in the previous art. 14.1 hereof may be made by any of the Parties, unless the Contract states otherwise, vis-a-vis the other Party via email or fax to the contact data of the other Party.

14.3 Each Party will inform the other Party without undue delay of any change in its contact data stated in Annex No. 3 hereof in the form of a registered mail or by email sent to the contact address stated in Annex No. 3 hereto (as amended). Upon proper delivery of this notice the mailing address of the relevant Party will be changed without any further amendments to the Contract.

14.4 Unless this Contract states otherwise, any communication in connection with this Contract will be considered delivered to the other Party:

14.4.1 if delivered by registered mail on the third (3rd) Business Day after the day of handing the notice in correctly addressed envelope to the postal service with postage prepaid,

14.4.2 if delivered by fax after a fax machine of the mailer prints out the confirmation of a successful transmission to the correctly entered fax number of the other Party, and

14.4.3 if delivered by email after the respective email message was delivered to the correctly entered email address of the other Party - confirmation from the addressee's email server.

15. OTHER PROVISIONS

15.1 The Contractor is not entitled to assign this Contract or any of his rights and obligations from this Contract to a third party without the Customer's previous written consent, not even partially.

15.2 The Parties have explicitly agreed that:

15.2.1 The Contractor has the right to offset his due and not yet due claims to the Customer only on the basis of a written agreement with the Customer.

15.2.2 The Contractor is not entitled to pledge any of his claims to the Customer arisen out of this Contract.

15.3 The Contractor is obliged to prove no later than by the day this Contract is concluded that he maintains general liability third party insurance for the insured sum which will not be less than CZK 1,000,000 to cover any damage caused during performance of the Work to the Customer or any third party. By entering into this Contract the Contractor also agrees to maintain this insurance coverage in the same or larger extent until the end of validity hereof. The Contractor agrees to submit to the Customer at any time during the Contract term at the Customer's request within two (2) Business Days a proof of the existence of such insurance.

16. FINAL PROVISIONS

16.1 If any provision of this Contract is held invalid, unenforceable or ineffective, the validity, enforceability or effectiveness of the remaining provisions hereof shall remain unaffected. The Parties will replace such invalid, unenforceable or ineffective provision within five (5) Business Days after delivery of the request of the other party by a new valid, enforceable and effective provision the contents of which will correspond to the purpose contemplated by the original provisions and this Contract as a whole.

16.2 Force Majeure.

16.2.1 Neither Party will be considered late with fulfilling its obligations arisen from the Contract due to occurrence of the event of Force Majeure, providing that such event hinders or substantially affects performance of the obligations of such party arisen from the Contract. The immediately preceding sentence of this subparagraph will apply only during the existence of such event of Force Majeure or consequences thereof and only in relation to the specific obligation or obligations of the Party directly or immediately affected by such event of Force Majeure.

16.2.2 Events of Force Majeure mean such circumstances that could not have been foreseen by the Party at the time of execution of the Contract and that objectively prevent the Party from performing its obligations arisen from the Contract. Events of Force Majeure include, without limitation, war, embargo, state or governmental interventions, terrorist attack, natural disasters and strikes of the Customer’s employees. For the avoidance of any doubts the events of Force Majeure do not include any delay in fulfilling the obligations by any of the Contractors or the Contractor's business partners vis-à-vis the Contractor, strikes of employees of the Contractor and the Contractor’s business partners, as well as insolvency, heavy indebtedness, bankruptcy, composition, winding up or the occurrence of other similar event related to the Contractor or any of the Contractor’s business partner and the execution of the assets of the Contractor or any of the Contractor’s business partners.

16.2.3 Should any of the events of Force Majeure occur as described in article 16.2.2 hereof, the Contracting Party on whose part the obstacle has occurred, shall take all necessary

measures which may be reasonably required from it that will lead to restoring normal activities in accordance with the Contract as soon as possible with respect to the circumstances that caused such event of Force Majeure. The Contracting Party shall inform the other party of the occurrence of any event of Force Majeure without undue delay after such communication becomes objectively possible.

16.2.4 Should the event of Force Majeure last longer than ten (10) Business Days, the Contracting Parties shall exercise the utmost efforts which may be reasonably required from them to find suitable solution of the situation occurre

16.3 The Customer notifies the Contractor and the Contractor acknowledges that the Customer intends to execute the merger in accordance with Act No. 125/2008 Coll., on transformations of companies and cooperatives. The parties expressly agree and the Contractor hereby expressly gives their consent with the transfer of the rights and obligations of this Agreement to the entity, which would be the legal successor of the Customer in accordance with Act No. 125/2008 Coll., on transformations of companies and cooperatives.

16.4 Should any of the Parties oversee or waive any default, breach, delay or non-compliance with any obligation arising out of this Contract, such activity or non-activity shall not constitute a waiver of such obligation with respect to its continuing or subsequent default, breach or non-compliance and no waiver shall be considered effective, unless explicitly expressed in writing for each individual case.

16.5 The rights and obligations of the Parties which are not explicitly regulated herein shall be governed by the provisions of the Civil code and other applicable legal regulations of the Czech Republic. The Contract, as well as the relationship between the Customer and the Contractor and the rights and obligations of the Contracting Parties arising out of it shall be governed and interpreted in accordance with the Czech law.

16.6 The Contractor assumes the risk of a substantial change of circumstances which may constitute an especially gross disproportion between the rights and obligations of the Parties pursuant to Section 1765 (2) of the Civil Code. Hence, the Contractor shall not be entitled to claim the restoration of negotiations about the Contract in case of such substantial change of circumstances pursuant to Section 1765 (1) of the Civil Code.

16.7 The Contractor is not entitled to file a motion with the court seeking a change of the obligations constituted by the Contract pursuant to the provisions of Section 1766 of the Civil Code.

16.8 This Contract is entered into between independent commercial operators within their course of business and therefore the Contract is not in accordance with the provisions of Section 1797 of the Civil Code subject to the provisions of Sections 1793 through 1795 of the Civil Code on disproportional reduction or the provisions of Section 1796 on usury.

16.9 Since the Contract is concluded between commercial operators within the course of their business activities, the Parties have also agreed in accordance with the provisions of Section 1801 of the Civil Code that for the purpose of this Contract the provisions of Section 1799 and Section 1800 of the Civil Code on contracts concluded in an adhesion manner will not apply.

16.10 The Parties have agreed that by payment of the contractual penalty by the Contractor, the Customer's right to claim damages in full remains unaffected. In case the contractual penalty is reduced by a court ruling, the Customer's right to claim damages in full remains unaffected. If any legal regulation sets a penalty for a breach of the contractual obligation (at any time during the term hereof), the Customer's right to claim damages in full will not be affected by such a claim.

16.11 This Contract contains a full agreement about the subject hereof and about all essential requisites which the Parties should and wanted to include in the Contract and which they consider important to make this Contract binding. Neither any manifestation of will made by the Party during negotiations regarding this Contract, nor any manifestation made after this Contract is concluded, will be construed in conflict with explicit provisions hereof, nor shall it establish an obligation on

the part of any of the Parties. This Contract supersedes all other written or oral agreements made in the matter of the subject hereof.

16.12 Unless otherwise explicitly stipulated herein, the Parties have agreed that they do not wish to derive any rights and obligations from the existing or future practise established between the Parties or usage maintained generally or in industries related to the subject hereof outside the explicit provisions hereof.

16.13 The Parties have informed each other of all and any material and legal circumstances which they have known or must have known as at the day of signing this Contract and which are relevant in relation to entering into this Contract. Except for the assurances the Parties have provided in this Contract, neither Party will have any other rights and obligations in connection with any facts which may appear and about which the other Party failed to provide information during negotiations about this Contract. The situations when the relevant Party wilfully confused the other Party regarding the subject hereof will be an exception.

16.14 For the avoidance of all doubts the Parties state that no obligation hereunder is a fixed obligation pursuant to Section 1980 of the Civil Code.

16.15 By means of the derogation from Section 1987 (2) of the Civil Code, the Parties have agreed that uncertain and/or unspecific claim of the Customer will be fit for offsetting.

16.16 The Customer may object invalidity of the Contract and/or any amendment hereto due to non-compliance with the requisite form at any time, even if performance has already started.

