Customer Agreement reference number:	**Supplier Agreement reference number:**
0227007385	

Agreement on provision of airport passenger processing system CUPPS/CUSS (the "**Agreement**"):

Letiště Praha, a. s.
Registered office: Praha 6, K letišti 1019/6, Post Code 161 00,
Incorporated in the Companies Register kept by the Municipal Court in Prague, Section B, Insert 14003,
Company ID no.: 282 44 532,
Tax ID: CZ699003361,
Bank connection: UniCredit Bank Czech Republic and Slovakia, a.s.,
Account number (CZK): 801812025/2700,

(hereinafter referred to as the "**Customer**")

and

Supplier's business name: SITA B.V.
Registered office: Heathrowstaat 10, 1043 CH, Amsterdam, The Kingdom of the Netherlands, Incorporated under laws of the Netherlands with registration number 34123443 and with its branch registered in Czech Republic as SITA B.V. – incorporated in the Commercial Register maintained by the Municipal Court in Prague, Part A, entry 43589, with a registered branch address of: V Parku 2336/22, 148 00 Prague 4, Czech Republic,
Incorporated in
Company ID no.: 70899061
Tax ID: CZ70899061
Bank connection: MUFG Bank (Europe) N.V. Prague Branch
Account number (CZK): 303327/2020

(hereinafter referred to as the "**Supplier**")

The Customer and the Supplier are hereinafter referred to jointly as "**Parties**" or individually as the "**Party**".

Preamble

Having regard to the fact that:

(A) The Supplier wishes to provide to the Customer services provision of airport passenger processing system CUPPS/CUSS Services as specified and defined below in this Agreement, and

(B) the Customer wishes to receive the Services from the Supplier, and

(C) on the basis of the results of the procurement procedure under Act no. 134/2016 Coll., on Public Procurement, as amended, the subject-matter of which was the award of a public Agreement titled The Provision of CUPPS/CUSS Systems for Prague Airport published in the Public Procurement Bulletin on 22.11.2019 under reg. no. Z20119-041989 (hereinafter referred to as the "**Tender**") the Customer has decided that the most suitable bid is the one submitted by the Supplier;

(D) The Customer represents and warrants that the System defined in this subject-matter of the Agreement shall be a part of the Prague Airport Basic Information System (hereinafter referred to as the "**PA BIS**") which was determined to be the basic service system in compliance with Act No. 181/2014 Sb., on cyber security and on amendments to relating acts (the Cyber Security Act), as amended, (hereinafter referred to as the "**Act**);

(E) The Customer considers the Supplier of the System defined in this subject-matter of the Agreement to be an important supplier in compliance with Regulation No. 82/2018 Sb., on security measures, cybernetic security incidents, reactive measures, cyber security reporting requirements and data disposal (hereinafter referred to as the "**Regulation**").

the Parties have agreed in compliance with the applicable provisions of Act no. 89/2012 Coll., Civil Code, as validly and effectively amended, as follows:

I. DEFINITIONS AND INTERPRETATIONS

1. The below-given terms used herein have the meaning defined in this clause 1.1 and are always capitalized in the text of the Agreement:

1.1 "**AODB**" means Airport Operation Database.

1.2 "**Authorized Person**" means any employee of the Customer and any employee or worker of any handling company, airline or any other entity who is entitled to work with End User Workplace on Prague Airport based on respective Agreement between the Customer and such entity.

1.3 "**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.

1.4 "**Category A System Error**" means the most severe Error, such as when

the System or *any* of its essential parts are absolutely non-functional or prevent usage of the System as a whole, or

1.4.1 the System or any of its parts features such non-standard behavior, which materially complicates usage of multiple Customer or airlines, interconnected with the system,

1.4.2 and an acceptable alternative or bypass previously agreed with the Customer is unavailable; or

1.4.3 the System or passenger processing core functionality in the System is down, corrupted or severely degraded (i.e. inoperable) in service, preventing the regular usage of the System and impacting a significant number of workstations and CUSS kiosks, and

1.4.4 no backup or workaround is available at the same time when 1.4.1, 1.4.2, or 1.4.3 is happening.

1.5 "**Category B System Error**" means the Error, such as when

1.5.1 the use or functionality of the System or any of its parts is limited by the Defect or Error, or

1.5.2 it is not possible to use a System functionality, or

1.5.3 data and/or work executed by a user is lost in consequence of such Error; or

1.5.4 the System or passenger processing core functionality in the System is down, corrupted or severely degraded (i.e. inoperable) in service, limiting the regular usage of the System and impacting over fifty percent (50%) of workstations and CUSS kiosks, and

1.5.5 a backup, workaround or a by-pass is available and implemented at the same time when 1.5.1, 1.5.2, 1.5.3, or 1.5.4 is happening; or

1.5.6 a single airline application can’t be used and no back up is available.

1.6 “**Category C System Error**” means the Error which

1.6.1 does not prevent proper usage or functionality of the System or has a minimal impact on it, and

1.6.2 has a minimal impact on the use of the System as a whole; and

1.6.3 the System or passenger processing core functionality is degraded; and

1.6.4 a backup is available, or a by-pass is installed with acceptable quality of service and Supplier resources are scheduled as available.

1.7 “**Category D System Error**” means an Error which Customer did not classify as Category A System Error, Category B System Error or Category C System Error and which the System or passenger processing core functionality in the System is insignificantly degraded and a system, an application or functionality is up and running, backup is available, and no need for a by-pass.

1.8 “**Category A Defect**” means the most severe Defect, such as when

1.8.1 the Work, Ordered Work or any of its essential parts are absolutely non-functional or prevent usage of the Work, Ordered Work or System as a whole, or

1.8.2 the Work, Ordered Work or any of its parts features such non-standard behavior, which materially complicates usage of other operating systems of the Customer or airlines, interconnected with the System,

1.8.3 and an acceptable alternative or bypass previously agreed with the Customer is unavailable.

1.9 “**Category B Defect**” means the Defect, such as when

1.9.1 the use or functionality of the Work, Ordered Work or System or any of its parts is limited by the Defect, or

1.9.2 it is not possible to use a System functionality, or

1.9.3 data and/or work executed by a user is lost in consequence of such Defect.

1.10 “**Category C Defect**” means the Defect which

1.10.1 does not prevent proper usage or functionality of the Work, Ordered Work or System or has a minimal impact on it, and

1.10.2 has a minimal impact on the use of the Work, Ordered Work or System as a whole.

1.11 “**Civil Code**” means Act. No. 89/2012 Coll., as amended.

1.12 “**Confidential Information**” has a meaning as set forth in art. XIII hereof.

1.13 "**Copyright Act**" means Act No. 121/2000 Coll., on copyright, on rights related to the copyright, and on amendment to some acts, as amended and supplemented, or any other legal regulation partly or entirely replacing the earlier.

1.14 “**Copyright Work**” means any output of the Supplier's activity arisen during performance of the Adjustment pursuant to this Agreement, which fulfils the elements of the work protected according to the provisions of Section 2 of the Copyright Act.

1.15 "**CUPPS/CUSS System**" (Common User Passenger Processing System)/(Common Use Self Service) means an Information System certified by IATA and used as a middleware for passenger check-in systems at airports, including CUSS Kiosks. Technical requirements and specification of the CUPPS/CUSS System are available in Annex No. 2 and further in the Documentation.

1.16 "**Defect**" means non-compliance between the Work or Ordered Work and the specifications in the Agreement or in respective Offer, or reduced functionality or usability of the Work or Ordered Work or any of its parts for the purpose intended by the Agreement or the respective Offer.

1.17 "**Documentation**" means (i) user manuals, (ii) administrator(s) manuals, (iii) network and System architecture scheme, and (iv) other official documentation provided by Supplier providing detailed description of the functionality, operating characteristics, and configuration of the Information System. The Documentation will be in Czech or English language.

1.18 "**End User Workplace**" or "**EUW**" means workplace or station consisting usually of PC, printer and other peripherals created by the Supplier for the Customer pursuant to the terms of this Agreement and as specified in Annex No 2.

1.19 "**Error**" means (i) defects in title of the System and/or (ii) a conflict between the real properties of the System and the properties which are set in the Agreement for Work or the Documents or this Agreement, or (iii) any deviation of the System from standard properties defined in the Agreement for Work or in the Documents or in this Agreement which may have an adverse impact on its activities or functionality.

1.20 "**EUW Error**" means the most severe Error of particular EUW, such as when

1.20.1 the Hardware of particular EUW or any part thereof has defects in title, or

1.20.2 the Hardware of particular EUW or any substantial part thereof is completely dysfunctional or excludes the use of the particular EUW as a whole, or

1.20.3 the use or the functionality of the Hardware of particular EUW, or any part thereof, is limited by the Error, or

1.20.4 any of the functions of the particular EUW cannot be used, or

1.20.5 data and/or work executed by a user is lost in consequence of such Error.

1.21 **"Extended Term"** has the meaning set forth in article 11.

1.22 "**Handover**" means the day when the Parties sign the Acceptance Certificate.

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

1.24 "**Hardware**" means hardware equipment which forms part of the subject of performance hereunder. Specification of the Hardware is available in Annex No. 2.

1.25 "**IATA**" means International Air Transport Association

1.26 "**Implementation**" means installation of the CUPPS/CUSS core System at the Place of Performance and putting it into full operation, including its adaptation to the specific needs of the Customer, as agreed between the Parties, in particular setting-up of Customer parameters.

1.27 **"Initial Term"** has the meaning set forth in article 11.

1.28 “**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 Agreement.

1.29 "**Integration**" means material and functional interconnection of the CUPPS/CUSS System with another element and/or software and/or hardware equipment of the Customer.

1.30 "**Installation**" means

1.30.1 in case of Hardware, execution of all activities necessary for commissioning of such Hardware comprising among others their connection to electricity at the place specified by the Customer and confirmed by the Supplier and interconnection of such Hardware with other Hardware of the CUPPS/CUSS System,

1.30.2 in case of software, and operating systems execution of all activities necessary for their commissioning on the platform stipulated by the Customer.

1.31 “**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.

1.32 “**Invoice**” means a tax document issued by the Supplier the essential elements of which are set forth in the Act No. 235/2004 Coll., on Value Added Tax, as amended.

1.33 "**License**" means a non-exclusive authorization to exercise the right to use the System within the scope specified in Article VI. hereof.

1.34 “**Normal Operation**” means the use of the System and the Ordered Work by the Customer when the System and/or the Ordered Work does not show any Errors or Defects and are in accordance with this Agreement.

1.35 “**Ongoing Information Period**” means a frequency of providing ongoing information about removal of Errors which must be delivered by the Supplier to the Customer.

1.36 “**Ordered Work**” means the work that will be ordered and specified in the respective offer made by Supplier as further detailed in article IX. Adaptations.

1.37 “**Penetration Test**“ means a special method of verification whether the System, after having been modified in the form of performance of the Ordered Work (if applicable), 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). Penetration Tests on the System may only be performed by the Customer on prior written notice and any Penetration Tests performed by the Customer will be subject to the terms of the Supplier. In the event that the Penetration Test was performed by a certification authority (e.g. Certified Ethical Hacker) of Supplier or of Customer and the outputs of such a Penetration Test are not older than twelve (12) months, the result of such a Penetration Test may be accepted by the Customer instead of performing a Penetration Test under this Agreement.

1.38 “**Pilot Operation**” means a period after successful completion of Verification Operation during which all Hardware will be installed and during which the properties of the System are verified and functionality of the System is observed in full operation. The Pilot Operation starts after Installation of the first EUW according to EUW Installation Schedule, unless otherwise agreed by the Parties and ends fourteen (14) Days after Installation of the last EUW according to EUW Installation Schedule.

1.39 “**Place of Performance**” means the area of Václav Havel Prague International Airport.

1.40 "**Production AODB**” means AODB for the exchange and processing of up-to-date operational AODB data.

1.41 “**Reduced Operation”** means a period of time, beginning the 1st day of a calendar month following a month, when the total actual number of passengers boarded within the System within that month didn’t exceed 50,000 passengers (“**The Exceeded Month**”) and ending the 1st day of a calendar month following a month, when the total actual number of passengers boarded within the System within that month exceeded 50,000 passengers and such month consecutively follows The Exceeded Month.

1.42 “**Report**” means a report made by the Customer by a telephone, email or any other agreed way to the Supplier's Support Centre regarding the existence of a Defect or an Error.

1.43 “**Response Time**” means a time period during which the Supplier is obliged to inform the Customer using a telephone line +420 220 113 000 (or another number notified for this purpose by the Customer) and using an electronic mail at the address helpdesk@prg.aero (or another email notified for this purpose by the Customer) of the manner in which the reported Error will be removed and by which Supplier's employees.

1.44 “**Service Period**” means 24 hours, 7 days a week.

1.45 "**Services**" means a group of activities specifically defined in Sections 2.1 – 2.4 hereof.

1.46 “**Service Time**" means time between 4:00 a.m. and 10:00 p.m. local time. Service Time may be updated based on mutual agreement between the Customer and the Supplier during a time of Reduced Operation according to actual conditions.

1.47 “**Service Window**" means time of a planned System outage for performing System updates or patches. It must be agreed with the Customer at least 48 hours in advance.

1.48 "**Support**" means part of the Service specified in more detail in Article No. VII of the Agreement.

1.49 “**Support Centre**” means the Supplier's Support Centre located (including personnel and technical staff) in the Place of Performance, serving as the single point of contact provided by the Supplier for the Customer´s phone, e-mail or other types of Reports of CUPPS/CUSS System´s Defects and Errors available on tel.: [redacted]

1.50 “**System**” means a functional structure consisting of the CUPPS/CUSS System and the Hardware.

1.51 "**System Availability**" means the time for which an Error is not reported for the CUPPS/CUSS System.

1.52 “**Time for Error Removal**” means a time period set forth obligatorily in this Agreement during which the Supplier is obliged to remove the reported Error.

1.53 “**Upgrade**” means providing new versions of the System, namely with an extended or corrected functionality which includes the Installation.

1.54 “**Update**” means providing updates of the System as a part of one version of the System (e.g. 1.1, 1.2 etc., including removal of errors and upgrades) which includes the Installation.

1.55 “**Verification Operation**” means a period of maximum two (2) months after Installation, Integration and Implementation of the CUPPS/CUSS core System and at least one (1) dedicated End User Workplace and at least one (1) CUSS kiosk, during which the properties of the System with Hardware will be verified and functionality of the System and individual airline applications listed in Annex No.7 will be tested. Verification Operation will run simultaneously and shall not interfere with current system operation. Part of the Verification operation will be also testing of compliance with the CIS hardening politics, as stated in Annex No. 2.

Additional expressions may be defined directly in the text of the Agreement, in which case the definition is in bold letters and introduced by words “hereinafter referred to as” and upon each next occurrence in the text of the Agreement the expression is written with capital initial letters.

Expressions in singular include the plural as well and vice versa, expressions referring to persons include both natural as well as legal persons.

II. SUBJECT-MATTER OF AGREEMENT

2. Under the terms and conditions agreed below the Supplier hereby undertakes to provide the Customer the following Services:

2.1 deliver the System to the Customer and perform its Installation, Integration and Implementation in the Customer’s environment the (hereinafter referred to as “**Work**”). The Supplier will begin with delivery of the Work under this Article 2.1. one (1) month from the date of the signature of the Agreement by both Parties, at the latest.

2.2 enable the use of the System to the Customer and Authorized Persons, perform local maintenance and remote management of installed Hardware,

2.3 provide the Support within the scope pursuant to Art. VII. of this Agreement,

2.4 provide Licenses for the CUPPS/CUSS System usage,

2.4.1 the Supplier will begin with delivery of Work under the Article 2.1 herein one month from the date of Agreement signature by both parties at the latest. In case that this Agreement is not signed until 15 September 2020, the deadline for implementation shall be prolonged accordingly.

2.4.2 The Customer undertakes to pay to the Supplier for the provided Services a price under the terms and conditions agreed in Article X. hereof.

2.5 Intellectual Property Rights within the Service are either the property of Supplier or the Supplier is entitled to them and other than as expressly provided in this Agreement, this Agreement does not convey to Customer any right, title or interest in them.

III. TIME AND DELIVERY PLACE

3. The Supplier will successfully finish the Pilot Operation no later than within 6 months from the day of this Agreement becomes effective and in accordance with the detailed time schedule of the Implementation which forms the Annex No. 6 hereto (hereinafter only as “**Time Schedule**”), whereas the Implementation of CUPPS System and Installation of End User Workplaces including the systems of airlines, listed in Annex No. 7 hereof and operating from Prague on 1st January 2021, shall be implemented until 31st December 2020. The Parties may mutually agree on phasing of the Time Schedule where the finish of the Pilot Operation deadline may be extended.

3.1 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 (hereinafter referred to as the “**Delivery Place**”). The Supplier has the right to perform works on the Work even outside the Delivery Place, however, only subject to a previous written consent of the Customer.

IV. DELIVERY OF THE SYSTEM

4. The Supplier undertakes to:

4.1 complete the Work at its own costs and risk in accordance herewith and the annexes hereto, with the instructions of the Customer's authorized employees that are not contrary to this Agreement or exceeding obligations of Supplier under this Agreement and to remove all Defects rebuked in the course of Handover.

4.1.1 complete the Work (or any part hereof) personally in accordance herewith. The Supplier is authorized to perform the Work (and any part thereof) via a subcontractor, without obtaining a previous written consent of the Customer. Supplier will perform the Work (or any part thereof) in accordance with this Agreement via a subcontractor. Supplier will notify Customer of Supplier’s subcontractor and Supplier will be responsible to the Customer for the completion of the Work (or the respective part thereof) in accordance with this Agreement in the same scope as if he performs the Work himself. The appointment of the subcontractor will not affect the Supplier's obligation to complete the Work in accordance herewith and this obligation stays with the Supplier during the whole Term of this Agreement;

4.1.2 comply with all generally binding legal regulations applicable to it generally as a provider of information technology services and remove all waste generated during performance of the Work in accordance with the applicable legislation at its own costs however Supplier is not responsible for the requirements of regulations or laws applicable to Customer’s business (including those relating to Work or Services that Customer acquires under this Agreement), or whether Suppliers’ provision of or Customer’s receipt of particular Work or Services under this Agreement meets the requirements of such regulations or laws;

4.1.3 report immediately by email 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 to the Supplier or the Supplier's employees. Similarly, the Supplier 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 The Customer will provide the Supplier with all necessary cooperation consisting particularly in:

4.2.1 providing an access to the Delivery Place and secure storage of the Hardware, both during the implementation project and for Hardware spares post implementation,

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

4.2.3 ensuring the operation of all technical infrastructure of the surrounding systems associated with the subject hereof.

Any Supplier time limits under this Agreement shall be extended for the duration of time during which the Customer fails to provide cooperation necessary for fulfillment of corresponding Supplier’s obligation under this Agreement.

4.3 <u>Handover and Takeover of the Work.</u> Handover and takeover of the Work will take place on the basis of the acceptance procedure which has the following stages:

4.3.1 Installation, Implementation and Integration of CUPPS/CUSS core System with the exception of airlines systems that are scheduled to be implemented later based on mutual agreement of the Parties and at least one (1) dedicated End User Workplace and at least one (1) CUSS kiosk,

4.3.2 Verification Operation,

4.3.3 Penetration Test,

4.3.4 End User Workplaces Installation and Pilot Operation,

4.3.5 Documentation handover,

4.3.6 Handover Protocol signing,

4.3.7 Implementation of airlines systems that are scheduled to be implemented later based on mutual agreement and Implementation Time Schedule.

4.4 <u>Verification Operation.</u>

4.4.1 After the successful Installation, Implementation and Integration of the CUPPS/CUSS core System and at least one (1) dedicated End User Workplace and at least one (1) CUSS kiosk, the Customer will carry out a Verification Operation, within ten (10) Business Days from the notification of the Supplier that the CUPPS/CUSS System is ready to be tested.

4.4.2 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 Supplier's repeated request, the Verification Operation will be considered finished without Defects.

4.4.3 The Parties will sign a record of the completed Verification Operation.

4.4.4 The number of Defects during the Verification Operation shall not exceed the following values:

4.4.4.1 Category A Defects…………………..0

4.4.4.2 Category B Defects………………….. 0

4.4.4.3 Category C Defects…………………..10

4.5 If the record of the completed Verification Operation implies that the CUPPS/CUSS System does not meet the criteria stated in art. 4.4.4 hereof, the Supplier will remove the detected Defects and, after they are removed, the Supplier will call the Customer to start the Verification Operation with the art. 4.4 hereof being applied as appropriate. The procedure of testing and subsequent defect removal will repeat until the Supplier meets the acceptance criteria stated in art. 4.4.4 hereof, however, no more than twice (2x) and no later than by two (2) months from the first round of Verification Operation.

4.6 Penetration Test.

4.6.1 Unless otherwise provided in article 1.37 (definition of "Penetration Test"), after the successful Installation, Implementation and Integration the Customer will carry out a Penetration Test, within ten (10) Business Days from the notification of the Supplier that the Work is ready to be tested. The performance of the Penetration Test will be supplied by a third party at the Customer's expense. The Supplier is obliged to provide all necessary cooperation for the performance of the Penetration Test.

4.6.2 Provider of Penetration Test will perform the penetration test report, which will be presented to the Supplier (hereinafter as „**Penetration Test Report**").

4.6.3 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 Supplier is entitled to proceed to EUW installation, as stated in art. 4.8. 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:

4.6.3.1 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.).

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

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

4.7 In the event that the Penetration Test Report uncovers that the Work shows any security issues of the Categories listed in art. 4.6.3 hereof, the Supplier undertakes to remedy the uncovered deficiencies and, after the removal thereof, to invite the Customer to initiate the Penetration Test again, with art. 4.6 hereof being applied as appropriate. This process and subsequent troubleshooting will be repeated until the Supplier meets the acceptance criteria as set forth in art. 4.6.3 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 Supplier's expense. Parties agree that Supplier is not responsible for the costs or expenses for performance of any repeated Penetrations Test that exceed costs or expenses expended by the Customer on the first Penetration Test under art. 4.6.1.

4.8 End User Workplaces Installation.

4.9 After successful Verification Operation, the Parties will mutually agree on the End User Workplaces Installation Schedule (hereinafter referred to as "**EUW Installation Schedule**") stating the schedule of replacement of the current EUW by Suppliers Hardware. The EUW Installation Schedule shall take into account operational possibilities of Prague Airport and most of the replacements will be carried out during night hours. Both Parties will exert reasonable effort to manage the Installation of End User Workplaces within four (4) weeks.

4.10 The risk of loss of the End User Workplace passes to the Customer to the date of the Installation of the respective EUW according to EUW Installation Schedule. From the moment of delivery until the risk transfers to Customer, Customer shall ensure that the Hardware comprising the End User Workplace shall be kept in a secure storage room with appropriate environmental conditions (Supplier shall notify Customer of these) with access only by authorised Customer personnel.

4.11 Pilot Operation.

4.11.1 The Pilot Operation starts after Installation of the first EUW according to EUW Installation Schedule, unless otherwise agreed by the Parties and ends fourteen (14) Days after Installation of the last EUW according to EUW Installation Schedule.

4.11.2 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 Supplier's repeated request, the Pilot Operation will be considered finished without Defects.

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

4.11.4 The number of Defects to the end of the Pilot Operation shall not exceed the following values:

4.11.4.1	Category A Defects…………………..	0
4.11.4.2	Category B Defects…………………..	0
4.11.4.3	Category C Defects…………………..	5

4.11.5 If the record of the completed Pilot Operation implies that the Work does not meet the criteria stated in art. 4.11.4 hereof, the Supplier will remove the detected Defects and, after they are removed, the Supplier will call the Customer to start the Pilot Operation with the art. 4.11 hereof being applied as appropriate. The procedure of testing and subsequent defect removal will repeat until the Supplier meets the acceptance criteria stated in art. 4.11.4 hereof, however, no more than twice (2x) and no later than by date set in the Time Schedule.

4.11.6 After the Pilot Operation is successfully completed and the acceptance criteria are met pursuant to article 4.11.4 hereof, the Customer will check and confirm the completeness of the Documentation 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 Pilot 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.

V. HARDWARE

5. The Supplier undertakes to deliver to the Customer Hardware in specifications and numbers specified in Annex No. 2 hereto and to enable the Customer to use such Hardware for the entire Initial Term and, if extended in accordance with article 11, the Extended Term of the Agreement subject to the terms of this article 5. Any upgrades required to the Hardware triggered by the Customer's request for change or new functionality should be at Customer's expense.

5.1 Customer shall have no interest or right in such Hardware, except to use it in accordance with this Agreement. Title to the Hardware shall remain with Supplier. Supplier retains the right to substitute the whole or any part of the Hardware with equipment of similar or improved specification, on reasonable prior notice to Customer, if Supplier deems such substitution necessary or desirable for the performance of the Agreement.

5.2 Customer will be responsible to Supplier for any damage to or loss of the Hardware, and will bear all risks related to the Hardware, from the moment of its Installation according to EUW Installation Schedule or the respective Order or from the moment of substitution of the Hardware under Article 5.1 of this Agreement. Customer shall maintain appropriate insurance covering the Hardware against these risks.

5.3 For the entire Initial Term of the Agreement, the Supplier will be responsible for functionality of the provided Hardware and shall eliminate any and all Errors. Notwithstanding the aforementioned, Customer undertakes:

5.3.1 to operate the Hardware in accordance with Supplier's or the relevant manufacturer's operating instructions and any applicable local, national and/or international regulations;

5.3.2 to ensure that proper environmental conditions as recommended by Supplier or the relevant manufacturer are maintained for the Hardware and that the exterior surfaces are kept in reasonable condition;

5.3.3 not to make any modifications to the Hardware, or disconnect, remove, alter or interfere with the Hardware; and

5.3.4 not to physically connect to the Hardware any accessory, exhibit or additional equipment other than that which has been supplied by or approved by Supplier and to maintain all necessary security procedures when operating the Hardware, especially to always use latest updated software with applied security patches and updated antivirus protection in any devices connected to the Hardware, if applicable;

5.3.5 to ensure that the Hardware is always kept in optimum operating condition (except only for fair wear and tear);

5.3.6 to keep possess of the Hardware, and not do anything that will interfere with Supplier's ownership interest in the Hardware, including without limitation, not selling, underletting or lending the Hardware nor allowing the creation of any mortgage, charge, lien or other security interest in respect of it, however the Hardware will be used by handling companies and airlines operating within Prague Airport;

5.3.7 to notify Supplier promptly of all material matters relating to the Hardware including if the Hardware is lost, stolen, damaged or confiscated; and

5.3.8 not to use or allow the Hardware to be used for any unlawful purpose.

5.4 The Supplier will not be liable for any Hardware Defects or Errors caused by use other than in clause 5.3, negligent acts or omissions, incorrect usage, improper treatment, or use of the Hardware, its physical damage, or theft caused by employees of the Customer or any third person; or modifications or maintenance of the Hardware that were not performed by or on behalf of Supplier, or exclusions from standard warranty terms as specified in Annex no. 8 . The Customer will be in such case obliged to indemnify the Supplier within the scope of costs relating to repair or replacement of the damaged or stolen Hardware.

5.5 To avoid any doubts, the Parties expressly stipulate that the Hardware shall be for the entire Initial Term and, if extended in accordance with article 11, the Extended Term of the Agreement owned by the Supplier and the Customer shall enable the Supplier to pick up the Hardware within fourteen (14) days from the termination of this Agreement; the Supplier shall pick up the Hardware within ninety (90) days from receiving the Customer's request to do so at the Place of Performance. A record signed by both Parties shall be drawn-up on Hardware pickup. Customer will ensure that Hardware that is returned to Supplier is in good working condition, except for fair wear and tear.

5.5.1 If Customer desires at its option to establish ownership of the Hardware at the end of the Initial Term or (if applicable) the Extended Term (described in Section 11), then no later than sixty (60) days prior to the end of such Initial Term or (if applicable) the Extended Term, Customer shall send written notice of such desire to Supplier. Upon Supplier's receipt of such notice, the Parties shall negotiate in good faith to agree the terms of ownership (including additional fees payable by Customer to Supplier) as agreed in writing and signed by both Parties. Once signed, Section 5.5 above shall no longer apply. If Supplier does not receive notice as described in this Section 5.5.1, or if Supplier receives notice but the Parties have not or are unable to agree the written terms of ownership prior to the end of the Initial Term or the Extended Term, then Supplier shall continue to own the Hardware and Section 5.5 shall continue to apply.

5.5.2 The Supplier furthermore undertakes to provide maintenance and remote administration of the Hardware for the entire Initial Term of the Agreement. Price of maintenance and remote administration of the Hardware is included in the Service Fee pursuant to this Agreement for the Initial Term. The Hardware maintenance services shall comprise the manufacturer's warranty and those services stipulated in clause 7.12 (On-Site support). During the Extended Term, the manufacturer's warranty of the Hardware will have expired. Accordingly, the Minimum Monthly Service Fee as specified in art. 10.2 hereof shall be increased up to 10% during the Extended Term to cover the support and maintenance of the Hardware during the Extended Term. However, in case that the particular Hardware will no longer be supported by the manufacturer or the particular Hardware will be beyond repair, a new Hardware shall be obtained by the Customer.