16.17 The provisions of Section 1932 and Section 1933 of the Civil Code will not apply to this Contract and obligations arisen out of the Partial Purchase Contracts. If more due obligations arisen out of this Contract exist, it is the reserved right of the Customer to determine which obligation must be fulfilled as first.

16.18 For the avoidance of doubts the Parties have agreed that a monetary debt arisen out of this Contract cannot be settled by means of a bill of exchange.

16.19 The Parties have agreed to resolve all disputes which may arise between them in connection with performance or interpretation hereof by amicable negotiations and reciprocal agreement. If they fail to resolve the dispute within thirty (30) days from the day it has arisen, such dispute will be submitted by one Party to the competent court having the local and subject-matter jurisdiction over the matter. The Parties have hereby agreed on the local jurisdiction of general court of the Customer pursuant to Section 89a of the Act No. 99/1963 Coll., the Rules of Civil Procedure, as amended.

16.20 The Customer notifies the Contractor and the Contractor acknowledges that the Customer is a person stated in Section 2 (1) n) of the Act No. 340/2015 Coll., on Special Requirements for Effectiveness of Certain Contracts, the Disclosure of These Contracts and the Register of Contracts (Act on the Register of Contracts). This Contract shall be published in the Register of Contracts.

16.21 Trade secrets. The Parties declare that no facts stated in this Contract [and its annexes] constitute a trade secret within the meaning of Section 504 of the Civil Code.

16.22 The Contract has been drawn up in three (3) counterparts in the English language of which the Customer will receive two (2) and the Contractor one (1) counterpart.

16.23 The Contractor, as a party against which the rights of the Customer as a creditor from this Contract are barred by the statute of limitation, hereby extends, after wise consideration, by his explicit representation the length of the prescription period with respect to the rights of a creditor (i.e. the Customer) arising out of this Contract for the time period of fifteen (15) years.

16.24 The Contract may be amended and supplemented only by written continuously numbered amendments signed by both Parties. Any change of this provision regarding a change of the

Contract must be made also by means of a written amendment signed by both Parties. The Customer may object invalidity of the Contract and/or any amendment hereto due to non-compliance with a written form at any time, even if performance has already started.

16.25 In case of any conflict between the text of the Contract and the Annexes hereto, the text in the Contract shall prevail.

16.26 The following annexes make an integral part of this Contract

16.26.1 Annex No. 1 – Technical and Functional Specification of the System

16.26.2 Annex No. 2 – Detailed Calculation of the Price of the Work

16.26.3 Annex No. 3 – Contact Persons

16.26.4 Annex No. 4 - Implementation Time Schedule

16.26.5 Annex No. 5 – Current Hardware description

16.26.6 Annex No. 6 – Hardware description

16.26.7 Annex No. 7 – Cyber security requirements

THE PARTIES HEREBY DECLARE THAT THEY HAVE READ THIS CONTRACT AND AGREE WITH ITS CONTENTS, IN WITNESS WHEREOF THEY ATTACH THEIR SIGNATURES:

Date:	Date:
For the Customer:	For the Contractor:
Signature: _____	Signature: _____
Name: Mr. Jiří Kraus	Name: Ing. Jakub Maléř
Title: Vice-Chairman of the Board of Directors Letiště Praha, a. s.	Title: Member of Board of Directors
Signature: _____	Signature: _____
Name: Mr. Jiří Černík	Name: Ing. Petr Otoupal
Title: Member of the Board of Directors Letiště Praha, a. s.	Title: Member of Board of Directors

Annex No. 1 – Technical and Functional Specification of the System

FLIGHT INFORMATION DISPLAY SYSTEM

Functional and Technical Specifications

CONTENTS

1. Introduction

The subject-matter of the contract is the replacement of the existing FIDS (Flight Information Display System) at Václav Havel Airport Prague. The operating IT environment is provided by the parent company Letiště Praha, a. s. (hereinafter referred to as the "Contracting Authority"). FIDS means primarily the system displaying information from the Airport Operational Database (AODB) on approx. 1,000 monitors in compliance with editable rules and in editable design. The system for data exchange with the AODB must support Message Queue Interface. The system must support different fields in accordance with the AODB and enable their modifications/extension according to the operating requirements. The system also contains the functionalities specified below.

The system will be installed and operated in the Contracting Authority's internal environment, its operation and administrator support will be covered by the Contracting Authority's employees, the servicing of the System will be contractually agreed with the supplier.

2. Accronyms and terms

FIDS of the System – Flight Information Display System
AODB – Airport Operational Database
Contracting Authority – Letiště Praha, a. s.
System – requested FIDS
Safe Mode – temporary state of the System enabling the use of selected functions in case of failure

STD – Scheduled Time of Departure
STA – Scheduled Time of Arrival
ATD – Actual Time Of Departure
ATA – Actual Time of Arrival

3. Technical requirements

3.1. Infrastructure

The System must support the Windows Server 2016 operating system running within the VMWARE virtual platform. The technical standards of the Contracting Authority's infrastructure are contained in Annex 1.

The System must be operated within the operating, backup and testing environments.

3.2. Database

The System must support at least one of the databases described in Annex 1.

If the System supports another database, provision of the particular database licenses, the installation of the database as well as its configuration and maintenance is provided by the Supplier.

3.3. Interface

The System must support transmission of data from the Contracting Authority's existing AODB through XML messages using one of the following interfaces supported by the existing AODB:

- ActiveMQ
- IBM MQ
- Oracle Advanced Queuing
- Web Services

The installation (or license) of such interface is included in the contract.

3.4. Data

The data to be displayed within the System which are available for transmission from the AODB are described in Annex 2. The System is able to receive and display all such data within all outputs (FIDS monitors, XML reports, HTML websites).

3.5. Production environment

The System must be primarily operated in the production environment which is optimized in terms of performance in order to utilize all the functions of the System.

3.6. Backup environment

In addition to the production environment, the System must be operated in the backup environment which is fully compatible with the production environment in terms of its functions and which is completly separated from production environment.

In case of failure of the production environment, the System must make it possible for trained employees of the CONTRACTING AUTHORITY to switch the System over to the operation in the Backup Environment within 20 minutes max., and the System run in the Backup Environment must be able to operate f at least the functions described in 4.1.

3.7. Test environment

In addition to the production and backup environments, the System must be operated in the test environment which is, in terms of its functions, fully compatible with the production environment. The test environment contains its own interface for data transmission from the test AODB.

3.8. Monitoring

The System must ensure the monitoring of its basic functions and in case of their failure it sends notification messages to pre-defined receivers via email or other channels.

3.9. Graphical user interface

The System must contain a graphical user interface for the System administration and configuration. The access to the graphical user interface must be subject to user authorization.

The System must make it possible to set/restrict privileges for the administration and configuration in the graphical user environment for each of the users.

4. Functional requirements

4.1. FIDS screens

The System must enable the operation of 1,500 FIDS screens with the option to extend the number further.

The System must enable the administration, monitoring, live preview and remote configuration of each screen, or graphic controller, if applicable.

Each screen may be configured separately, and each screen may display different information.

The System must enable at least in the 1280x768, 768x1280 display resolution (portrait orientation), and 1920x1080, 1080x1920 display resolution (landscape orientation).

Each display may use any relating data from the AODB described in Annex 2.

Any displayed information may be defined and changed depending on the data from the AODB (such as specific display for selected airlines etc.).

The number of defined displayed information is not limited.

4.1.1. Departures + arrivals

In order to display the departure/arrival information, the System must enable filtering and sorting by any relating field (e.g. it must be capable of displaying only flights from T1 sorted by departure time etc.).

Display of each flight may be changed depending on the relating data from the AODB (e.g. differentiate a flight of XXX in the list of departures).

It is possible to set a time window for the flights for each displayed departure/arrival depending on the data from the AODB (e.g. X minutes before STD/STA to X minutes after ATD/ATA and/or X minutes after STD/STA).

4.1.2.Check-ins

A special type of information display defined on the basis of data about check-in desks. Information displayed for each flight/check-in desk may be changed depending on all the relating data from the AODB.

4.1.3.Gates

A special type of information display defined on the basis of data about gates. Information displayed for each flight/gate may be changed depending on all the relating data from the AODB.

The System must be able to process information about gate change with respect to a flight so that information about the original gate is displayed with the currently handled flight.

4.1.4.Arrival belts

A special type of information display defined on the basis of data about arrival belts. Information displayed for each flight/belt may be changed depending on all the relating data from the AODB.

4.1.5.Departure belts

A special type of information display defined on the basis of data about departure belts. Information displayed for each flight/belt may be changed depending on all the relating data from the AODB

4.1.6.User texts

A web GUI is operated in the System which can be used by the users, once they login using their username and password, to enter user texts linked to a specific screen of the System. Such texts may be used in the System to display on such screens. The web GUI may be used to activate/deactivate already entered texts for display on screens, while using their value in the GUI. The GUI must support Firefox and Google Chrome browsers.

The web GUI may be used to manage (light up/switch off) screens in other desks, except for standard check-in desks and boarding desks, and to display user texts on them.

Using the web GUI, the System must enable to enter a running text on selected screens.

4.1.7.Staff screens

A special type of screens, or graphic controller, which enable to scroll within the display, and to switch between supported, pre-defined displays in the System using a connected numeric keypad. Privileges to different, pre-defined displays may be configured for each staff screen, thus determining/limiting which displays may be switched between each particular screen.

4.1.8.Presentation monitors

The System must make it possible to define information to be displayed on screens without links to data from the AODB.

4.1.9.External screens

The System makes it possible to operate screens, or graphic controller, if applicable, outside the premises of the LKPR airport, communicating online with part of the system V DMZ according to the description of technical standards in Annex 1.

4.1.10. Other functions

4.1.10.1. Emergency

The System contains a module enabling to pre-define special information to be displayed on defined groups of screens in the event of emergency, and to launch/cancel such scenarios easily via the administration GUI.

4.1.10.2. Translations

The System must contain multilingual lists of codes of airlines, city destinations, operating notes. Such code lists in all language versions (incl. special characters) may be used for displaying.

4.1.10.3. Fonts

The System must make it possible to enter and use any True Type and Open Type Font. One display may use multiple fonts.

4.1.10.4. Colours

The System must support True Color.

4.1.10.5. Data editing

The System must make it possible to manage (suspend, initiate) transmission of data from the CAODB and simple data editing directly in the System in order to ensure operational functioning in the event of failure of the AODB.

4.1.10.6. DISPLAY PagES

The System must make it possible to display various number of departures/arrival list pages. The System must enable automatic change of information size on the basis of its number in the given display.

4.1.10.7. Planning

The System must make it possible to plan automatic change of displayed information on a particular screen/group of screens on the defined day and at the defined time.

4.1.10.8. HTML display

The System must make it possible to display an external html page or RSS feed on the whole page or part of the page.

4.1.10.9. CodesharEs

The System must support the display of code-shared flights, both in the variant one flight per codeshare, and also in the variant of displaying only the core flights and animation of numbers of code-shared lines. The System must support at least 10 codes-hared flights.

4.1.10.10. Images and videos

The System must support the display of usual image formats, at least JPG, PNG. The System enables displaying different images using the data from the AODB, such as logotypes of airlines, handling companies etc.

The System must support the display of usual video formats, at least WMV, MP4, in FullHD. The System enables displaying different videos using the data from the AODB, such as videos by airlines, etc.

4.1.10.11. Animation

The System must make it possible to animate texts, both pre-defined and amended texts, depending on the data from the AODB, as well as images, both pre-defined and amended images, depending on the data from the AODB, at least in the number of 50. Animation may be defined as rolling horizontally and vertically, instant gradient and blend.

4.1.10.12. Synchronization

All animations, as well as video playing, must be synchronized on screens.

4.1.10.13. History

The System must make it possible to track the history of changes of displayed data from the AODB in relation to a specific flight without any time restrictions.

4.1.10.14. Code lists

The System contains its own multilingual code lists of city destinations, airlines, system notes and user texts. The code lists of city destinations, airlines, system notes and user texts, or their values in English language, will be automatically uploaded from the AODB via the interface.

4.1.10.15. Weather

The System must make it possible to display information about the weather in the city of destination or the city of origin in the form of temperature in degrees Celsius and infographics about the current weather conditions (clear, cloudy etc.). If the use of such information is licensed, the license fee must be included in the price of the System. Information about the weather must be included in the XML report defined in 4.3 and exported out of the System.

4.2. HTML pages

The System makes it possible to generate websites compatible with the Firefox and Google Chrome browsers, with the content definable in a similar way as in case of the FIDS screens, using any data from the AODB described in Annex 2. The System must make it possible to enter images in the websites in a similar way as in case of the FIDS screens. The websites are published in the web server within the System infrastructure, both within the internal network of the Contracting Authority and within DMZ for online access. For online access, the websites are secured with a username and password which are managed directly by the System and which are available via a HTTPS protocol.

4.3. XML reports

The System must enable generic reports in the XML format with the content definable in a similar way as in the case of FIDS screens, using any data from the AODB described in Annex 2. The System must enable creating reports for arrivals and departures separately. The reports are published on the web server within the System infrastructure, both in the internal network of the Contracting Authority and within the DMZ for online access. With respect to online access, the reports are secured with a username and password which are managed directly by the System, and they are available through a HTTPS protocol. The required structure of XML report is described in Annex 3.

5. Non-functional requirements

5.1. Installation

The installation of the System is ensured by the Supplier in cooperation with the employees of the Contracting Authority in accordance with the installation plan previously approved by the employees of the Contracting Authority.

5.2. Training

The Supplier shall organize System administration training for 2 employees of the Contracting Authority.

6. Graphic controllers

6.1. System operation on newly supplied graphic controllers

The target of the System is 1,100 pcs of graphic controllers, incl. licenses necessary for their operation within the System.

The graphic controllers will be supplied with pre-installed software necessary for their operation within the System.

The supply of the graphic controllers will include their certification for 24x7 operation from the manufacturer.

The supply of each graphic controller will include 1 power cable 1.5m, 1 power adapter (if applicable), 1x HDMI cable 1.5m, 1x Patch Cord UTP CAT5E 1m.

The graphic controllers contain the following inputs and outputs: HDMI, VGA, 3,5mm jack audio, 2x USB, 100MB/s LAN

The graphic controllers are fanless, with memory storage without mechanically moving parts.

Maximum dimensions of graphic controllers: 25 x 22 x 7cm.

The Supplier provides a 4-year warranty for the graphic controllers supplied.

6.2. System operation on existing graphic controllerS of Contracting Authority

If the System enables the operation on the existing graphic controllers of the Contracting Authority described in cl. 6.2.1 and 6.2.2., the Supplier shall be provided with 400 pcs of graphic controllers for their reinstallation, using the existing licenses on the Windows 7 Pos Ready possessed by the Contracting Authority. If another license is necessary for their operation, the same shall be provided by the Supplier. The re-installed graphic controllers will be used within the contract in accordance with cl. 6.1, except for the warranty for delivered graphic controllers. The graphic controllers are provided to the Supplier in a demonstrably functional condition. If they are damaged during the re-installation, the Supplier shall ensure their repairs, or replacement in accordance with cl. 6.1, if applicable. The Supplier shall provide a 6-month warranty for the existing reinstalled graphic controllers.

6.2.1. AMD G-T40E 1GHz 2 cores, 4GB RAM, 16GB HD, RadeoN HD6250

340 pieces

6.2.2. INTEL CELERON J1900 1,99GHz 4 cores, 4GB RAM, 32GB HD, INTEL ATOM E3800

60 pieces

6.3. System operation on other graphic controllers

The Supplier must enable the operation of the System on other graphic controllers of the Contracting Authority complying with the recommended HW configuration of the Supplier.

6.4. Requirements for operation of graphic controllers

- Graphic controllers support network authentication 802.1x - EAP-TLS and the System must support remote, mass distribution of certificates to graphic controllers. If the System does not provide this kind of support, the Supplier will provide a list of MAC addresses of all graphic controllers and each graphic controller will bear a label with the relevant MAC address.
- If graphic controller is run without any connection to the server, an image provided by the Contracting Authority is displayed.
- In the event of failure of communication between the graphic controller and server which lasts less than 10 minutes, the latest existing state is displayed.
- In the event of failure of communication between the graphic controller and server which lasts more than 10 minutes, an image provided by the Contracting Authority is displayed.
- Updates of the System on graphic controllers may be done in a remote and mass manner.
- graphic controllers must support 1280x768, 768x1280 resolution (portrait orientation), 1920x1080, 1080x1920 (landscape orientation).