5.6 The Supplier declares that Hardware:

5.6.1 complies with the specifications given in Annex No. 2 hereof,

5.6.2 will be free from any Defects,

5.6.3 satisfies all the requirements laid down by applicable legal regulations, and legally binding public health, healthcare standards as well as similar standards concerning such goods,

5.7 The Supplier undertakes to deliver together with the Hardware to the Customer the papers and documents relating to the Hardware, including in particular:

5.7.1 instructions for use of the Hardware and possibly also other documents necessary for a proper and complete training of the operators of the Hardware,

5.7.2 documents confirming the usability of the Hardware on the territory of the Czech Republic and their compliance with applicable EU legal regulations.

5.8 Customer shall only use Hardware provided or certified by Supplier within the System. If Customer uses equipment not provided or certified by Supplier within the System, the System may be compromised and additional System support charges may be payable.

5.9 Certain third party software may be included with the Hardware (e.g. Windows), which will be governed by the terms of the applicable license agreement. Customer is responsible for complying with the terms of the license agreement, provided that compliance with the terms of the license agreement will not restrict Customer’s ability to use the System to the extent contemplated by this Agreement.

5.10 Customer shall ensure that its users and personnel comply with PCI DSS standards when using the relevant System to process, capture or enter credit card details. Customer shall ensure physical security of the relevant Hardware at Customer's premises to ensure they are not tampered with in a way that could put at risk PCI DSS compliance. Customer shall allow relevant PCI DSS audits of the relevant System and components. Customer shall indemnify and hold harmless Supplier and its affiliates in respect of any third party claims and losses arising directly or indirectly from a breach of this provision and the limitation of liability shall not apply. Supplier reserves the right to introduce technical or procedural mechanisms to contain or mitigate any breach hereof. In case of Customer failure to comply with this clause, Supplier reserves the right to disable the affected non-compliant functionality. Supplier shall not be responsible for PCI-DSS compliance of airline or other third party applications and systems.

VI. LICENSE

6. Based on this Agreement, the Supplier provides the Customer with a License to (i) use the CUPPS/CUSS System and (ii) the End User Workplaces, which are limited in time to the Initial Term and, if extended in accordance with article 11, the Extended Term of this Agreement, limited to the Prague Airport within the Czech Republic and limited in to the number of End User Workplaces then connected to the CUPPS/CUSS System according to Annex No. 2 hereof, for an unlimited number of transactions, without any limitation to processed data volumes. The License to use the CUPPS/CUSS System and End User Workplaces is non-exclusive and non-transferrable and can be used in unchanged object code form only for the purposes of the Customer pursuant to the Agreement. Notwithstanding the foregoing, the Supplier hereby agrees that the End User

Workplaces will be used by Authorized Persons and such usage is included in the License and the Service Fee for the Services. The Customer hereby accepts this License.

6.1 In order to avoid any doubts, the Parties hereby agree that the remuneration for the provision of the License is included in the Service Fee as specified in this Agreement.

6.2 Customer must not use, or permit any person to use, the CUPPS/CUSS System in any way not permitted by this Agreement or license terms. Without limiting the generality of the foregoing, unless permitted by this Agreement or the relevant third party software provider's licence terms, Customer will not:

6.2.1 use, integrate or combine the CUPPS/CUSS System with other software not installed, provided or approved by Supplier;

6.2.2 modify, adapt, create derivative works, translate, disassemble or otherwise discover or access the source code of, decompile or reverse-engineer or rent, sell, lease, sublicense, distribute, assign, or attempt to do so for any reason the CUPPS/CUSS System or use the Services for the benefit of any third party through any outsourcing arrangement; however for clarity, Customer may permit its Authorized Persons and handling companies to access and use the Services on Customer's behalf in accordance with this Agreement (unless such restrictions are expressly prohibited under the relevant law, in which case the Parties shall discuss in good faith to agree in writing the scope of the restriction);

6.2.3 copy, reproduce or transmit to the public any of the CUPPS/CUSS System; or

6.2.4 cause or permit any person to do any of the things referred to in Section 6.2.1 to 6.2.3. hereof.

6.3 Customer will:

6.3.1 ensure that all such measures as Supplier may prescribe from time to time for the protection of the CUPPS/CUSS System from unauthorized use are adhered to by Customer unless such measures do not impair the Customer's ability to use the CUPPS/CUSS System properly; and

6.3.2 notify Supplier immediately of the existence or the suspected existence of any unauthorized use of the CUPPS/CUSS System.

6.3.3 responsible for all acts and omissions of each Authorized Persons as if they were the acts and omissions of Customer. Authorized Persons shall have no entitlement to enforce this Agreement and Customer shall fully indemnifying Supplier and its affiliates against any claims by Authorized Persons. Customer agrees and procures that each Authorized Person agrees and acknowledges that Customer is solely responsible and liable for their use of the Services and any Customer data.

6.3.4 Customer grants (and Customer shall ensure that Authorized Persons grant) to Supplier, its affiliates and subcontractors a non-exclusive, non-transferable, world-wide right during the Initial Term and, if extended in accordance with article 11, the Extended Term of the Agreement (or as necessary thereafter under sub-clause b below) to access and use the Customer's Intellectual Property (IPR) and IPR provided to Supplier or its affiliates, by or on behalf of Customer or its Authorized Persons, in connection with Customer's or Authorized Persons' use of the Services and all documentation supplied to Supplier exclusively for the following purposes:

a) for the purpose and in minimal necessary extent of the performance of the Services, the fulfilment of Supplier's obligations under this Agreement, or for the resolution of disputes; or

b) as required by applicable law, demand, order (including injunctive relief), supervisory or regulatory authorities, court or government agency and by auditors; and

6.3.5 ensure Supplier and its subcontractors the right to verify Customer's use of the CUPPS/CUSS Systems, by remotely accessing the equipment; and

6.3.6 ensure the notices containing information of Supplier or its licensors ownership (i.e. reservation of rights, reference to trademarks, copyright notices, confidentiality obligations etc.) are not altered or deleted; and

6.3.7 Customer shall ensure that Customer and Authorized Persons IPR does not contain any advertising, announcement, solicitation, imagery, video, sound, music, hypertext link, or any other form of information, material, or communication that infringe any IPR; and

6.4 Customer acknowledges that certain components of the Service may be covered by open source software, free software, or shared source software, or other software license limiting or restricting the distribution or licensing of software to third parties (hereinafter referred to only as "**Open Source Components**"). In such cases:

6.4.1 to the extent required by the license covering an Open Source Component, the terms of such license will apply in lieu of the terms of this Agreement; and

6.4.2 to the extent that the license covering an Open Source Component prohibits any of the restrictions in this Agreement, such restrictions will not apply to such Open Source Component.

6.5 Some Open Source Component implementations will require the Customer to download the relevant Open Source Component from a reputable website. If the Customer requests Supplier, Supplier will download such Open Source Components for and on behalf of the Customer either remotely onto Customer equipment or at the relevant Customer location.

6.6 In order to access or use a Service:

6.6.1 Customer will only use equipment, which Supplier has certified for use in conjunction with such Service; and/or

6.6.2 if Customer desires to use any other equipment, such equipment must be certified by Supplier or by CUPPS/CUSS System developer in advance of Supplier providing the Service. Supplier reserves the right to charge for the certification of such equipment at the rates, which will be announced to Customer in advance.

6.6.3 Supplier will provide Customer, upon Customer request, with the list of equipment, if any, which Customer will provide for the purposes of accessing or using the Services and which has been, or will be, certified for use.

6.7 Customer acknowledges that:

6.7.1 all IPR used by or subsisting in the Hardware are and shall remain the sole property of Supplier or its licensor. The Customer shall not at any time make any unauthorised use of such Intellectual Property Rights, nor authorise or permit any of its affiliates, employees, agents or contractors or any other person to do so.

6.7.2 The CUPPS/CUSS System may contain components that are subject to third party license or ownership rights. Where Supplier incorporates into the CUPPS/CUSS System any intellectual property or proprietary information which include IPR owned by a third party, Supplier shall ensure that the use of such third party components shall not affect any use rights, warranties or indemnities granted to Customer or its personnel by Supplier. If Supplier is advised by its third party licensors of any change to the license terms that Supplier considers would likely affect Supplier's provision of the CUPPS/CUSS System, Supplier shall advise Customer and the Parties shall consult and use commercially reasonable efforts to agree on any workaround required to mitigate any inability or difficulty of Supplier's provision of the CUPPS/CUSS System.

6.7.3 Supplier will have no obligation for: any claim that relates to open source software or freeware technology or any derivatives or other adaptations thereof that is not embedded by Supplier into the CUPPS/CUSS System; or

any claim that relates to Linux or Android open source software, even when it has been embedded into or distributed with the CUPPS/CUSS System.

VII. ENSURING FUNCTIONALITY, AVAILABILITY AND SUPPORT FOR THE SYSTEM

7. Functionality.

7.1 Functionality. During the Initial Term and, if extended in accordance with article 11, the Extended Term of this Agreement, the Supplier will ensure Normal Operation of the System and of the Ordered Work hereunder by removing Errors in accordance with the terms and conditions stipulated in this Agreement.

7.2 Error Reports. The Customer is obliged to report an Error to the Support Centre in such time after the detection thereof which may be reasonably required from the Customer. The Customer is obliged to describe the Error and the procedure or condition which led to the Error occurrence in the report and to provide all available information, error reports and data regarding the Error to the Supplier. Customer is obliged to specify a responsible contact person in the report.

7.3 Support Centre. The Supplier shall provide for during the Service Period:

7.3.1 availability of the Support Centre 24/7 for accepting Error Reports and for telephone consultations with the Supplier's employees having the necessary qualification (certification) and experience in relation to the System.

7.3.2 recording the following information to the reported Error:

7.3.2.1 description of procedure or conditions which led to the Error occurrence,

7.3.2.2 Error reports and entry data at the Supplier's request,

7.3.2.3 Customer's contact persons for negotiations with the Supplier.

7.3.3 responding to telephone, email or any other types of Error Reports made to the Support Centre by the Supplier's responsible employees who have the corresponding qualification and experience related to the System, in keeping the Response Times according to this Agreement.

7.3.4 performing localization and identification of Errors and their causes.

7.3.5 providing information on the status, procedure and the method of removing Errors, in keeping the Ongoing Information Period.

7.3.6 performing updates of the Documentation in the form of sending change reports so that the Customer had continuously at disposal up-to-date Documentation to the System which the Customer uses at the relevant moment.

7.4 General Parameters. In providing Services the Supplier will comply with the following time limits:

Error category	Response Time/Start of Error Removal	Time for Error Removal	Information frequency (Frequency of ongoing information)
Category A System Error	within 15 minutes	Up to 30 minutes	Every 15 minutes until the Error is removed
Category B System Error	Up to 2 hours	Up to 8 hours	Every 2 hours until the Error is removed
Category C System Error	by the next Business Day	Up to 14 calendars days	Every 24 hours until the Error is removed
Category D System Error	Within the next 5 Business Days	Next application release	n/a

Type of End User Workplace	Term for EUW Error removal during Service time hours	Term for EUW Error removal outside Service time hours
Check-in	30 minutes	120 minutes
Gate	30 minutes	120 minutes
Transit	30 minutes	120 minutes
Back-office	120 minutes	120 minutes
Training room	120 minutes	120 minutes
CUSS kiosk	60 minutes	120 minutes

7.4.1 Times for Error Removals of Category A System Error, Category B System Error, Category C System Error and time limits and Term for EUW Error removal are doubled during a time of Reduced Operation.

7.5 The Response Times and the Time for Error Removal stated in this article start when the Customer's Report with information described in article 7.2 hereof is delivered to the Supplier's Support Centre. The same applies for setting the Frequency of Ongoing Information.

7.6 The Customer determines the Error Category and deliver the Report to the Supplier's Support Centre.

7.7 The Parties have agreed on the procedure of providing ongoing information so that the Customer's employee contacts within the limits of the agreed Frequency of Ongoing Information the Supplier's Support Centre and the Supplier will inform him about the current status of the process of the Error removal.

7.8 Removal of the Software Errors and the Software Support.

7.8.1 The Supplier will remove the System Errors within the Time for Error Removal, unless otherwise agreed between the Parties, as follows:

An Error is removed when an Error is not presently affecting the Service once:

a) the Service impact has ceased or been removed or;

b) a documented Error workaround has been carried out by Supplier; or

c) a workaround has been identified, provided to and agreed by the Customer; or

d) a permanent solution has been implemented via a recovery Problem Tracking Record.

The Customer is obliged to provide the Supplier with all available information and cooperation necessary for Error Removal as described in article 7.2 hereof.

7.9 Removal of the Hardware Errors and the Hardware Support.

7.9.1 The Parties hereby agree on the following Defect of Hardware rectification methods:

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

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

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

7.10 System Shut-Down. Except for removing the reported Error, the Supplier has the right to shut down the System only during the Service Windows or upon a previous agreement with the Customer.

7.11 Excluded Liability for Errors. No penalties shall apply and the Supplier will not be liable under art XII or otherwise in this Agreement pursuant to the previous provisions of this art. VII for an Error occurred by third party or airline applications or systems outside Supplier’s control, or a planned System outage or events of Force Majeure or an intervention of persons other than the Supplier or the Supplier's subcontractors or by the use of the System in conflict with the provided Documentation. For avoidance of any doubt the Parties hereby agree that notwithstanding of the foregoing the Supplier shall stay fully responsible and liable for applications and systems provided by its subcontractors.

Furthermore, Supplier shall not be responsible and no penalties shall apply for any failure to perform to the contracted standards or to maintain Normal Operation of the System or to meet service levels or the parameters described in this Section 7 or 7.4 to the extent that such failure is directly attributable to any of the following:

i. Unvalidated changes introduced by an external party other than Suppliers subcontractor (Airport, airlines, ground handlers) to the System (e.g., functionality changes that require a difference in the CUPPS/CUSS system or the System, which were introduced without the CUPPS/CUSS system or the System provider validation); or

ii. Any time the System is not available as a result of Supplier's scheduled Service Windows or extraordinary scheduled Service Windows, Airport or airline-initiated maintenance or any other agreed-to scheduled downtime activity; or

iii. Unavailability of or errors in the System developed by or incorporated by the Airport or Authorized Persons through (I) modifications or plug-ins to the System, or (II) unsupported programming, unsupported integrations or malicious activities; or

iv. Unavailability of or errors in the System because of the Airport or Authorized Persons using the System contrary to the then-current Documentation; or

v. Events outside Supplier's reasonable control that could not have been mitigated against by Supplier taking reasonable steps and implementing all relevant disaster recovery and back-up procedures in a timely manner; or
vi. Any issue caused by a Force Majeure event.