7. Annexes

Annex 1 – Technical standards for ICT in the environment of CONTRACTING AUTHORITY

Annex 2 – Data from AODB to be displayed within the System

Annex 3 – Specifications of XML reports

Annex No. 1 Technical standards for ICT in the environment of CONTRACTING AUTHORITY of Annex No. 1 – Technical and Functional Specification of the System

CONTENTS:

I Acronyms and terms

I.1 Acronyms

Acronym	Explanation
AS	Application server
LP	Letiště Praha, a.s. - parent company of holding structure
DB	Database
DMZ	Demilitarized zone (FW separated network; Access to computers and applications is controlled by FW rules)
FW	Firewall
ICT	Information and communication technology – LP's organizational unit
MQ	WebSphere MQ - communication middleware for sending and receiving messages between distributed systems
OS	Operation system
M/INF	Manager of ICT Infrastructure OU
HM/IL	Head Manager of ICT and Legal OU
CEO/ICT	CEO of ICT OU
UNIX, WINDOWS, AIX, Linux, RedHat SUN, SYBASE, IBM, Oracle etc.	Abbreviations for individual technological solutions as per manufacturers and field of service
TCP/IP	Network communication protocol

WMB	WebSphere Message Broker

I.2 Terms

Term	Explanation
Application	An application/system ensuring required functions for certain user group in LP
Interface	Program element intended for linking two or more different systems for data sharing or transfer
Login	Unique user name in LP's computer network environment
User	Employee with access rights for ICT environment (identified by login)

II Responsibility and competences

Role/position name	Description of responsibilities and competences
Administrator	A person in charge of administration of an application/system or technological layers (operation system, database, application server...)
Employee	Employee of LP or its subsidiary or an external employee (identified by personal ID number)
Application administrator	A person on the part of ICT, who is responsible for operation of the application, operational requirements (application shutdown etc.) and change requests (changes in functions, modifications, application setup) for the application

a)

III Scope

The following standards are mandatory for all equipment and technological solutions operated in the internal environment of LP's computer network, regardless the user.

III.1 If the technology is operated in the partial hosting mode (the entire technology is located in LP a.s. premises but it is separated from the internal environment by firewall and fully administered by the supplier), it is possible to grant an exception from these standards based on agreement).

III.2 The standards do not cover technological solutions operated in full hosting mode (the entire technology located outside LP a.s. internal environment).

III.3 Exceptions are always granted by CEO/ICT based on agreement with other ICT units.

III.4 Certain technical standards are indicated as critical. These cases required, besides CEO/ICT approval, an expressed approval by HM/IL. These standards are marked with *.

III.5 Critical applications include all applications requiring 24x7x365 operation/support with reliability over 99% or recovery time under 30 minutes.

III.6 If the application is located in the Internet area or if it forms a part of the backbone infrastructure, it is always considered as critical.

III.7 For applications located in the Internet area, the acceptance requirements always include documentation of positive results of the penetration tests of the supplied application, carried out by an independent subject (approved by LP). If LP requires so, a revision of the application source code can also be required.

IV Individual standards of IT environment

IV.1 *Servers*

IV.1.1 Operation systems

Type of application/system	Type of OS*	Currently supported OS
Critical applications	UNIX	SUN Sparc Solaris 9.05 or higher
	Linux	Linux (RedHat Enterprise 6.x or higher)
		Linux (distribution Debian 8 or higher)
		Linux (distribution Ubuntu 12.04 or higher)
	Windows	Windows Server 2012 R2 US
	AIX	AIX 6.1 or higher
Other applications/systems	UNIX	SUN Sparc Solaris 9.08 or higher
	Linux	Linux (RedHat Enterprise 6.x or higher)
		Linux (distribution Debian 8 or higher)
		Linux (distribution Ubuntu 12.04 or higher)
	Windows	Windows Server 2012 R2 US
	AIX	AIX 6.1 or higher

IV.1.2 Database engines

Type of application/system	Type of DB*	Currently supported versions
Critical applications	ORACLE	12.1 or higher - Enterprise Edition without extra licensed option packs (Spatial, Partitioning)
	SYBASE	ASE – SYBASE 15
	MS SQLServer	MS SQL Server 2012 SP 2 or higher
	MySQL	5.1 or higher
	MariaDB	10.1 or higher
Other applications/systems	ORACLE	12.1 or higher - Enterprise Edition without extra licensed option packs (Spatial, Partitioning)
	MS SQLServer	MS SQL Server 2012 SP 2 or higher
	MySQL	5.1 or higher
	MariaDB	**10.1 or higher**

IV.1.3 Mandatory setup of DB engine

IV.1.3.1 MS SQLServer

- The application database is preferably located on a shared SQL Server reserved for application databases. Only in case it is not possible to locate the applications on this shared server (for performance, safety or other reasons), a separate SQL Server shall be prepared for the application.
- For the shared MS SQL Server, the following rules apply:
    - Default Collation of the shared database server is "SQL_Latin1_General_CP1_CI_AS". Collation for the application database is set up as needed for given application.
    - Applications/application accounts have dbowner rights for the application database.
    - Applications/application accounts do not have any rights at the SQL Server administration level. (Sysadmin, Securityadmin etc.)
    - Database roles are linked to ActiveDirectory groups

- For application users, both SQL and Domain authentication can be used. For users, only Domain authentication can be used.

IV.1.3.2 ORACLE

- The database server is located in the DB area of the internal network, not allowing direct access of end users to the server.
- Backup is ensured using the RMAN utility.
- The database name can only contain A-Z and 0-9 characters.

IV.1.3.3 MySQL / MariaDB

- End users are not granted direct access to the database server.
- The database name can only contain A-Z and 0-9 characters and "_" (not at the first position).

IV.2 *Communication*

IV.2.1 TCP/IP v4, private address range under LP's control (unless expressly defined otherwise in LP's requirements).

IV.2.2 The network topology and network elements are under the exclusive administration of LP.

IV.2.3 Generally, the network environment is divided into 2 categories:

IV.2.3.1 DMZ

- This area includes servers, which can communicate directly to Internet and provide certain services to clients in the Internet.

IV.2.3.2 Internal

- This area includes servers and devices, which do not have permission to direct access to the Internet and are not accessible for clients in the Internet.

IV.2.3.3 Both environments are protected by firewall gates and, by default, cannot communicate neither to the Internet nor to other DMZ or internal networks.

IV.2.4 Devices located in DMZ cannot initiate communication with devices in the internal environment. If it is necessary to publish any data on the servers in the DMZ environment, it must be loaded from the internal environment so that it is the servers in the internal environment which initiate the transfers. The requirements for exceptions from this rule are conditioned by preceding approval by M/INF or CEO/ICT.

IV.2.4.1 If the servers in DMZ are deployed in a multi-layer architecture, then all the child servers (both application and database servers) must also be located in DMZ environment. This point respects the requirement for prohibited initiation of communication from DMZ to the internal environment.

IV.2.5 Users can only connect to the data network using end devices, doing so only at places intended for this purpose. It is expressly prohibited to connect devices such as routers, switches or wireless access points. The requirements for exceptions from this rule are conditioned by preceding approval by M/INF or CEO/ICT.

IV.3 *Remote access*

IV.3.1 *Remote user access*

IV.3.1.1 For remote access to LP environment, the rules are defined by the VPN Access Rules workflow.

IV.3.2 B2B remote access

IV.3.2.1 B2B remote access is intended for permanent connection between LP's internal environment and the environment of an external company using an IPSec tunnel. This access is intended for application purposes only. This B2B remote access cannot be required for the purposes of remote administration; for this purpose, the User remote access is intended.

IV.3.2.2 Third-party companies with this type of access must guarantee that no other subjects can access the systems in their environment that use this connection, i.e. no shared service is provided.

IV.3.2.3 The parameters of the IPSec tunnels are described in Annex No. 1.

IV.3.2.4 Implementation of B2B remote access is conditioned by preceding approval by M/INF or CEO/ICT.

IV.4 *Messaging Middleware*

IV.4.1 Technology

IBM Websphere Message Queue v 7.X *

IV.4.2 Data layer

For data exchange, the XML format is preferred.

Use of another format requires approval by CEO/ICT.