Additionally, the achievement of the parameters described in this Section 7 or 7.4 may be impacted by factors outside of Supplier's control. Accordingly, no service levels or performance warranties apply for transmissions through the Internet or any other network or interactions with systems outside of Supplier's control such as (non-exhaustively) local network performance degradation, or third party systems or application settings that are not in the control of Supplier to establish and maintain.

Notwithstanding the foregoing, the Parties hereby agree that services (including transmissions and connections) provided by Suppliers' subcontractors shall not be deemed outside of Suppliers control.

Connectivity between the Supplier data centres, if applicable, and the airlines' DCS hosts is excluded from these parameters described in this Section 7 and 7.4. These links are managed by each of the airlines.

7.12 On-Site Support. A local field service team of Suppliers representatives qualified to remove Errors shall be present at Prague Airport during Service Time. Outside the Service Time hours, the Supplier representative will be available on-call. The Customer will provide to the Supplier office space equipped with furniture, electricity, water, necessary facilities and internet connection in the Place of Performance based on separate rental agreements and warehouses free of charge. Among the main tasks of the local field service team will belong:

7.12.1 Device troubleshooting including checking and correcting configuration issues.

7.12.2 Installing and configuration of new devices.

7.12.3 Replace faulty devices – a local field service team is required to remove the defective device and replace it with a spare device.

7.12.4 Repair faulty device – depending on the device, the local field service team may be able to perform the local repair of the device.

7.12.5 As further described in Section 7.12.10, return faulty devices to manufacturer or service partner – depending on the device, the local field service team may package and dispatch the device to the manufacturer or service partner for repair or replacement.

7.12.6 Maintain an asset register – the location and status of all local devices should be identified and managed via an asset register.

7.12.7 Conduct Preventative Maintenance – preventive maintenance and cleaning of the local devices in regular intervals.

7.12.8 Maintain and provide Consumable Stock Supplies – maintaining sufficient stock and refilling of all consumables, either supplied by Supplier (e.g. ATB and BTP print heads and print tapes for DCP) or Customer at its cost (e. g. CUSS boarding passes, bag tags, and DCP paper rolls) to not interrupt operations. These consumables will be replenished by Supplier at each EUW and kiosk when needed.

7.12.9 Perform hardware relocations, e.g. CUSS kiosks or any other peripherals due to operation changes and requirements.

Tasks under articles 7.12.1 – 7.12.9 hereof are covered by the regular monthly Service Fee and will not be charged separately.

7.12.10 If it is necessary according to manufacturer's capabilities to return the Hardware/devices to the designated manufacturer's office for repair or replacement, Customer and Supplier agree that:

a) Supplier will coordinate at Supplier's cost with a courier to have the Hardware/devices delivered to the designated manufacturer's office;

b) Supplier is responsible for packing such Hardware/devices according to the standards necessary to prevent damage to the Hardware/devices in transit; and

c) Supplier will bear all costs and risk (including delivery costs and associated taxes) for return of the Hardware/devices to the designated manufacturer's office and, where the applicable defect is within warranty, the designated manufacturer will bear the costs and risk of return of the Hardware/devices, provided that such Hardware/devices is returned to Supplier's original address of dispatch.

7.12.11 The designated manufacturer's office may be a regional office if so specified in this Agreement or Supplier's customer service plan.

7.13 Availability

7.14 The Supplier will provide for the Availability of the System so that the sum of all times of durations of the reported Category A System Errors did not exceed during the relevant calendar year six (6) hours.

7.15 The Supplier shall meet the following:

7.15.1 the maximum consecutive time of the non-planned failure (Category A System Error) of the System will not exceed two (2) hours

7.15.2 a non-planned failure (Category A System Error) will not occur more than three (3) times per calendar year.

7.16 The evaluation of Availability will take place on a monthly basis by comparing reports on the System Errors recorded by the Customer and the Supplier. The Supplier will send for the purpose of such comparison to the Customer monthly reports on the Reported Errors to the contact data stated in the Annex No. 1 hereof, each time within the fifteenth (15th) day of the following month after the evaluated month. Such report will contain a list of all reported Errors with their identification numbers, time snapshot of their solution, a brief description of their solution and the evaluation of fulfilment of time periods for removal of Error and Defects agreed hereunder.

7.17 Changes of applicable legislation. The Supplier will ensure that the System and the Ordered Work in any moment of the Initial Term and, if extended in accordance with article 11, the Extended Term of this Agreement (i) is in accordance with the applicable legislation regarding particularly personal data protection as further described in Section 1.1.4a of Annex No. 4, cyber security and tax legislation applicable to Supplier generally as a provider of information technology services. Supplier is not responsible for determining the requirements of legislation applicable to Customer's business, (including those relating to services, Systems or Ordered Work that Customer acquires under this Agreement), or whether Supplier's provision of or Customer's receipt of particular Services, Systems or Ordered Work under this Agreement meets the requirements of such legislation . In case of change of legislation concerning the System or the Ordered Work applicable to Supplier's obligations under this Agreement and imposing mandatory functional or technical requirements on the provision of the System or the Ordered Work, or deliverables, or the composition of the components provided under this Agreement, the parties shall negotiate in good faith to agree a change (including to govern any development work) signed by Customer and Supplier subject to agreement by Customer to pay charges if any charges relate to such change.

VIII. OTHER RIGHTS AND OBLIGATIONS OF PARTIES

8. The Customer will be authorized to print and use the Documentation regarding the System in unlimited number of copies, however, only for the internal use by the Customer,

8.1 The Customer undertakes to cooperate with the Supplier in System adaptations and service actions during System faults consisting in assurance of:

8.1.1 access to the End User Workplaces,

8.1.2 provision of information on CUPPS/CUSS System functioning in form of consultation with Customer's employees,

8.1.3 provision of access for CUPPS/CUSS System updates,

8.1.4 informing about the changes in CUPPS/CUSS System settings and about changes of infrastructure directly influencing the CUPPS/CUSS System functionality.

8.2 The Customer undertakes to

8.2.1 treat the System with due care in order to avoid any damages and prevent any possible damages.

8.2.2 notify the Supplier immediately of any Errors of the System or provided Services or any other claims exercised by third parties that prevent the Customer from using the Services, by the means specified in the Agreement.

8.2.3 use and secure all documentation obtained within the framework of the System so that no third party can obtain such documentation without the Supplier's consent.

8.2.4 secure appropriate power supply (230V) and underlying network infrastructure which is not part of the Services provided under this Agreement.

8.3 The Supplier undertakes to:

8.3.1 provide the Services with efficiency and professional care that can be expected from a competent communications and information technology services provider operating in the air transport industry, in accordance with this Agreement, and through employees having sufficient education and experience with provision of given performance.

8.3.2 provide reasonable cooperation to all handling companies and airlines operating on Prague Airport in order to successfully install and run their applications (for the scope of initial implementation listed in Annex No. 7 hereof) used for passenger, luggage and aircraft processing and operation (e.g. Departure control systems, reservation systems, weight and balance systems etc.). The remuneration for such cooperation is already included in price for the Services pursuant to Art. 10 hereof. Implementation of non DCS (DCS in a meaning of Departure control systems, reservation systems, weight and balance systems) applications other than those listed in Annex No. 7 hereof shall be subject to additional charges at the man day rate for the agreed effort payable by Customer to Supplier. Supplier reserve the right to refuse to implement non DCS application.

8.3.3 make sure that his employees or employees of his subcontractors 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 Supplier's employee an entry to the Delivery Place. In case that such a breach results in a delay in completing the subject of the Agreement, the liability will reside with the Supplier. The parties have agreed that the same procedure will apply also if any employee of the Supplier and of the Supplier's subcontractor commits a crime at the Delivery Place or in case of a violent behavior to the Customer's employees or other persons at the Delivery Place.

8.3.4 make sure that his employees or employees of his subcontractor 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 familiarized by the Customer.

8.4 The Supplier may use subcontractors and such use shall not be subject to prior written consent of the Customer. Supplier will notify Customer of Supplier’s subcontractors. The Supplier will be responsible for any and all performance provided through its subcontractors and affiliates within the same scope and quality as if such performance was provided by themselves.

8.5 CUPPS/CUSS System is an information system that collects, stores and processes large amounts of data. The Supplier undertakes not to use the data obtained by CUPPS/CUSS System for any purpose other than for the proper provision of Services under this Agreement. In particular, the Supplier shall not pass on such acquired data or its derivatives to third parties or use it for its own commercial purposes.

8.6 Warranties and Representations.

8.6.1 The Supplier shall warrant to the Customer that the CUPPS/CUSS System correctly (in the form received by it from third party systems) processes all data to or from all defined System interfaces as specified in the Annex No. 2 hereto.

8.6.2 The Supplier hereby warrants to the Customer that the CUPPS/CUSS System installed by the Supplier will not contain at the date of delivery known viruses, malware or other functions that would prevent the Customer from using the

CUPPS/CUSS System or which would render the System non-functional or which would limit or otherwise impair the system functionality.

8.6.3 The Supplier represents that he has the right to grant to the Customer a License to the System and the Ordered Work, or a Sublicense, if appropriate. The Supplier hereby warrants that the relevant Ordered Work or other supplies of the Supplier pursuant to this Agreement, or the use of the Ordered Work by the Customer will not infringe and will not result in any infringement of any third party intellectual property rights. Should the Supplier breach his obligation arising out of the warranty stated in this article, the Supplier will be liable for all and any consequences resulting from such a breach, including, without limitation, the obligation to immediately ensure the right for the Customer to use the hardware or the System or the Ordered Work which will not infringe any third party intellectual property rights and to indemnify the Customer for any damage (both pecuniary and non-pecuniary) which may be caused to the Customer.

8.6.4 The assurances provided by the Supplier pursuant to the provisions of Section 8.6 hereof shall apply for the entire Initial Term and, if extended in accordance with article 11, the Extended Term hereof. Should it appear during the Term hereof that any of the assurances pursuant to the provisions of Section 8.6 hereof were untrue, the provided Service will be considered to be defective. The Supplier undertakes to eliminate such Defects within thirty (30) Business Days from Defect notification.

IX. ADAPTATIONS

9. Adaptations:

9.1 Assignment. In the course of the Agreement Initial Term and, if extended in accordance with article 11, the Extended Term the Customer has the right to send to the Supplier at any time requests for the assignment for

9.1.1 adaptations and/or other changes of the System and/or

9.1.2 providing professional consultations in relation to the System and/or

9.1.3 activities related to the System which need special certificates required by the System manufacturer

9.1.4 delivery of additional Hardware

(hereinafter only as “**Adaptation**”) in the form of delivery of the assignment by email or in writing to the contacts of the Support Centre (hereinafter only as “**Assignment**”).

Provided that these Adaptations as described herein are not considered as a deviation from the Works and/or Ordered Works and both Parties agree to the terms and conditions that are applicable to these Adaptations.

9.2 Offer.

9.2.1 Unless a longer delivery period is determined by the Customer, the Supplier will send within fifteen (15) Business Days from the receipt of the Assignment to the Customer's contact person stated in the Annex No. 1 hereto either a response explaining that the Supplier cannot fulfill the Assignment and/or Adaptation (“**Rejection**”) or a quotation for the execution of the Assignment (hereinafter only as “**Offer**”) which will contain at minimum:

9.2.2 the method of calculation of the price for the Assignment using the Price List pursuant to the Annex No. 3 hereto and other costs, if applicable, unless otherwise agreed by the Parties

9.2.3 requests for the Customer's cooperation,

9.2.4 time schedule of the Assignment execution,

9.2.5 validity of the Offer which must not be less than 60 days, and

9.2.6 any other terms included by Supplier at its discretion.

The Offer shall always include all Supplier's costs of the Assignment execution.

9.3 Order.

9.3.1 The Supplier will perform the Adaptation only on the basis of an order delivered to the contacts of the Support Centre (hereinafter referred to as the "**Order**").

9.3.2 The Order will include:

written specification of the scope of the Adaptation requested by the Customer and in the version corresponding to the Offer, and Offer.

9.4 The Supplier will confirm the Customer's Order within five (5) Business Days after the receipt thereof. If the written confirmation of delivery of the Order is not delivered to the Customer within the time limit pursuant to the previous sentence, it is assumed that the Supplier confirmed delivery of the Order, unless the procedure pursuant to subparagraph 9.5 hereof applies.

9.5 The Supplier is not obliged to confirm delivery of the Customer's Order pursuant to art. 9.4 hereof only providing that:

9.5.1 the Customer has delivered the Order to the Supplier for works or supplies which are in conflict with the Assignment or the Offer, or

9.5.2 the Customer did not deliver the Order corresponding to the Offer to the Supplier on or before the end of validity of such Offer.

9.6 For the avoidance of any doubts, the Parties have explicitly agreed that the Order delivered to the Supplier will be considered a part agreement the subject of which is delivery of supplies specified therein (hereinafter only as "**Ordered Work**") for the price determined according to the Offer (hereinafter only as "**Price for the Ordered Work**") and in accordance with the time schedule specified in the Offer (hereinafter only as "**Delivery Date of the Ordered Work**") and which is governed by this Agreement as regards the terms that are not explicitly agreed in the Order. Each Order will always refer to the reference number of this Agreement and will be numbered in an ascendant Order.

9.7 For the avoidance of any doubts the Parties have agreed that the Ordered Work will always include an amendment to the Documentation containing the update of a change related to the Ordered Work.

9.8 Handover and Takeover of the Ordered Work (for Hardware are applicable only subparagraphs 9.8.4 and 9.8.5 of art. 9.8 hereof)

9.8.1 Handover and takeover of each Ordered Work will take place on the basis of the acceptance procedure which has following stages, if Parties have not agreed otherwise:

9.8.2 Verification Operation

9.8.3 Penetration Test (unless the Customer specifically determines that the Penetration Test is not required), and

9.8.4 Pilot Operation, if applicable, and

9.8.5 Handover Protocol signing.

9.9 If the subject of the Ordered Work is provision of professional consultations in relation to the System, the acceptance procedure will include only signing of the Handover Protocol.

9.10 For Verification Operation, Penetration Test, Pilot Operation and Handover Protocol in respect to Ordered Work, the provisions of articles IV – VIII hereof shall apply accordingly, unless mutually expressly agreed otherwise.

X. PRICE, PRICE MATURITY, INVOICING

10. The Customer will pay the Supplier for the Services monthly fees as specified in articles 10.1 – 10.3 and in Annex No. 3 hereof (hereinafter only as **"Service Fee"**) starting from the first day of the month following the month in which the Handover Protocol regarding the System was signed. The Service Fee will consist of:

10.1 Monthly Hardware Leasing Fee,[redacted] for provisioning of the initial Hardware delivery ("**Initial Hardware Delivery**") as further described in Annex 3, payable monthly by Customer to Supplier for thirty six (36) consecutive months during the Initial Term starting the month of signature of the Handover Protocol as described in article 10.9. The breakdown of the fee is provided in Annex 3 hereto.

10.2 Minimum Monthly Service Fee, [redacted] for provisioning of the System (excluding Hardware), Services and Support, payable by Customer to Supplier starting the month of signature of the Handover Protocol as described in article 10.9. This fee might also cover processing a certain number of passengers boarded within the System per calendar month (hereinafter referred to as "**Basic Monthly Passenger Limit**"). However, Basic Monthly Passenger Limit must not exceed 150 000 (one hundred and fifty thousand) passengers per calendar month. The parties hereby agree, that the Basic Monthly Passenger Limit is equal to 50 000 (fifty thousand) passengers boarded. The Minimum Monthly Service Fee is payable during the Initial Term and, if extended in accordance with article 11, the Extended Term. During the Extended Term, the Minimum Monthly Service Fee shall be increased for out-of-warranty Hardware support as described in article 5.5.2.

10.3 If the actual total number of boarded passengers within the System in any calendar month exceeds the Basic Monthly Passenger Limit, then, in addition to the Minimum Monthly Service Fee, Customer shall pay Supplier the following passenger fee,[redacted] (hereinafter referred to as "**Passenger Fee**"), multiplied by the number of boarded passengers exceeding the Basic Monthly Passenger Limit.

10.4 The Customer agrees to pay the Supplier for the Ordered Work the Price for the Ordered Work as a monthly fee if agreed between Customer and Supplier in the Order or such other amount and payment period as set forth and agreed in the Order.

10.5 The Service Fee and the Price for the Ordered Work include all direct and indirect costs of the Supplier which must be necessarily or efficiently expended in the course of performance of the Services, unless otherwise agreed by the Parties ad hoc. The Service Fee and the Price for the Ordered Work do not include a value added tax which will always be added at the statutory rate according to the applicable legal regulations as at the day of taxable transaction. The Parties agree to use reasonable endeavours to do everything required by the relevant value added tax legislation to enable or assist the other Party to claim or verify any input tax credit, set off, rebate or refund in respect of any value added tax paid or payable in connection with Services. No other taxes, duties, levies will be charged additionally.

10.6 The Customer is authorized to decrease the Service Fee or Price by the paid withholding tax or other similar tax in the case when such payment shall be in, accordance with Czech tax regulations, subject to withholding tax or other similar tax. In such case the sum representing withholding tax or any other similar tax shall not be considered as an unpaid liability of the Customer against the Supplier. Supplier hereby declares that its country of tax residence (in the meaning of the Agreement for the Avoidance of Double Taxation concluded between the Czech Republic and The Netherlands is The Netherlands and maintains permanent establishment/branch in the Czech Republic. In order to confirm it Supplier shall provide Customer with Supplier's valid certificate of tax residence issued by appropriate tax authority of its country for each calendar year for which the services specified in this Agreement will be performed. Supplier shall immediately inform Customer about any changes related to its tax residency; especially the changes of tax status of permanent establishment in the territory of Czech Republic. The new tax residency certificate or any other similar document will be sent by Supplier to Customer as well. Provided that Supplier does not inform Customer about the changes of tax residency and as a result the Customer will be required by any tax authorities to pay any additional taxes, duties or charges, including penalties; the Supplier will reimburse such expenses in the full extent to Customer.. Each contracting Party shall be responsible for its own corporate taxes imposed by the state of tax residence of any Party, or by international and local tax law no matter if such taxes are administrated by the other contracting Party.

10.7 Both Parties agree to co-operate to eliminate or reduce any applicable taxes, duties, interest, penalties or similar charges which may be payable by either Party, including, where applicable, providing or issuing the necessary documentation to support or secure exemptions or recoveries.

10.8 The Service fee and Price for Ordered Work (if set in a form of a monthly fee) will always be paid on the basis of an Invoice which may be issued by the Supplier at the last day of a calendar month in which the Service have been provided. For the purpose of the value added tax the Services are considered delivered on an ongoing basis. The date of taxable transaction is the last day of the month for which the invoice is issued.

10.9 The Price for the Ordered Work will always be paid on the basis of an Invoice which may be issued by the Supplier no sooner than on the day following the acceptance pursuant to art. 9.8 hereof. In case the Price for the Ordered Work is calculated as a monthly fee, the Service Fee will be respectively extended starting from the first day of the month following the month in which the Handover Protocol regarding the Ordered Work was signed. A copy of the Handover Protocol will be an integral part of the invoice. For the purpose of the value added tax, the day of signing of the Handover Protocol by the Customer will be the day of taxable transaction.

10.10 Maturity. The maturity period of an Invoice will be thirty (30) days from the day of delivery thereof to the Customer's address or by electronic means in the PDF format to the e-mail address specified in art. 10.14 hereof. 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 following business day. The price shall be paid directly to the bank account of the Supplier specified in the Agreement, unless a different bank account is indicated on the invoice. The Customer's obligation is settled when the invoiced amount is debited from the Customer's bank account in accordance with the payment data stated on the issued invoice.

10.11 Currency. All payments according to this Agreement will be made in Czech crowns.

10.12 The received Invoice must comply with all requirements set for a tax document pursuant to the applicable legal regulations of the Czech Republic, namely the Act on VAT, and must contain objectively correct data in relation to the supply. The Supplier is obliged to deliver an invoice to the Customer to the invoicing address set forth in this Agreement no later than by the 10th day following the date of taxable transaction. After the Customer receives the invoice, he has a maximum of 10 days to assess whether or not it is correctly issued or return it, if it is not. The Customer is not entitled to return the invoice after the 10 days have passed. The invoice must also include information about the Order number and the Customer's contract reference number based on which the supply is made, if applicable. 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. If Supplier’s invoice does not include sufficient detail and supporting documentation to enable Customer to reasonably determine whether Supplier’s fees or charges specified in such invoice are in accordance with the Agreement and/or the Customer disputes any amount in any invoice, the Customer shall pay the undisputed portion and shall endeavour to notify Supplier as soon as possible but, in any event, no later than on the due date of such invoice. Customer shall notify Supplier of the extent to which it disputes in good faith any of the fees or charges paid by Customer and of the reason for such dispute. The Parties shall meet to resolve such dispute in good faith, escalating the dispute where appropriate in accordance with Section 17.20 of the Agreement. After the resolution of any disputed amount the Customer shall promptly pay the agreed balance due to the Supplier.

10.13 Each party shall bear their own expenses and bank fees related to the wire transfer.

10.14 All amounts paid hereunder shall be due by electronic funds transfer within thirty (30) days of Customer’s receipt of the Supplier’s invoice using the bank details below (or such other details as Supplier may provide from time to time in writing).

Currency:	CZK
Name of bank:	MUFG Bank (Europe) N.V. Prague Branch
Address of bank:	Klicperova 3208/12, 150 00 Prague 5-Anděl, Czech Republic
Account number:	303327/2020
SWIFT/BIC:	BOTKCZPP
IBAN:	CZ9420200000000000303327

Supplier shall submit invoices to Customer as follows:

In documentary form to the address:
Letiště Praha, a. s.
evidence faktur (register of invoices)
Jana Kašpara 1069/1

160 08 Praha 6

or

By electronic means in the PDF format to the e-mail address:
invoices@prg.aero.

10.15 If in accordance with Act no. 235/2004 Coll., on Value Added Tax, as amended, the Supplier:

10.15.1 is declared by tax administrator's decision an unreliable payer, or

10.15.2 demands a payment for the taxable performance provided under this Agreement to a bank account which is not published by the tax administrator in a manner enabling remote access or to a bank account maintained with a payment services provider outside the territory of the Czech Republic

10.15.3 the Customer has the right to only pay to the Supplier's bank account the Invoice amount for the provided taxable performance without the value added tax (hereinafter referred to as "**VAT**"). The Customer may pay the VAT, if charged and if constituting a part of the Customer's payment under this Agreement, directly to the account of the relevant tax administrator. In such case the amount of the VAT shall not be regarded as an unpaid liability towards the Supplier and thus the Supplier may not demand the additional payment of the VAT or apply any contractual sanctions, late payment interests or contractual penalties. The Customer is obligated to inform the Supplier on this procedure and do so within no later than the date of the payment of the Price.

10.16 The Parties have agreed that any changes in the legal tender regulations of the Czech Republic do not have any impact on the validity of the Agreement and do not give either of the Parties the right to demand changes in the Agreement, except for technical changes, if necessary, directly ensuing from the regulations relating to the change in the legal tender of the Czech Republic. The Parties further declare that the potential fixation of the exchange rate of the Czech crown (CZK), as the only currency in the Czech Republic, to Euro (EUR) or the conversion of the financial liabilities under the Agreement from the Czech crown (CZK) to the Euro (EUR) will not be a reason for an early termination of or a change in the Agreement or for the prepayment of the amounts payable hereunder and will not be a reason giving rise to one Party's liability vis-à-vis the Party for any direct or indirect damage arising on the basis of the above described facts and the exchange rate risks thereto related, unless expressly agreed otherwise between the Parties.

10.17 Once the Czech crown (CZK) is no longer the legal tender of the Czech Republic, all the payment obligations ensuing from the Agreement shall be converted to the Euro (EUR) at an exchange rate which by law shall be fixed as of the date of the introduction of the Euro (EUR) in the Czech Republic. If the Euro ceases to exist, all the obligations hereunder shall be denominated in the Czech crown under conditions, including in particular the conversion rate, determined by the applicable legal regulation.

XI. TERM OF AGREEMENT

11. Agreement Term. This Agreement has been concluded for the time period of sixty (60) months counted from the date of signing of the Handover Protocol (hereinafter the "**Initial Term**"). If the

Customer does not notify the Supplier in writing that this Agreement is to be terminated at the end of the above 60 months, at least twelve (12) months before the date of termination, then this Agreement shall be extended for 12 months from the end of the Initial Term (hereinafter the "**Extended Term**"), at which time this Agreement shall expire. The Initial Term and the Extended Term together constitute the ("**Term**") of this Agreement. This Agreement 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 Agreement may enter into force at the earliest on a certain day which is later than the date of signature of this Agreement by the last Party, this Agreement shall become effective only on the date on which this Agreement may become effective in the first instance (hereinafter only as "**Effective Date**")

11.1 Methods of Termination of the Agreement. The effectiveness and force of this Agreement terminates only:

11.1.1 upon the lapse of the agreed Initial Term and if extended Extended Term, or

11.1.2 by a written agreement of the Parties, or

11.1.3 upon the lapse of the notice period on the basis of a notice filed in accordance with the requirements stipulated in art. 11.2 or art. 11.3 hereof

11.2 Notice of Termination filed by the Customer. The Customer has the right to terminate the Agreement, providing that:

11.2.1 the Supplier has repeatedly and despite a written notice materially breached his obligations pursuant to this Agreement, or

11.2.2 the Supplier has failed to remedy a breach of the warranties pursuant to art. 8.6 hereof, not even within the additional grace period of 20 (twenty) Business Days from the day he received the Customer's written request, or

11.2.3 the Supplier breaches his obligation pursuant to art. 12.1 hereof, whereas the Excess reaches at least 24 hours within a calendar year, or

11.2.4 the Supplier repeatedly breaches his obligation pursuant to art. 7.15.1 and/or 7.15.2 hereof.

Such notice does not need to be made without undue delay, but the Customer is not entitled to terminate the Agreement by notice after more than 12 calendar months have passed after the relevant breach.

11.3 Notice of Termination filed by the Supplier. The Supplier has the right to terminate the Agreement, providing that:

11.3.1 the Customer is despite a written notice late with payments of any amounts due hereunder and such delay continues longer than 30 calendar days.

11.4 Notice Period. The Parties have explicitly agreed that after the notice of termination is filed pursuant to art. 11.2 or art. 11.3, this Agreement will be terminated upon the lapse of the notice period of three (3) months computed from the first day of a calendar month following delivery of the notice to the other Party.

11.5 Termination for Change of Control. The Customer is entitled to terminate this Agreement unilaterally in case of a significant change of control over the Supplier or a change of control over significant assets used by the Supplier to make the supply under the Agreement. Such termination shall be effective to the date when notice of termination is delivered to Supplier.

11.6 Exclusion of Other Causes for the Agreement Termination. The Customer and the Supplier agree that this Agreement may only be terminated for the causes stipulated hereunder, unless the mandatory provisions of legal regulations imply an option to terminate the Agreement for other causes.

11.7 Surviving Provisions. The Parties have agreed that the provisions on contractual penalties which are a part of this Agreement, including the provisions of the Agreement which condition the right to claim the contractual penalty and all provisions which, by their nature, should remain after the termination of this Agreement, will remain in full force and effect even after this Agreement is terminated by any of the manners stipulated in this Agreement, except that such right to claim such contractual penalties incurred during the Agreement remains no later than six (6) months after termination of the Agreement.

XII. CONTRACTUAL PENALTIES AND INDEMNIFICATION

12. Contractual Penalties.

12.1 In case the Supplier breaches his obligation to remove an Error within the Time for Removal set forth in art. 7.4 hereof, the Supplier will pay the Customer for each such breach a Contractual penalty calculated according to the following table:

Error Categories	Contractual Penalty
Category A System Error	CZK 150,000 for each commenced hour of delay
Category B System Error	CZK 50,000 for each commenced hour of delay
Category C System Error	CZK 25,000 for each commenced day of delay
EUW Error	CZK 2,500 for each commenced hour of delay

12.2 If the Supplier breaches his obligation pursuant to art. 7.14 hereof, the Supplier will pay the Customer a Contractual penalty in the amount according to the following table:

Excess	Contractual Penalty
More than 6 hours for a calendar year, but less than or equal to 12 hours in a year	CZK 450,000 for each commenced hour of delay
More than 12 hours for a calendar year, but less than or equal to 24 hours in a year	CZK 750,000 for each commenced hour of delay
More than 24 hours for a calendar year	CZK 900,000 for each commenced hour of delay

12.3 In addition, the Supplier will pay the Customer:

12.3.1 a Contractual penalty in the amount which will be determined as a sum of the amount of CZK 20,000 for each day of delay in proper fulfilment of the terms set in Annex 6. hereof (Implementation Time Schedule) , or

12.3.2 a Contractual penalty in the amount of CZK 10,000 (in words: ten thousand Czech crowns) for each breach of any obligation set forth in art. 4.1 hereof, which penalty must be paid by the Supplier even repeatedly, providing that the default status of the respective obligation continues more than two (2) Business Days, or

12.3.3 a Contractual penalty in the amount of CZK 10,000 (in words: ten thousand Czech crowns) for each breach of the obligation set forth in art. 7.3.1 hereof, or

12.3.4 a single-time penalty the amount of which will be determined as a sum of the amount of CZK 20,000 and the amount corresponding to 0.1% of the Price for the Ordered Work for each day of delay in proper fulfilment of the obligation in case the Supplier breaches his obligation to hand over the Ordered Work or remove the Defects described in the Handover Protocol within 14 (fourteen) Business Days from the day of signing of the Handover Protocol pursuant to art. 9.8 hereof and/or the obligation to supply the Ordered Work by the Delivery Date of the Ordered Work, or

12.3.5 if a Penetration Test is conducted by Customer’s third party authority (and not by Supplier’s third party authority as further described in Section 1.37), then a Contractual penalty of CZK 20,000 for each commenced day of delay in proper fulfilment of the obligation in case the Supplier breaches his obligation to remove the detected Defects and security issues discovered during the Penetration Test described in the record on the completed Pilot Operation within 20 Business Days from the day of signing of the Record or any other agreed term, pursuant to art. 4.11.6 hereof.