IV.5 *Application servers*

Currently operated:

Environment	Type of AS	Currently operated AS
UNIX environment	GlassFish	GlassFish 3.x or higher
Windows environment	IIS	IIS 8 or higher

IV.5.1 Application Windows servers are monthly patched using the WSUS service.

IV.5.2 All application Windows servers are protected with the Forefront antivirus system.

IV.5.3 On Windows servers, an SCOM agent is installed for server monitoring.

IV.5.4 For GlassFish, an external balancer is used. Use of HADB **is not** supported.

IV.5.5 Use of AS from the subset WebSphere, Oracle AS and JBoss/Tomcat requires approval by CEO/ICT. Use of AS out of this subset is not acceptable.*

IV.6 *WWW applications*

IV.6.1 LP part:

	WWW server *	Supported versions
All applications	Apache MS IIS GlassFish	2.2 or higher IIS 8 or higher 3.x or higher*

the specific version, ask M/INF. It is acceptable to use PHP v. 5.3 or higher (in internal environment - specific version of supported SW is derived from current versions in the official repositories of the operated OS).

Use of JAVA applets and ActiveX components requires approval by M/INF.

IV.6.2 Client part

- Support of MS IE 11.0 or higher required*
- Support of Firefox browser

IV.7 *E-mail, messaging*

IV.7.1 The internal mail system is based on Microsoft Exchange platform, version 2010, 2013. Support of Exchange Online – Office 365 required

IV.7.1 For access to the e-mail box, the service EWS (Exchange Web Services) is used by default. Use of other protocols - IMAP, POP3 - with approval by CEO/ICT only

IV.7.2 E-mail sending within the application is only possible using TLS and authentication with login/password of the domain user. Use of Open Relay is not supported.

IV.7.3 TypeB messaging is addressable through X400 and MQ.

IV.7.4 If using any cryptographic security tool, it is necessary to obtain approval by CEO/ICT for given technology and designed process.

IV.7.5 By standard, PGP is used for cryptographic security of communication.

IV.8 *Authentication*

IV.8.1 All rules regarding authentication are defined in the directive Identity and Access Administration.

IV.8.2 Active Directory acts as the basic repository. Access to LDAP requires secured connection - use LDAPS protocol.

IV.9 *Windows Server infrastructure environment*

IV.9.1 Active Directory

IV.9.1.1 Domain functional Level of LP domain is set to “Windows Server 2008 R2”

IV.9.1.2 For user authentication in ActiveDirectory, the Kerberos protocol is preferred. Use of LM and NTLM is prohibited. With approval by CEO/ICT, it is also acceptable to use NTLMv2. If Basic authentication is used, the connection must be encrypted.

IV.9.1.3 During routine operation, the application must not require any permissions in Active Directory out of scope of a normal user account.

IV.9.2 Application Windows Servers

IV.9.2.1 The application must not require interactive login to the server for its operation. This means that it must run in “service”, “planned task” etc. mode.

IV.9.2.2 The application account (local server/domain account) must not be used for local login to the server. (Deny logon locally)

IV.9.3 The application must not make any entries in the Registry outside the HKCU structure.

IV.9.4 If there is any connection between application and database, the application must not require installation on the same server as the database.

IV.10 *End stations*

IV.10.1 Common end stations

IV.10.1.1 OS: Windows 7, 8.1, 10 Enterprise 32-bit and 64-bit

IV.10.1.2 Office package: MS Office 2013, 2016, O365 CZ/US *

IV.10.1.3 Users have “User” rights only

IV.10.1.4 The computers are periodically patched using the WSUS service

IV.10.1.5 On the computers, the antivirus system Forefont is installed

IV.10.2 Restrictions for applications/clients

IV.10.2.1 The application must bot use “higher” permissions than “User” for its operation.

IV.10.2.2 The application must be compatible with UAC safety technology.

IV.10.2.3 The application must support so-called “silent installation”.

IV.10.2.4 The application must run on the virtualization platform Microsoft Application Virtualization App-V

IV.10.3 “Dumb” end stations

IV.10.3.1 Operation system: Elux, EluxNG (Linux modifications)

IV.10.3.2 Elux/EluxNG native clients: RDP, Citrix Metaframe, Mozilla, X11, XDCMP, VT320, ANSI terminal, 3250, 3270.

IV.10.3.3 Dell Wyse P20

IV.11 *Terminal access*

IV.11.1 The support includes the Microsoft Remote Desktop Services (RDS) platforms

IV.11.2 By standard, the RDP channel for peripherals (printers, COM ports etc.) is not supported.

IV.12 *Virtualization*

IV.12.1 Server virtualization is ensured by VMWare. Current version: VMWare vSphere 5.5.

IV.12.2 When designing the application architecture, it is possible to use VMware HA technology to ensure high availability of the virtual server. Alternatively, it is possible to use VMware SRM to ensure high availability of the application in case of DataCenter drop-out.

IV.12.3 Virtualization of applications on end stations is ensured by APP-V v5 platform.

IV.13 *Development environment*

IV.13.1 The recommended development platforms include:

IV.13.1.1 Case for analytical work

- Enterprise Architect
- BPA

IV.13.2 Administration of source codes

- As CVS repository, the product Subversion is used

IV.13.3 End stations (PC)

- Delphi XE (if the application is developed in-house or if the source code is handed over to LP)
- C/C++
- C#
- JAVA 8
- .NET 4.0 Framework
- .NET 4.5 Framework or higher

IV.13.4 UNIX servers

- C, C++, JAVA
- JAVA 1.6. EE or higher for application deployed on the application server
- PHP v 5.3 or higher
- Script languages - PERL, Shell etc. - with approval by CEO/ICT only.

IV.13.5 NT servers

- JAVA 8
- C/C++
- .NET 4.0 Framework
- .NET 4.5 Framework or higher
- Visual WebGui

IV.14 *Individual standards for IT environment for applications in DMZ*

For applications operated in DMZ, the following standards apply:

IV.14.1 HW PLATFORM: Intel 64bit

IV.14.2 OS: RedHat Enterprise Linux - x86_64 (release 6.x or higher), Debian 8 or higher, Ubuntu 12.04 or higher

IV.14.3 DB:

- MySQL 5.1 or higher (for so-called non-sensitive data only)
- MariaDB 10.1 (for so-called non-sensitive data only)
- Oracle 12.1 or higher, only in Standard Edition ONE version

IV.14.4 Application server

- GlassFish Server 3.x or higher
- Apache 2.2 or higher
- Tomcat/JBoss

IV.14.5 Script languates

- PHP 5.3 or higher
- PERL 5.10 or higher
- Shell - only with approval by CEO/ICT.

For the specific version, ask M/INF. Version of supported SW is derived from current versions in the official repositories of the operated OS.

V Standards for Cloud and Cloud-operated applications

V.1 Devices located in Cloud cannot communicate directly with devices in the internal environment. If it is necessary to publish any data from the servers in the internal environment, it must be done using the application interface, e.g.

- IBM MQ
- Web services

V.2 The application interface must be located in DMZ.

The requirements for exceptions from this rule are conditioned by preceding approval by M/INF or CEO/ICT.

VI Standards for use of mobile devices for access to applications

This access can be classified by environment as internal and external.

VI.1 *Access from internal environment*

If given devices are connected in the internal network, i.e. they run on MS Windows and are assigned to LP Active Directory, they can access to any internal applications.

VI.2 *Access from trusted external environment*

A trusted external environment is a private secured access, e.g. 3G/4G access with a private operator APN or a wireless network in the airport, secured by authentication and encryption of the transfer channel.

Access to internal applications from this environment are subject to explicit approval by M/INF or CEO/ICT, after consideration of related risks.

VI.3 *Access from non-trusted external environment*

This types of access include access from the Internet (e.g. 3G/4G connection) as well as access through the public wireless network at the airport. The devices connected in this environment can only access applications located in DMZ and are accessible from the Internet.

VII Exceptions from mentioned rules

Any exceptions from the standards described above can only be applied with explicit approval by CEO/ICT.