12.4 In case the Supplier breaches any obligation set forth in art. XIII. hereof, including the obligation to keep a confidential character of information in relation to the use of VPN system, he will pay the Customer a Contractual penalty in the amount of CZK 100,000 for each such breach.

12.5 In case the Customer fails to pay the Supplier a legitimately invoiced Price for the Ordered Work within the maturity period set forth herein, the Supplier is entitled to claim a late payment interest in the amount of 0,02% of the outstanding amount for each, even commenced, day of such delay.

12.6 If one fact results in a breach of more articles hereof and therefore the Supplier's obligation to pay the Contractual penalty should be constituted pursuant to two or more provisions of art. 12 hereof, the Supplier will pay to the Customer the Contractual penalty only according to the provision of art. 12 hereof which constitutes the obligation to pay higher Contractual penalty.

12.7 The total Contacting penalties and penalties claimed by the Customer pursuant to this Agreement shall not exceed in aggregate the amount of CZK 30,000,000.

12.8 Limitation of liability

The total liability of the Supplier towards the Customer and other party on any and all claims, whether in contract, warranty, tort (including negligence of any degree), or otherwise arising out of, or resulting from, the Agreement, is limited to CZK 20,000,000 (in words: twenty millions Czech Crowns) (hereinafter “**Liability Cap**”). In no event, whether as a result of breach of contract, warranty, tort (including negligence of any degree), patent infringement or otherwise shall the Supplier or its subcontractors be liable for any pure financial loss, consequential or indirect damages including but not limited to: loss of profit or revenue, loss of business, anticipated savings, goodwill or reputation or data or third party claims under EC Regulation 261/2004 (or similar law applicable in other countries and/or from time to time in force including in all cases any amendment thereto or replacement thereof) for loss or damage or other compensation, loss of use of the goods or system, facilities, services, downtime costs, costs to prevent or mitigate these kind of damages or claims from the Customer's business relations regarding such losses or damages. The aforementioned limitation does not apply in case of:

12.8.1 Material damages to property of Customer, as well as the consequential damages resulting from the material damage that is covered under the General Third Party Liability Insurance of the Supplier with a higher cover than CZK 20,000,000 (in words: twenty millions Czech Crowns) per year. In that case the liability of the Supplier is limited to the paid out amount under said insurance;

12.8.2 compensation for harm caused to the natural rights of an individual;

12.8.3 a claim under this Agreement that is due to willful misconduct and/or gross negligence of the Supplier.

XIII. CONFIDENTIAL INFORMATION

13. The Parties have agreed that all information which will be marked by the disclosing Party as "confidential" and all information processed or accessible by the System will be kept in secrecy by the receiving Party (hereinafter only as **"Confidential Information"**).

13.1 The Parties have agreed that the receiving Party will not disclose the Confidential Information of the disclosing Party to any third parties and he 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:

13.1.1 the receiving Party has an opposite obligation by the operation of law; and/or

13.1.2 the receiving Party discloses such information to persons who have a confidentiality obligation by the operation of law, providing that the receiving Party informs the disclosing Party in writing to which third party the Confidential Information has been disclosed and makes sure that such a third party is committed under the same confidentiality obligation which bounds the receiving Party himself.

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

13.1.4 the disclosing Party has granted his previous written consent to disclosure of the specific Confidential Information.

13.2 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.

XIV. NOTICES

14. All and any notices or documents which are to be made in writing in accordance with this Agreement must be delivered personally or mailed as a registered mail to the contact data of the other Party. Contact data are contained in the Annex No. 1 hereto.

14.1 The communication other than stated in art. 14 hereof may be made by any of the Parties vis-a-vis the other Party via email or fax to the contact data of the other Party.

14.2 Either Party is entitled to change its contact data by sending a written notice to the other Party.

XV. OTHER PROVISIONS

15. Neither Party may assign, not even partially, any of its rights from this Agreement to a third party without a prior written consent of the other Party.

15.1 The Parties have expressly and irrevocably agreed that

15.1.1 The Supplier may not in any way pledge any of its receivables in the Customer arising under this Agreement.

15.2 The Supplier as the Party in relation to which the Customer's rights as a creditor under this Agreement are time barred extends by this explicit declaration the limitation period of the creditor’s rights ensuing from this Agreement to five (5) years.

15.3 The Supplier is obliged to arrange for and keep throughout the Initial Term and, if extended, the Extended Term of this Agreement the insurance for all liabilities for damage caused by Supplier in connection with the Services with the minimum amount of CZK 100,000,000 (in words: one hundred million Czech crowns). Such insurance shall cover also the damage caused by an interruption of the Supplier’s business activities

15.4 No later than three (3) Business Days from the Supplier’s receipt of written request of the Customer the Supplier undertakes to submit to the Customer (i) an insurance certificate; or (ii) certified copy of the relevant insurance policy; or (iii) a corresponding certificate of an insurance company certifying the conclusion of an insurance policy (insurance policies) in compliance with the relevant provisions hereof (hereinafter the “**Proof of Insurance**”).

15.5 If the Supplier fails to submit the Proof of Insurance to the Customer within the deadline specified in Article 15.4 hereof, the Customer may claim from the Supplier and the Supplier is required to pay to the Customer a contractual penalty in the amount of CZK 10,000 (ten thousand Czech crowns) for every commenced day of delay with fulfilment of such obligation. The contractual penalty shall be paid within 3 (three) days from the delivery of the Customer’s request for the payment of the contractual penalty to the Supplier. The Supplier shall use its identification number (IČO) for the payment variable symbol.

XVI. INTELLECTUAL PROPERTY RIGHTS

16. At the Effective Date of this Agreement, each Party hereby warrants to the other Party that to the best of its knowledge, in the case where Supplier is the warrantor, the System or any other performance provided by the Supplier under this Agreement or the use of the System by the Customer or any Authorized Person under this Agreement and in the case where Customer is the warrantor, the Customer IPR described in Article 6.3.4, does not violate and will not result in the violation of any intellectual property rights of third parties. Intellectual property right means all patents, copyrights, design rights, trade marks, company and business names, protected designations of origin, copyright-related rights, special rights of a database producer, trade secrets, know-how and any and all other intellectual property rights of any nature (whether or

not registered), including any registration applications and exclusive rights to apply for the protection of any of the above anywhere in the world.

16.1 Each Party (an "**Indemnitor**") shall indemnify and defend the other Party and its affiliates and its and their officers, directors, employees, agents, representatives, successors and assignees (each an "**Indemnitee**") against any and all losses finally awarded by a court or arbitral tribunal or agreed by the Indemnitor in settlement arising from;

16.1.1 subject to Article 16.4.1, any third party claim that any use by an Indemnitee (or any of its Authorized Persons), in accordance with this Agreement, of materials or Services supplied pursuant to this Agreement by the Indemnitor infringes any IPR of a third party; or

16.1.2 subject to Article 16.4.1, where Customer is the Indemnitor, any third party claim that any use, other than in accordance with this Agreement, by Customer or any Authorized Persons of materials or Services supplied by Supplier pursuant to this Agreement, infringes any IPR of a third party; or

16.1.3 subject to Article 16.4.1, where Supplier is the Indemnitor, any third party claim that any use, other than in accordance with this Agreement, by Supplier or its subcontractor of documents, information, materials supplied to the Supplier pursuant to this Agreement, infringes any IPR of a third party.

16.2 The Indemnitor shall have no liability under the indemnity granted in Article 16.1 to the extent that any third party claim arises as a result of:

16.2.1 modifications made by the Indemnitee or its sub-contractors;

16.2.2 the Indemnitee's combination of the Indemnitor's services, work product, software or materials with items not provided for under this Agreement;

16.2.3 a breach of this Agreement by the Indemnitee;

16.2.4 failure of the Indemnitee immediately to use corrections or modifications provided by the Indemnitor offering equivalent features and functionality (except where the correction or modification provided by the Indemnitor does not relate to such failure); or

16.2.5 documents or materials provided by the Indemnitee.

16.3 As a part or full alternative to indemnifying any Indemnitee in accordance with Article 16.1.1, Supplier may, in its sole discretion, perform one or more of the following to minimize or eliminate the disturbance to such Indemnitee's business activities, if it becomes aware of any claim for IPR infringement under the Agreement:

16.3.1 obtain for the Customer the right to continue using any infringing Services, materials, equipment or software; or

16.3.2 modify the item(s) in question so that it is no longer infringing, and the Customer shall implement any such modifications immediately; or

16.3.3 replace such item(s) with a non-infringing replacement item without loss of functionality, and the Customer shall implement any such replacements immediately; or

16.3.4 if, having taken the action referred to in one or more of Articles 16.3.1, 16.3.2 or 16.3.3, the infringement has not been brought to an end, cease to provide the affected infringing Services or deliverables (or require the Customer to cease such use), and if this has a material adverse impact on the Services or materials provided, Supplier shall pay a reasonable refund to Customer,

and any amounts recoverable pursuant to the indemnity set out in Article 16.3.1 shall be reduced to the extent that the losses incurred by the Customer are reduced as a result of any of the above actions by Supplier.

16.4 With respect to all third party claims, in respect of which either party has agreed to indemnify the other party under this Agreement, the following procedures shall apply:

16.4.1 As soon as practicable after the Indemnitee receives notice of any third party claim qualifying for an indemnity under this Agreement, it shall notify the Indemnitor. Within thirty (30) days of being so notified (but no later than ten (10) days before the date on which any response to a complaint is due), the Indemnitor may assume control of the defence and settlement of that third party claim by giving a "Notice of Election". The Indemnitee shall provide to the Indemnitor reasonable assistance relating to any third party claim at the Indemnitor's reasonable request and cost.

16.4.2 The amount due pursuant to the relevant indemnity shall be reduced by the extent to which the Indemnitee has made any admissions (save where required by court order or governmental regulations), in relation to the third party claim, without the prior written approval of the Indemnitor and such admissions prejudice the Indemnitor.

16.4.3 the Indemnitor shall not settle or compromise any third party claim, if such compromise or settlement:

would assert any liability against the Indemnitee or impose any obligations or restrictions on such Indemnitee, such as imposing an injunction or other equitable relief upon the Indemnitee; or

does not include the third party's release of the Indemnitee from all liability relating to such third party claim.

16.4.4 If the Indemnitor does not deliver a Notice of Election pursuant to Article 16.4.1, fails to defend the third party claim in time, or ceases to defend the third party claim, the Indemnitee shall have the right to defend the third party claim in such manner as it may deem appropriate.

The indemnity in Article 16.1 is the Indemnitor's sole obligation and liability under or in connection with this Agreement, and the Indemnitee's sole remedy, in respect of claims by third parties relating to infringement of their IPR.

16.5 The warranty granted by the Supplier under clause 16.1 hereof shall be valid for this Agreements Effectivity.

XVII. FINAL PROVISIONS

17. Should any of the provisions hereof become invalid or unenforceable, the validity and enforceability of the remaining provisions hereof shall not be affected. The Parties agree to

replace an invalid or unenforceable provision with a new provision which shall correspond in its wording to the objective expressed by the original provision and this Agreement as a whole.

Force Majeure.

17.1 Neither Party will be considered late with fulfilling its obligations arisen from the Agreement 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 Agreement. 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.

Events of Force Majeure mean such circumstances that could not have been foreseen by the Party at the time of execution of the Agreement and that objectively prevent the Party from performing its obligations arisen from the Agreement. 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 Supplier's or the Contractor's business partners vis-à-vis the Contractor, strikes of employees of the Supplier and the Supplier's business partners, as well as insolvency, heavy indebtedness, bankruptcy, composition, winding up or the occurrence of other similar event related to the Supplier or any of the Supplier's business partner and the execution of the assets of the Supplier or any of the Supplier's business partners.

17.2 Should any of the events of Force Majeure occur as described in previous article 17.1. hereof, the Party on which 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 Agreement as soon as possible with respect to the circumstances that caused such event of Force Majeure. The Party shall inform the other party of the occurrence of any even of Force Majeure without undue delay after such communication becomes objectively possible.

17.3 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 occurred.

17.4 If either of the Parties disregards or excuses any non-fulfilment, breach of, delay or non-compliance with any of the obligations arising here from, such conduct shall not give rise to the waiver of such obligation in relation to its lasting or subsequent non-fulfilment, breach or non-compliance and no such waiver of right shall be deemed effective unless expressed in writing for each single case.

17.5 Where the Supplier is supposed to pay the Customer any financial amount which bears an interest, the Parties have expressly agreed that in such cases it is possible to demand interest on interest.

17.6 This Agreement and the relationships ensuing here from shall be governed by the legal order of the Czech Republic, in particular Civil Code.

17.7 Pursuant to Section 1765(2) of Civil Code the Supplier assumes the risk of material change of circumstances which may give rise to a gross disproportion in the rights and obligations of the Parties. Thus the Supplier will not have the right to seek the renegotiation of the Agreement in the event of such material change of circumstances pursuant to Section 1765(1) of Civil Code or the right to file with a court a motion for the change of an obligation under the Agreement in accordance with the provision of Section 1766 of Civil Code.

17.8 With regard to the fact that the Agreement is entered into between entrepreneurs in the course of their business the Parties have also agreed in accordance with the provision of Section 1801 of Civil Code that for the purposes of this Agreement the provisions of Section 1799 and Section 1800 of Civil Code on standard Agreements shall not apply.

17.9 The Parties have agreed that the payment of a Contractual penalty by the Supplier shall not affect the Customer's right to demand full compensation of damage to the limit set in art. 12.8. hereof. If any legal regulation lays down a fine (penalty) for the breach of a Contractual obligation (at any time during the Initial Term and if extended the Extended Term of this Agreement), such claim shall be without prejudice to the Customer's entitlement to a full compensation of damage. If the Supplier causes any non-material harm to the Customer, the Supplier is obligated to compensate for the harm.

17.10 The Parties have not agreed an advance payment under Sections 1808 and 1809 of Civil Code. However, for the avoidance of any doubt the Parties state that no performance provided by the Customer shall be regarded as an advance.

17.11 For the avoidance of doubt the Parties have agreed that a pecuniary debt under this Agreement may not be settled by using an exchange note.

17.12 In the event of the breach of several articles of this Agreement by a single circumstance, which would give rise to the Supplier's obligation to pay a Contractual penalty under two or more provisions hereof, the Supplier shall only pay the Customer the Contractual penalty under that provision of this Agreement which gives rise to the obligation to pay a higher Contractual penalty.

17.13 For the avoidance of any doubt, an obligation under this Agreement is not a fixed obligation as defined in Section 1980 of Civil Code.

17.14 The provisions of Section 1932 and Section 1933 of Civil Code shall not apply to this Agreement. If there are several due obligations arising from this Agreement, then the Parties agree to discuss in good faith to determine which of the obligations is to be fulfilled primarily.

17.15 This Agreement contains the entire arrangement on the subject-matter of this Agreement and all the matters which the Parties were supposed and wished to agree in the Agreement and which they consider important for this Agreement to be binding. Neither declaration of will of the Parties made during the negotiations on this Agreement nor declaration of will made after the entry into this Agreement may be interpreted in conflict with the explicit provisions of this Agreement and gives rise to any obligation of any of the Parties. This Agreement substitutes all other written or oral agreements made with regard to the subject-matter of this Agreement.

17.16 The Parties expressly agree that the Supplier's general or other similar terms and conditions shall never apply to the relationships defined or envisaged by this Agreement, not even if such terms and conditions are part of the communication between the Parties.

17.17 The Customer informs the Supplier and the Supplier is aware that the Customer is a person listed in Section 2 Subsection 1 Letter n) of Act no. 340/2015 Coll., on Special Conditions for the Effectiveness of Certain Agreements, the Disclosure of These

Agreements and on the Register of Agreements (Act on the Register of Agreements). This Agreement will be published in the register of Agreements. The Parties hereby agree that unit prices stated in this Agreement and its annexes constitute a business secret under Section 504 of Civil Code. The Parties declare that no other facts stated in this Agreement and its annexes constitute a business secret under Section 504 of Civil Code.

17.18 The Parties have agreed that they do not wish for any rights and obligations beyond the scope of the explicit provisions of this Agreement to be inferred from the current or future practice established between the Parties or the usage applied generally or in the sector concerning the subject-matter hereof, unless expressly agreed otherwise in this Agreement. In addition to the above, the Parties confirm to each other that they are not aware of any business usage or practice established between them.

17.19 The Parties have informed each other about all facts and legal circumstances of which they were aware or had to be aware as of the date of the signature hereof and which are relevant for the entry into this Agreement. Apart from the assurances mutually given by the Parties herein, none of the Parties shall have any other rights and obligations in connection with any facts which are revealed and of which the other Party was not informed during the negotiations on this Agreement. This applies with the exception of cases when a given Party has intentionally misled the other Party in respect of the subject-matter of this Agreement.

17.20 The Parties agree to settle all disputes arising between them in connection with the performance or interpretation of this Agreement amicably and by mutual agreement. If they fail to settle a given dispute within thirty (30) days from its occurrence, such dispute shall be brought by one of the Parties to the court having the subject-matter and local jurisdiction. The Parties hereby agree on the local jurisdiction of the general court of the Customer pursuant to Section 89a of Act no. 99/1963 Coll., Civil Procedure Code, as amended by later regulations.

17.21 This Agreement may only be changed and supplemented by way of written serially numbered amendments signed by both Parties.

17.22 This Agreement is drawn up in four (4) counterparts with the validity of original, of which the Supplier shall receive one (1) counterpart and the Customer shall receive three (3) counterparts. This Agreement is entered into in the English language.

17.23 This Agreement contains as its integral part all the annexes listed below:

17.23.1 Annex No. 1 – Contacts

17.23.2 Annex No. 2 – CUPPS/CUSS System Functional and Technical Specification

17.23.3 Annex No. 3 – Service Fee, Price list

17.23.4 Annex No. 4 – Cyber security requirements

17.23.5 Annex No. 5 – CUPPS/CUSS System description

17.23.6 Annex No. 6 – Implementation Time Schedule

17.23.7 Annex No. 7- List of airline systems to implement

17.23.8 Annex No. 8 – Standard warranty exclusions

THE PARTIES HEREBY DECLARE THAT THEY HAVE READ THIS AGREEMENT AND AGREE WITH ITS CONTENT, IN WITNESS WHEREOF THEY ATTACH THEIR SIGNATURES.

Date:	5.10.2020	Date:	
For the Customer:		For the Supplier:	
Signature:	___________________________	Signature:	___________________________
Name:	Ing. Václav Řehoř, PhD., Chairman of the Board of Directors	Name:	Ing. Michal Koscelansky, Country representative
Office:	Letiště Praha, a.s.	Office:	SITA B.V.

Signature: ___________________________

Name: Ing. Jiří Černík, Member of the Board of Directors

Office: Letiště Praha, a.s.

Annex No. 1 – Contacts

Mailing address:

(a) Address for delivery to the Customer:

Letiště Praha, a.s.
K letišti 1019/6, Prague 6, 160 08
Czech Republic

attn: Airport Operation Systems Manager

(b) Address for delivery to the Supplier:

SITA B.V.
V Parku 2336/22
148 00 Prague 4

Responsible persons:

The representative authorized to represent **the Supplier's party in Contractual matters** related to perfo[redacted]

[redacted]

The representative authorized to represent **the Supplier's party in technical matters** related to perfo[redacted]

[redacted]

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

[redacted]

[redacted]

The representative authorized to represent **the Customer's party in technical matters** related to performance hereof and in the matters of Assignments, Offers and Orders will be:

[redacted]

Contact data in case of fire, leakage of unknown substances or another emergency situation:

Operation Centre of Fire Protection

Unit of the Fire Brigade:	3333, 2222
Ambulance:	3301, 3302
Safety control center:	1000

In case of any inquiries or ideas for improvement aimed to the particular areas:

(a)	Occupational Health and Safety:	bozp@prg.aero
(b)	Environment:	zivotni.prostredi@prg.aero
(c)	Fire prevention:	technik.po@prg.aero
(d)	Complaints:	stiznosti@prg.aero
(e)	ID cards:	karty@prg.aero

Customer's contacts – authorized persons in the matters of resolving Errors, Defects and Adaptations

Name	Email	Telephone	Mobile

Customer's escalation contacts:

Order	Person	Email	Telephone
1			
2			

Customer's escalation procedure:

In order to provide for a smooth solution of Errors, the Supplier's Support Centre with the above mentioned contacts is determined as a contact point. In case of any doubts on the Customer's part regarding the method of solution of the problem, it is possible to address the following Supplier's contact persons for the purpose of the problem escalation:

Order	Contact	Person	Telephone	Escalation cause
1	Technical Support On duty person		[redacted]	operational issues, problems reporting
2	[redacted]	[redacted]	[redacted]	escalations
3	[redacted]	[redacted]	[redacted]	escalations
4	[redacted]	[redacted]	[redacted]	escalations

Passenger Processing System CUPPS/CUSS - Minimal technical conditions

This document contains the minimum technical conditions for the performance of a public contract, which must always be respected by the tenderer.

The tenderer will complete this table in accordance with its tender and submit it to the Contracting Authority as part of its pre-bid.

Detailed details and technical parameters are given in the Functional and technical specification.

Note: Please note that all cross references refer to the Proposal submitted on 17th of April 2020

Feature section in FTS	**Description of the requirements**	**Solution compliance (Y/N)**	**Note**
	CUPPS		
3.1.2	Solution certified for IATA CUPPS v1.03 standard	Y	Compliant. Please refer to Annex 2 and 3 CUPPS Certificate and Section 2.3 Standards, Continued Improvement and Technology Innovation
3.1.3	Scalable system architecture, ensuring that that an increase in system size (i.e. adding new workstations – at least up to 500 pieces) will not adversely affect the system performance.	Y	Fully Compliant Please refer to Section 2.6.9 Core System Design
3.1.4	Ability to run CUPPS, CUTE and other applications on common use workstations (WKS) to maximize the use of the terminal infrastructure.	Y	Fully Compliant Please refer to Section 2.5 Access IT applications in real time from any shared equipment
3.1.6	Solution must be able to run all airline applications listed in Annex no. 1.	Y	Compliant Please refer to Annex F Win10 App Inventory
3.1.7	Solution must be able to deploy and run LKPR's internal applications listed in Annex no.2.	Y	Fully Compliant All applications requested in Annex C LKPR's Applications of the Tender documents are supported by the AirporConnect Platform
3.1.9	Ability to deploy new CUPPS/CUTE or other applications, including their regular updates or patches.	Y	Fully Compliant Please refer to Section 2.8.1 Modular, reliable, intuitive
3.1.10	Capability of running multiple applications in parallel on a single WKS and under one user account, with the possibility to use connected printers or other peripheral devices.	Y	Fully Compliant Please refer to Section 2.6.2 Multiple Concurrent Applications
3.1.11	Possibility of a customized WKS configuration with regards to used peripheral devices, to be able to create unique end user workplace according to	Y	Fully Compliant Pleast refer to Section 2.6.7 The CUTE Intelligent Workstation (IWS)

	particular location needs (check-in, gate, back-office etc.). The system will also allow to share resources (peripheral devices), that are physically connected to one WKS, with other WKS(s).		
3.1.12	System must support 24/7 operation, designed with full redundancy and no single point of failure.	Y	Fuly Compliant Please refer to Section 2.6.1 Redundancy and Resilience allows for high availability and speedy recovery
3.1.14	System must support user account management, allowing setting of configurable user accounts, groups and roles. The user access to the system must be secured with user ID and a password.	Y	Fuly Compliant Please refer to Section 2.6.4 System Security
3.3	System must support operational data availability and exchangeability, as stated in 3.3.1 – 3.3.3	Y	Fully Compliant Please refer to Sections 2.9.6 Statistics and Reporting and 2.14.1 Introduction
	CUSS		
4.1.1	Solution in accordance with IATA RP1706c, allowing multiple airlines to operate the kiosks using airline CUSS compliant applications.	Y	Fully Compliant Please refer to Section 2.3 Standards, Continued Improvement and Technology Innovation
4.1.3	Customizable common launch screen (CLA).	Y	Fully Compliant Please refer to Section 2.8.1 Modular, reliable, intuitive
4.1.5	Solution supporting min. CUSS standard 1.3	Y	Fully Compliant Please refer to Annex 01_CUSS 1.4 certificate APC Open
4.1.6	Ability to deploy new CUSS or other applications, including their updates or patches.	Y	Fullly Compliant Please refer to Section 2.8.1 Modular, reliable, intuitive
4.1.10	Branding of all or each individual kiosk shall be customizable according to LKPR requirements.	Y	Fully Compliant Please refer to Section 2.8.4 Branding and design
4.3	System must support operational data availability and exchangeability, as stated in 4.3.1 – 4.3.2	Y	Fully Compliant Please refer to Sections 2.9.6 Statistics and Reporting and 2.13.2 Reported Data

Annex No. 3 – to be inserted by the Supplier as Appendix H – Sheet Service Fee and Price list

Price Breakdown - tender price calculation		
Provision of Initial Hardware Delivery	**Quantity**	[redacted]
WKS or terminals	425	[redacted]
Monitors 17"	70	[redacted]
Monitors 19"	351	[redacted]
Monitors 24"	4	[redacted]
MSR/OCR keyboards	330	[redacted]
Standard keyboards	95	[redacted]
Document printers	85	[redacted]
ATB	275	[redacted]
BTP	250	[redacted]
BTP with RFID	10	[redacted]
BGR	135	[redacted]
Check-in BCR	190	[redacted]
CUSS check-in kiosks	35	[redacted]
Total Monthly Hardware Leasing Fee, according to article 10.1 of the Agreement, for thirty six (36) consecutive months during the Initial Term	Price (CZK/month) without VAT	[redacted]
Minimum Monthly Service Fee, according to article 10.2 of the Agreement	**Price (CZK/month) without VAT**	[redacted]
Total monthly Service Fee, in the first thirty six (36) consecutive months during the Initial Term	Price (CZK/month) without VAT	[redacted]
Total monthly Service Fee, in the last twenty four (24) consecutive months during the Initial Term	Price (CZK/month) without VAT	[redacted]
Basic Monthly Passenger Limit, according to article 10.2 of the Agreement (if applicable)	**Passengers per month**	[redacted]
Passenger Fee, according to article 10.3 of the Agreement	**Fee CZK per passenger without VAT**	[redacted]

[redacted]

Following items are not part of the guaranteed service delivery. They represent expected, but not guaranteed future service extension and they are stated only for the purpose of offer evaluation process:

Additional items	Quantity	[redacted]
WKS or terminals	25	[redacted]
Monitors 19"	25	[redacted]
MSR/OCR keyboards	25	[redacted]
Document printers	5	[redacted]
ATB	25	[redacted]
BTP	25	[redacted]
BTP with RFID	10	[redacted]
BGR	20	[redacted]
Check-in BCR	20	[redacted]
CUSS check-in kiosks	5	[redacted]
CUSS payment terminal extension	40	[redacted]
CUSS biometric camera/senzor extension	40	[redacted]
Man-hours	120	[redacted]
		[redacted]

fields to be filled by the Supplier

* expected numbers of passengers boarded per month for the purpose of making evaluations (actual numbers may vary)

** Calculation of the corresponding price per month will be based on the following formula: Price (CZK/month) = (Variable price*60/30) + Fixed price)* Quantity Variable and Fixed price values should correspond with the values stated in the **Price list.**

*** Calculation of the corresponding total price is based on the following formula: Total Price = Price (CZK/month) * 30

[redacted]