VIII Related documentation

(1) Directive “Identity and Access Administration”

(2) Directive “Antivirus Protection Rules”

(3) Directive “VPN Access Rules”

(4) Directive “Administration of Firewalls and Network Elements”

(5) Directive “Administration of Encryption Keys and Cryptographic Support of Systems”

IX Annexes

Annex No. 1 – Parameters of B2B IPSec tunnel

Partner info		
Company:		***LP***
Address:		
City:		Prague
Country:		CZE
VPN endpoint		
Supplier:		Juniper
Type:		SRX 1400
Public IP Peer address:		
Mode	Main	
IKE Parameters - Phase 1		
Authentication Mode:	preshared key	
Preshared Key:	via sms	
Authentication Algorithm:	SHA2-256	
Encryption Algorithm:	AES-256-CBC	
Diffie-Hellman Group:	14	
Aggressive mode:	disabled	
Lifetime Measure:	time	
Lifetime (seconds):	28800	
IPSEC Parameters - Phase 2		
Protocol:	ESP	
Authentication Algorithm:	SHA2-256	
Encryption Algorithm:	AES-256-CBC	
Encapsulation Mode:	tunnel	
PFS:	no	
PFS Group:	no	
Lifetime Measure:	time	
Lifetime (seconds):	3600	
Local network		
Test IP for ICMP (ping)		
Technical Contact		
	email: phone: comment:	email: phone: comment:

Annex No. 2 - Data from AODB to be displayed within the System of Annex No. 1 – Technical and Functional Specification of the System

The System is able to receive and display all such data within all outputs.

Data	*Related to:*	*Datatype*	*Notes*
flightId	Departure/Arrival	int	
flightDate	Departure/Arrival	date	in both LT and UTC version
ICAO	Departure/Arrival	varchar(3)	
IATA	Departure/Arrival	varchar(2)	
flightNumber	Departure/Arrival	varchar(9)	
handling	Departure/Arrival	varchar(3)	
deiceHandling	Departure	varchar(3)	
flightCategory	Departure/Arrival	char(1)	
terminal	Departure/Arrival	varchar(3)	
public	Departure/Arrival	int(1)	
bus	Departure/Arrival	int(1)	
arrivalBeltAllocId	Arrival (Belt allocation - multiple per flight)	int	
arrivalBelt	Arrival (Belt allocation - multiple per flight)	varchar(3)	
arrivalBeltState	Arrival (Belt allocation - multiple per flight)	char(1)	
checkinDeskAllocId	Departure (counter allocation - multiple per flight)	int	
checkinDesk	Departure (counter allocation - multiple per flight)	varchar(3)	
checkinDeskState	Departure (counter allocation - multiple per flight)	char(1)	
checkinDeskRemark1	Departure (counter allocation - multiple per flight)	varchar(30)	
checkinDeskRemark2	Departure (counter allocation - multiple per flight)	varchar(30)	
checkinDeskClass	Departure (counter allocation - multiple per flight)	char(1)	
destinationICAO	Departure (multiple per flight)	varchar(3)	
originICAO	Arrival (multiple per flight)	varchar(3)	
firstChin	Departure	varchar(3)	
lastChin	Departure	varchar(3)	
gateAllocId	Departure (gate allocation - multiple per flight)	int	
gate	Departure (gate allocation - multiple per flight)	varchar(3)	
gateState	Departure (gate allocation - multiple per flight)	char(1)	
gateRemark1	Departure (gate allocation - multiple per flight)	varchar(30)	
gateRemark2	Departure (gate allocation - multiple per flight)	varchar(30)	
gateClass	Departure (gate allocation - multiple per flight)	char(1)	
STA	Arrival	time	in both LT and UTC version
ETA	Arrival	time	in both LT and UTC version
ATA	Arrival	time	in both LT and UTC version
hallState	Departure	varchar(3)	
registration	Departure/Arrival	varchar(10)	
scheduledCheckinTime	Departure	time	in both LT and UTC version
STD	Departure	time	in both LT and UTC version
ETD	Departure	time	in both LT and UTC version
ATD	Departure	time	in both LT and UTC version
arr_dep	Departure/Arrival	char(1)	

stand	Departure/Arrival	varchar(3)	
pax	Departure/Arrival	int(3)	
order	Departure/Arrival	int(2)	
primaryFlightID	Departure/Arrival	int	
remarkCode	Departure/Arrival	int	
remarkSupplement	Departure/Arrival	varchar(10)	
addRemarkCode	Departure	int	
addRemarkSupplement	Departure	varchar(10)	
planeType	Departure/Arrival	varchar(5)	
firstBag	Arrival	time	in both LT and UTC version
lastBag	Arrival	time	in both LT and UTC version
cdm_EOBT	Departure	time	in both LT and UTC version
cdm_AOBT	Departure	time	in both LT and UTC version
cdm_CTOT	Departure	time	in both LT and UTC version
cdm_TOBT	Departure	time	in both LT and UTC version
cdm_TSAT	Departure	time	in both LT and UTC version
cdm_TTOT	Departure	time	in both LT and UTC version
distand	Departure	time	in both LT and UTC version
cdm_EDIT	Departure	time	in both LT and UTC version
cdm_ADIS	Departure	time	in both LT and UTC version
cdm_ADIF	Departure	time	in both LT and UTC version
cdm_EDIS	Departure	time	in both LT and UTC version
cdm_EDIF	Departure	time	in both LT and UTC version
cdm_ERDL	Departure	time	in both LT and UTC version
flightStatus	Departure	char(1)	
callsign	Departure	varchar(8)	
runway	Departure	varchar(3)	
firstDest	Departure	varchar(3)	
firstOrigin	Arrival	varchar(3)	
rotationFlightID	Departure/Arrival	int	

Annex No. 3 – Specifications of XML reports of Annex No. 1 – Technical and Functional Specification of the System

1. Report Header

Every report contains standard XML header
<?xml version="1.0">
, using UTF-8 encoding.

2. Tags

Every report's body is marked by tag:
<Picture_YYMMDDHHMM></Picture_YYMMDDHHMM >
where YYMMDDHHMM is timestamp.

2.1. Record

Every record (every departure/arrival) is inside tag:
<Content></Content>

2.2. Data

Every record contains columns in following format:
<ColumnName>Value</ColumnName>
Name of every column can be defined by administrator. Every report can be defined with different column names.

3. Notes

Maximum records in every report can be defined. Reports are generated separately for departures and arrivals (two files).

4. Report sample

```
<?xml version="1.0" ?>
  <Picture_1711141200>
  <Content>
   <FLIGHTID>311542830</FLIGHTID>
   <DATE>26.10.2010</DATE>
   <TIME>16:55</TIME>
   <ICAO>CSA</ICAO>
   <ICAOAIR>CZECH AIRLINES</ICAOAIR>
   <IATA>OK</IATA>
   <NUM>0778</NUM>
   <FLGTNUM>OK 0778</FLGTNUM>
   <S1>WAW</S1>
   <S1CIT>WARSAW</S1CIT>
   <HAL>T2</HAL>
  </Content>
  <Content>
   <FLIGHTID>259139561</FLIGHTID>
   <DATE>26.10.2010</DATE>
   <TIME>12:10</TIME>
   <ICAO>AZA</ICAO>
   <ICAOAIR>ALITALIA - COMPAGNIA AEREA ITA</ICAOAIR>
   <IATA>AZ</IATA>
   <NUM>7517</NUM>
   <FLGTNUM>AZ 7517</FLGTNUM>
   <S1>VCE</S1>
   <S1CIT>VENICE/MARCO POLO</S1CIT>
   <HAL>T2</HAL>
```

<CHIN_F>**220**</CHIN_F>
<CHIN_L>**225**</CHIN_L>
<PARID>**311522420**</PARID>
<REMARK>**CHECK-IN**</REMARK>
</Content>
</Picture_1711141200>

Annex No. 2 – Detailed Calculation of the Price of the Work

Flight information Display System						
Item name	**Product type**	**Product/Support specification**	**MU**	**Number of MU**	**Price in CZK without VAT per MU**	**Total price in CZK without VAT**
Price for implementation - mentionet in contrct for Work						
Software license	License/Software	Server license	units	1	6 000 000,00 CZK	6 000 000,00 CZK
Controller license	License/Software	License up to 1100 controlers	units	1100	7 500,00 CZK	8 250 000,00 CZK
Implementation	works		units	1	14 000 000,00 CZK	14 000 000,00 CZK
Training	works		units	1	750 000,00 CZK	750 000,00 CZK
Post-implementation adjustments	works		manday	25	25 000,00 CZK	625 000,00 CZK
Other licenses	License/Software	Other required licenses	units		- CZK	- CZK
					TOTAL price for implementation	**29 625 000,00 CZK**
Database						
Database license			units	1	- CZK	- CZK
Database maintenance			month	96	- CZK	- CZK
					TOTAL price for database	**- CZK**
Controllers						
Controllerswith OS & all required licenses			unit	700	18 500,00 CZK	12 950 000,00 CZK
Existing controllers AMD	6.2.1. AMD G-T40E 1GHZ 2 CORES, 4GB RAM, 16GB HD, RADEON HD6250	Tenderer will determine how many controller can be used, this amount will be deducted	units available	340	units to be used	340
Existing controllers Intel	INTEL CELERON J1900 1,99GHz 4 cores, 4GB RAM, 32GB HD, INTEL ATOM E3800	Tenderer will determine how many controller can be used, this amount will be deducted	units available	60	units to be used	60
					Total prices for Controllers	12 950 000,00 CZK
System Service Support fee						
System service support			month	96	90 000,00 CZK	8 640 000,00 CZK
Price for system adjustments						
Additional Controllers with OS & all required licenses			controller	400	18 500,00 CZK	7 400 000,00 CZK
License extension			license per controller	400	7 500,00 CZK	3 000 000,00 CZK
Man-day rate	works		manday	150	25 000,00 CZK	3 750 000,00 CZK
License for another additional hardware		according to sec 6.3 of annex E	license per unit	10	20 000,00 CZK	200 000,00 CZK
TOTAL TENDER PRICE IN CZK WITHOUT VAT						**65 565 000,00 CZK**

Annex No. 3 - Contacts

Mailing address:

(a) Address for delivery to the Customer:

Letiště Praha, a. s.
Jana Kašpara č.p. 1069/1, Prague 6, 160 08
Czech Republic

Attn. Company Executive Manager of ICT

(b) Address for delivery to the Contractor:

Simpleway Europe, a.s.
Na Okraji 335/42, Prague 6, 162 00
Czech Republic

Responsible persons:

The representative authorised to represent **the Contractor's party in contractual matters** related to performance hereof will be:

[redacted]
Tel: [redacted]
Email: [redacted]

The representative authorised to represent **the Contractor's party in technical matters** related to performance hereof will be:

[redacted]
Tel: [redacted]
Email: [redacted]

The representative authorised to represent **the Customer's party in technical matters** related to performance hereof will be:

[redacted]
Tel: [redacted]
Email: [redacted]

The representative authorised to represent **the Customer's party in contractual matters** related to performance hereof will be:

[redacted]
Tel: [redacted]
Email: [redacted]

Annex No. 4 - Implementation Time Schedule

We are proposing the following implementation schedule:

Milestone	Relative Time
Contracts and Agreements signed and official project start	D
Final requirements clarification	D + 1 month
Final solution design proposed to customer for approval	D + 1.5 months
Simpleway software customization / integration	D + 4 months
Software / Hardware delivery on TEST environment	D + 4.5 months
Software / Hardware delivery of 100 screens to production	D + 5 months
Software / Hardware delivery of 300 screens to production	D + 6 months
Software / Hardware delivery of remaining screens to production	D + 7 months
Documentation handover, official project closure, training	D + 8 months

*D is the date of when contract is signed.

Annex No. 5 – Current Hardware description

Fan less MiniPC (24cm x 21cm x 5cm) with following specification:

(a) Type 1 (340 pieces):

Motherboard: AAEON GENE-HD05

CPU: AMD G-T40E 1GHz 2 cores

RAM:4GB

HD: 16GB CFast Card 3ME Series

GA: Radeon HD6250

(b) Type 2 (60 pieces):

Motherboard: Asrock D33C20

CPU: INTEL CELERON J1900 1,99GHz 4 cores

RAM:4GB

HD: 32GB minSata

GA: Intel Atom E3800

Annex No. 6 –Hardware description

Fan-less graphic controller (25 x 22 x 7cm) with the following technical specifications:

- CPU: minimum 1.1GHz+ dual core
- 4 USB 2.0 ports, LAN, WiFi 802.11ac + Bluetooth 4.2
- RAM: 4GB+
- HD: SSD 32GB+
- GA: minimum Intel HD500+

I/O specification:

HDMI, VGA, 3,5mm jack audio, 2x USB, 100MB/s LAN

The supply of each graphic controller will include 1 power cable 1.5m, 1 power adapter, 1x HDMI cable 1.5m, 1x Patch Cord UTP CAT5E 1m.

Annex No. 7 – Cyber Security requirements

SECURITY REQUIREMENTS IN CONTRACTUAL RELATIONS

Introduction

The purpose of the present document is to define binding security requirements for Providers providing services and/or products for the Purchaser (exclusively or as part of providing other services) consisting in the development, implementation and/or servicing of software or hardware, (hereinafter referred to as "**SW**" or "**HW**"), and/or who, in connection with the provision of services and/or products for the Purchaser, access the information and communication system of the Purchaser (hereinafter also referred to as the "**ICT System**"), and/or who, in connection with the provision of services and/or products for the Purchaser, process and/or transmit and/or store and/or archive any data and information of the Purchaser and/or its customers (hereinafter also referred to as the "**Security Requirements**"). The purpose of the present document is also to define the requirements for the suppliers in compliance with the valid legislation, in particular pursuant to Section 5 paragraph 2e) of Act No. 181/2014 Sb., on cyber security and on amendments to relating acts (the Cyber Security Act) and Section 7 of Decree No. 316/2014 Sb., on security measures, cyber security incidents, reactive measures and on establishing the requirements for filings in cyber security (the Cyber Security Decree), taking account of other applicable valid legislation.

General Requirements

In connection with the provision of services and/or products for the Purchaser, the Provider shall fulfil the following obligations:

a) In case the Provider provides services and/or products through a subcontractor, the Provider shall cause the Security Requirements to be met by incorporating them in contractual relations with its subcontractors; and the Provider shall prove such fact at the Purchaser's request by presenting the relevant contractual documentation entered into with such subcontractor, or by producing a sworn declaration about proper discharge of such obligation;

b) Unless otherwise stated in the agreement of the parties, the Provider shall appoint a contact person within 3 days after the signing of the agreement who shall be responsible for the compliance with the Security requirements and communication between the parties (hereinafter also referred to as the "**Contact Person**");

c) Compliance with the applicable provisions of the Purchaser's security policies, methodologies and procedures, and/or valid management documentation, or any part thereof, provided such documents or parts thereof were made available to the Provider.

SW Development Security Requirements

3.1. In connection with the provision of services and/or products for the Purchaser, the Provider shall ensure:

a) Assistance with security testing during the SW development phase or after the SW acceptance as required by the Purchaser, each within deadlines fixed by the Purchaser or without undue delay;

b) Delivery of system and operational security documents no later than on the SW acceptance date in the manner set forth in the agreement, at least in the scope set forth in cl. 4 hereof;

c) That the services provided and/or products delivered shall contain only such parts which are actually necessary for the proper operation of the SW and/or which are expressly specified in the agreement (the SW may not contain any unnecessary components, any software samples etc.);

d) That if the services provided and/or products delivered include any installation of any third-party's operating system and/or SW, such installation shall involve only versions required by the Purchaser, incl. the latest security patches;

e) That no confidential information[1] provided to the Provider in connection with the provision of services and/or delivery of products by the Provider shall be stored without encryption and the same shall be protected against unauthorized use unless otherwise agreed by the parties on a case-by-case basis;

f) That any SW installation and/or its upgrade shall be made in compliance with the Purchaser's security standards (applicable to the Providers who were acquainted with such security standards) and in compliance with the Purchaser's technical and process regulations which (in accordance with the generally acceptable standards, such as CIS Benchmarks, NIST etc.) provide for the configuration of applications and systems (hereinafter referred to as the "**Hardening Security Policy**");

g) That the ICT system production environment shall contain only complied or executable code and other data necessary for the operation of the ICT system;

h) That before the start of SW in the ICT system production environment, the Provider shall check the compliance of the SW with the Security Requirements of the Hardening Security Policy and in case of any discrepancy, the Provider shall ensure the compliance of the SW with the Security Requirements of the Hardening Security Policy without any undue delay (applicable to the Providers who were acquainted with such security standards);

i) That it will check the integrity of the source code and if requested by the Purchaser, the Provider shall give the source code to the Purchaser in a secure form ensuring the integrity of the source code, provided that the Provider keeps records of and store source codes of the applications, on a regular basis, even if source codes are given to the Purchaser; and the Provider undertakes to develop the SW in such a manner so as:

- the source code of programmes developed by the Provider will be subject to version control;
- the source code of programmes is backed up and stored outside the production environment, and workflow has been set up to build the system from the source code;
- configuration changes are made in line with the Purchaser's change control;
- configuration files are backed up on a regular basis;
- the Provider will record any change of configuration;

System and Operations Security Documents Requirements

Security documents about security settings, functions and mechanisms pre shall constitute an integral part of the services and/or products provided. In connection with the provision of services and/or products for the Purchaser, the Provider undertakes to deliver security documents to the Purchaser at least in the scope mentioned below:

- Recovery strategy
- As-built documentation
- Description of authorization concept and authorizations
- Backup and archiving processes
- Installation and configuration processes

[1] Confidential Information, as used in the present Annex, shall include (without limitation) certificate identification details, passwords, configuration files, system programmes, critical libraries, recovery procedures etc.

- Security settings

Physical Protection and Environment Security

a) The Provider undertakes to adhere to the Operating Rules of the buildings (security measures) and used areas, in particular in the area of physical protection of security zones where ICT components and/or data media are located (hereinafter also referred to as the "**Workplace**").
b) The Provider undertakes not to leave any installation, backup or archive media or documentation for the ICT system which is the subject-matter of the present Agreement unattended and freely available anywhere in the Workplace.

Access Control

a) The Provider acknowledges that the access to the ICT system may be granted only to the physical identity of the Provider's / Provider's subcontractor's employee entered in the Identity Registry kept by the Purchaser following a request for access by the Provider.
b) The Provider acknowledges that its employee must give a demonstrable consent with the processing of their personal data necessary for opening an access; otherwise the Purchaser is not obliged to grant such employee an access to the ICT system. Provider's employees who were granted (physical, logical) access to the ICT system must give a demonstrable consent with the processing of their personal data which are processed during the evaluation of data about the movement and activities carried out in the Purchaser's premises (such as Security Incident and Event Monitoring), where such consent must be given by a written consent or a digital consent in the form of an email, unless otherwise agreed by the parties.
c) The Provider acknowledges that access privileges to Provider's employees must be limited to an as-needed basis and such privileges are not granted automatically to all its employees.
d) The Provider undertakes to ensure that access granted to one employee may not be shared with another employee of the Purchaser or the Purchaser's subcontractor.
e) The Provider undertakes to ensure that the access to the ICT system via a mobile application shall always be made via a secure VPN connection.
f) The Provider undertakes to seek approval of connection from the Purchaser's Contact Person prior to connecting any terminal equipment, mobile terminal equipment or active network components, such as network switches, WiFi access points, routers or hubs, to a computer network.
g) The Provider undertakes to deactivate any unused terminals of the network or unused ports of any active network component.
h) The Provider shall not install or use the following types of instruments in the Purchaser's environment:
    - Keylogger
    - Sniffer
    - Vulnerability scanner and Port scanner
    - Backdoor, rootkit and Trojan Horse or another form of malware.
i) The Provider undertakes to ensure that all the ICT systems of the Provider connecting to the Purchaser's network infrastructure are protected against malware at least for the duration of the connection of such Provider's system to the Purchaser's network infrastructure.
j) The Provider undertakes not to develop, compile or distribute a program code in any part of the ICT system which intends to illegally control, disrupt or discredit the ICT system or to illegally obtain data and information.

k) The Provider undertakes to ensure that persons involved in providing services or products to the Purchaser in the Purchaser's infrastructure do not:
    - visit websites with ethically inappropriate content[2];
    - store and/or share data and information of ethically inappropriate content contrary to accepted principles of morality or damaging the Purchaser's reputation;
    - download, share, store, archive and/or install data and executable files contrary to the license terms and conditions or the Copyright Act;
    - store and/or share the Purchaser's data and information in prohibited data stores or media (a list of approved data stores and media is within the records of the Purchaser's assets);
    - send chain emails.

l) The Provider undertakes to ensure that persons involved in providing services or products to the Purchaser who access the Purchaser's internal network and/or the Purchaser's ICT system respect and comply with the following restrictions:
    - Equipment, such as laptop/computer, must:
        - apply security patches (of the operating system, internet browser and Java)
        - have antivirus software, which is installed, run and updated;

m) The Provider undertakes to ensure that persons involved in the provision of services and/or products to the Purchaser who access the Purchaser's internal system and/or the ICT system protect authentication means and data for the Purchaser's ICT systems. The Provider acknowledges that in case of any unsuccessful user authentication attempt, the relating user account may be blocked and handled as a security incident pursuant to the applicable management documentation, and that security incident handling procedures may be applied (such as immediate termination of an access to information assets for natural persons of an external entity). The Provider acknowledges that the procedure of handling a security incident or another consequence of breaching the Security Requirements shall not be assessed as a circumstance excluding the Provider's liability for a delay in proper and timely performance of the subject-matter of the agreement and shall not constitute grounds for any compensation of any damage to the Provider or another person by the Purchaser.

Monitoring

a) The Provider acknowledges that any and all Provider's activities carried out in and/or services provided and/or products delivered for the Purchaser's system environment shall be monitored and evaluated by the Purchaser on a continuous and regular basis in accordance with the contents of the agreement and internal documents of the Purchaser with which the Provider was acquainted.

b) The Provider undertakes to present the records/logs containing the results of the monitoring, successful and unsuccessful logins to the ICT system, as well as user administration records to the Purchaser at its request without undue delay throughout the term of the agreement and even after the termination thereof.

Acceptance

a) The Provider acknowledges that any failure to comply with the Security Requirements, incl. the requirement for the delivery of complete system and operational documentation, shall constitute a

[2] Data and information containing elements of extremism, terrorism, pornography and/or incitement to hatred or social prejudice relating to a social group identified on the basis of a race, religion or faith, gender, sexual orientation, nationality and ethnicity or another difference.

defect preventing the acceptance of the subject-matter of the agreement (a Category A defect) and the Purchaser is not obliged to accept such defective services and/or products unless and until the defect is rectified.

b) The Provider shall be responsible for the fact that the ICT systems administered by the Provider contain the latest applicable security updates (patches)[3].

Information Exchange

a) If the subject-matter of the agreement involves any information exchange between the parties, the parties must enter into an Information Security Agreement with respect to any exchange, storing, archiving of the information and the termination of the agreement.
b) The Provider undertakes to ensure security of any and all data and information transmission in terms of security classification, i.e. requirements for data/information confidentiality, integrity and availability.
c) The Provider undertakes to ensure that online transactions made using web technologies are protected with SSL certificates.

Security Incident Handling[4]

In connection with the provision of services and/or products for the Purchaser, the Provider shall:

a) Report any Security Incident through the Purchaser's Contact Person specified in the Agreement without any delay;
b) In case of any occurrence, handling and evaluation of any Security Event and/or in case of any suspected Security Incident, the Provider shall provide assistance requested by the Purchaser (e.g.: logs and identification data (such as the IP address, MAC address, HW type, serial number, or IMEI) of the terminal equipment or mobile terminal equipment of the Provider's employee or the Subcontractor's employee participating in the provision of the services and/or products in order to analyze the content, and/or to take any measures requested by the Purchaser without any undue delay).
c) Make an analysis of the Security Incident causes and propose measures aiming to avoid repetition provided the Provider caused the Security Incident or participated in the Security Incident.

[3] Software upgrade to a higher development version.

[4] The terms Security Incident and Security Event are equivalent to the terms "Cyber Security Event / Cyber Security Incident defined in Act No.181/2014 Sb. on cyber security. For the purposes of the present Document, the terms shall have the following meanings:

"Security Event": any breach of security policy or failure of security measures. This may also involve another situation which has yet not occurred but may be significant in terms of security. It may cause or have an effect on the occurrence of the Security Incident.

"Security Incident": one or multiple undesired or unexpected Security Events which are highly likely to compromise processes/activities of the Purchaser and to pose a threat to information security.