Service Fee

Provision of the Intial Hardware Delivery	**Quantity**	[redacted]
WKS or terminals	425	[redacted]
Monitors 17"	70	[redacted]
Monitors 19"	351	[redacted]
Monitors 24"	4	[redacted]
MSR/OCR keyboards	330	[redacted]
Standard keyboards	95	[redacted]
Document printers	85	[redacted]
ATB	275	[redacted]
BTP	250	[redacted]
BTP with RFID	10	[redacted]
BGR	135	[redacted]
Check-in BCR	190	[redacted]
CUSS check-in kiosks	35	[redacted]
Total Monthly Hardware Leasing Fee, according to article 10.1 of the Agreement, for thirty six (36) consecutive months during the Initial Term	Price (CZK/month) without VAT	[redacted]
Minimum Monthly Service Fee, according to article 10.2 of the Agreement	**Price (CZK/month) without VAT**	[redacted]
Total monthly Service Fee, in the first thirty six (36) consecutive months during the Initial Term	Price (CZK/month) without VAT	[redacted]
Total monthly Service Fee, in the last twenty four (24) consecutive months during the Initial Term	Price (CZK/month) without VAT	[redacted]
Basic Monthly Passenger Limit, according to article 10.2 of the Agreement (if applicable)	**Passengers per month**	[redacted]
Passenger Fee, according to article 10.3 of the Agreement	**Fee CZK per passenger without VAT**	[redacted]

Price list

Hardware item CUPPS	Quantity	[redacted]
WKS or terminal	1	[redacted]
Monitor 17"	1	[redacted]
Monitor 19"	1	[redacted]
Monitor 24"	1	[redacted]
MSR/OCR keyboard	1	[redacted]
standard PC keyboard	1	[redacted]
standard PC mouse with a mouse pad	1	[redacted]
Document printer	1	[redacted]
ATB	1	[redacted]
BTP	1	[redacted]
BTP with RFID	1	[redacted]
BGR	1	[redacted]
Check-in BCR	1	[redacted]
Mobile WKS according to 3.1.25	1	[redacted]

Hardware item CUSS	Quantity	[redacted]
CUSS check-in kiosk	1	[redacted]
Optional lightweight kiosk version according to 4.1.11	1	[redacted]
CUSS payment terminal extension	1	[redacted]
CUSS biometric camera/senzor extension	1	[redacted]

The calculation of the corresponding price per month will be based on the following formula:
Monthy fee = (Variable price*60/Remaining Months till the end of contract) + Fixed price

Support item	Quantity	[redacted]
Man-hour	1	[redacted]

Other items	Quantity	[redacted]
Price for maintaining the connection between CUPPS/CUSS platform and airline DCS host connection (if applicable, e.g. If the connection is not established separately at the airport, but between the DCS host and the Supplier's datacenter)	1	[redacted]

Annex No. 4 – Cyber security requirements

SECURITY MEASURES

Pursuant to Section 4 (4) of Act No. 181/2014 Sb., on cyber security and on amendments to relating acts (the Cyber Security Act), as amended (hereinafter referred to as the "**Act**"), in conjunction with Annex 7 to Regulation No. 82/2018 Sb., on security measures, cybernetic security incidents, reactive measures, cyber security reporting requirements and data disposal (Cyber Security Regulation) (hereinafter referred to as the "**Regulation**), The purpose of this Annex is to specify binding security measures applicable to the Supplier whose supplies for the Customer as described in this Agreement include any development, implementation and/or servicing of software or hardware (hereinafter also referred to as "**SW**" and "**HW**" respectively), and/or which, in connection with the supply, accesses the Customer's information system that was classified as an essential service information system pursuant to Act No. 181/2014 Sb., (hereinafter also referred to as "**PA BIS"),** and/or which processes and/or transmits and/or stores and/or archives information and operating data of the Customer and/or its customers (hereinafter also referred to as the "**Security Measures**").

1. GENERAL REQUIREMENTS

1.1 When providing supplies for the Customer, the Supplier shall fulfil the following obligations:

1.1.1 The Supplier shall act in compliance with applicable legislation applicable to it generally as a provider of information technology services, including the requirements arising for the Customer as the administrator and operator of the essential service information system, and arising from the Act and Regulation. Supplier shall take account of any amendments to legislation and/or new legal regulations, if applicable provided however Supplier is not responsible for the requirements of regulations or laws applicable to Customer's business (including those relating to Work or Services that Customer acquires under this Agreement), or whether Suppliers' provision of or Customer's receipt of particular Work or Services under this Agreement meets the requirements of such regulations or laws. The Parties shall negotiate in good faith to agree a change of the Work or Service by signed written amendment (including to govern any development work), subject to agreement by Customer to pay any charges related to such change of Work or Service.

1.1.2 Unless otherwise agreed by the parties, the Supplier shall appoint a responsible Contact Person within 3 days after concluding the Agreement in order to ensure the compliance with the Security Measures arising from the Agreement and to ensure communication between the Parties (hereinafter also referred to as the "**Contact Person**"). The Supplier shall notify the Customer of the Contact Person within the same deadline. The Customer shall be notified of any change of the Supplier's Contact Person within 5 days after such change.

1.1.3 The Supplier shall ensure that the Contact Person confirms the Customer no later than 30 days after concluding the Agreement, that any and all persons involved in the supply under this Agreement for the Supplier and/or its subcontractors have demonstrably been informed of these Security Measures.

1.1.4 Whenever the supply under the Agreement involves processing of personal data for the Customer by the Supplier, the Supplier shall enter into a personal data processing agreement pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and on repealing Directive 95/46/EC (General Data Protection Regulation);

1.1.4 a) (Data Privacy)

"Data Processing Subcontractor" means any processor engaged by Supplier in the Processing of Personal Data.

"Data Protection Legislation" means all applicable laws and regulations relating to the Processing of Personal Data and privacy including the GDPR and the laws and regulations implementing or made under them and any amendment or re-enactment of them.

"Data Subject" means an identified or identifiable natural person.

"General Data Protection Regulation" or **"GDPR"** means regulation EU 2106/679/EC on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data and repealing Directive 95/46/EC.

"Instructions" means the Services as described in the Agreement shall be considered to be instructions of the Customer to Process Personal Data.

"Personal Data" means any information that relates to an identified or identifiable living individual.

"Personal Data Breach" means a breach of Supplier's security commitments set out in this Agreement leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Supplier in connection with this Agreement.

"Process or **Processing"** of Personal Data means the use, collection, storage, Processing, modification, transfer, blocking or erasure of Personal Data by Supplier on behalf of Customer.

(i) In the provision of the Services, Supplier shall Process Personal Data on behalf of Customer. This Processing includes such activities as specified in the service descriptions under this Agreement. Under this Agreement, Customer remains responsible for the compliance with provisions of Data Protection Legislation.

(ii) Supplier shall only Process Personal Data in accordance with the Instructions of Customer except to the extent that any applicable law prevents Supplier from complying with such Instructions or requires the Processing of Personal Data other than as instructed by Customer.

(iii) Customer acknowledges that in the provision of the Services, Supplier may transfer Personal Data to locations outside the European Economic Area in accordance with applicable Data Protection Legislation.

Supplier shall ensure that any personnel authorized by Supplier to access the Personal Data are subject to a duty of confidentiality in respect of the Personal Data.

(iv) Supplier shall ensure that any Processing of Personal Data is subject to appropriate technical and organizational measures against unauthorized or unlawful Processing of the Personal Data and against accidental loss or destruction of, or damage to, the Personal Data in accordance with applicable Data Protection Legislation applicable to Supplier.

Subcontractors

v) Supplier shall inform Customer of the Data Processing Subcontractors used in the Processing of Personal Data as at the effective date of this Agreement. Supplier shall inform Customer of any changes to the Data Processing Subcontractors used in Processing of Personal Data made after the effective date of this Agreement. Where Supplier engages Data Processing Subcontractors, it shall impose the Personal Data Processing obligations set out in this clause on such Data Processing Subcontractors. Customer hereby grants Supplier a general written authorization to engage Data Processing Subcontractor in the Processing of Personal Data in accordance with the provisions set out in this Clause.

vi) Supplier shall inform Customer of any requests or queries from a Data Subject, regulatory authority or any other law enforcement authority regarding Processing of Personal Data under this Agreement and provide Customer with any information and assistance (at Customer’s cost) that may reasonably be required to respond to any such requests of queries.

vii) Supplier shall provide reasonable assistance to Customer (at Customers cost) in respect of the customers compliance with Articles 32 – 36 of the GDPR, taking into account the nature of the Processing undertaken by Supplier and the information available to Supplier.

viii) Supplier shall at the choice of Customer, delete or return all Personal Data to the Customer after the end of the provision of the Services relating to Processing unless Supplier is required to retain the Personal Data by applicable law.

viiii) Supplier shall notify Customer without undue delay on becoming aware of a Personal Data Breach;

x) Supplier shall make available to Customer information reasonably necessary to demonstrate compliance with Supplier’s Personal Data Processing obligations under this Agreement.

xi) The Customer warrants, represents and undertakes that it has all necessary consents, approvals or licenses to:

- Make Personal Data available to Supplier for the purposes of this Agreement and for Supplier to Process Personal Data as envisaged in this Agreement;

- Permit the Customer to access Personal Data using the Supplier platform as envisaged in this Agreement; and

- to permit Supplier and its Data Processing Subcontractors to transfer Personal Data to locations outside the European Economic Area as necessary for the performance of the Services as envisaged in this Agreement in accordance with applicable Data Protection Legislation.

xii) Customer data (if any) in Supplier's control shall be accessible by Customer via its user interface.

xiii) Customer shall be solely responsible for the Customer data and for procurement of any approvals or consents or licenses relating to the collection, Processing or use of such Customer data by or on behalf of Supplier. Supplier is not required to validate the Customer data for correctness or usability nor process Customer data if such Processing will or is likely to render Supplier, its affiliates or their personnel in breach of any applicable law.

xiv) Notwithstanding the foregoing, Supplier and/or its affiliates may gather, compile, commingle, and use Customer data for aggregate statistical or analytical purposes and/or for evaluation of its provision and the use of the Services. Such aggregate data may be used by Supplier for financial, accounting, product optimization, customer support, and other internal business purposes. Aggregate or derivative data and information may be used by Supplier as input for business intelligence solutions sold to third parties, provided that such data and solutions do not contain any Personal Data and do not directly or indirectly identify Customer. Supplier and its affiliates shall have all rights to those aggregated or derivative data and business intelligence solutions.

1.1.5 The supply may not be inadequate in terms of information security, where the term "inadequate" means any supply that contains technologies/key elements against the Supplier's own security policies and compliance with Act. Supplier complies with information security and quality control industry recognized standards as accredited through certificates, attestations and reports issued by independent third party authorities (e.g. auditors) such as ISO27001 as attached to Supplier's response to Customer's request for proposal relating to this Agreement. During the Agreement Term, if requested in writing by Customer to Supplier (annually or less frequently), Supplier will make available to Customer information reasonably necessary to demonstrate its compliance with regards to such standards. If Customer, acting reasonably, considers that such information insufficient, Customer may notify Supplier in writing providing evidence of such concerns and Supplier will endeavor to furnish Customer with information suitable to resolve Customer's concerns, provided such information is not proprietary, subject to confidentiality or restricted from disclosure generally.

1.1.6 The Supplier shall make an analysis and security risk assessment of the information infrastructure which is part of the subject-matter of the Agreement (the solution supplied hereunder) and, based on the results, it shall propose measures to minimize or eliminate any detected risks and present such measures to the Customer. Such measures must be proposed and consolidated, taking account of the risk assessment results.

1.1.7 The Supplier shall keep records of any significant facts relating to the supply provided under the Agreement (technical records, organizational records regarding trainings, authorizations, etc.) and shall inform the Customer about them;

1.1.8 The Supplier shall implement measures to protect the backup of data relating to the supply provided under the Agreement and shall test the functionality of such backup on a regular basis.

1.1.9 Whenever required by the Customer, the Supplier shall guarantee the ability to restore the functionality of the asset so that its condition complies with the Agreement.

1.1.10 The Supplier shall detect technical vulnerabilities and configuration discrepancies of the supply under the Agreement on a regular basis. Detected technical vulnerabilities must be evaluated in the light of any relating risks and the Supplier must implement corrective measures depending on the nature of the supply.

1.1.11 The Supplier shall implement security measures to protect data relating to the supply hereunder.

1.1.12 The Supplier shall fulfil any and all security requirements in development and support processes at least in the scope according to the requirements stipulated in ISO/IEC 27001 A. 14.

1.1.13 The Supplier shall store data about the operation (operational and localization data) in compliance with the applicable legislation applicable to it and shall meet all the requirements in Supplier’s own security policies applicable_to it generally as a provider of information technology services arising from the Regulation for the contents of operating incidents.

1.1.14 The Supplier shall secure any transmission of data and information in order to meet the security requirements for their confidentiality, integrity and availability throughout the provision of the supply for the Customer.

1.1.15 The Supplier shall deliver the system and operational security documentation on the day on which the SW is to be accepted at the latest and in the method specified in the agreement, at least in the scope specified by the Customer.

1.1.16 The supply shall contain only components which are objectively required for operating the SW properly and/or which are expressly specified in the agreement, the SW or HW shall not contain any unnecessary components.

1.1.17 If the supply includes any installation of the operating system, or third-party SW, only the latest security updates of such products may be used for installation.

1.1.18 Supplier implements appropriate technical and organizational measures, in compliance with industry best practices such as ISO27K and PCI DSS, to ensure a level of security appropriate to the risk for confidential information.

1.1.19 If the supply includes any installation of SW or its upgrade, the Supplier shall proceed in accordance with its ISO27001 compliance or equivalent hardening security policies.

1.1.20 The production environment of the PA BIS system shall contain only compiled or executable code, if applicable, and other data necessary to operate the PA BIS system.

1.1.21 Prior to the launch of the SW in the PA BIS production environment, the Supplier shall check the compliance of the SW with security requirements of its ISO27001 compliance or equivalent security policies and where non-compliance is detected, the Supplier shall ensure compliance of the SW with the security requirements of the policies without undue delay.

1.1.22 The Supplier shall install any new SW or new versions of SW on the basis of pre-approved migration procedures[1] on at least one affected System as agreed between the Parties in accordance with the procedure described in Article 9 adaptations.

2. REQUIREMENTS FOR SYSTEM AND OPERATIONAL SECURITY DOCUMENTATION

2.1 The supply shall include, as an integral part, the documentation of all security settings, functions and mechanisms in the form of security documentation. In connection with the supply for the Customer, the Supplier shall give the Customer documentation at least in the following scope:

2.2 Business continuity plan and disaster recovery plans

2.3 Operational and security documentation and as-built documentation

2.4 Description of authorization concept and privileges

2.5 Backup and archiving procedures

2.6 Installation and configuration procedures

2.7 Security settings

3. PHYSICAL PROTECTION AND ENVIRONMENT SECURITY

3.1 The Supplier shall comply with the operating rules of buildings (safety precautions) and leased areas, in particular as regards the physical protection of security zones where the components of the PA BIS systems and/or data carriers are located (hereinafter also referred to as the “**Site**”).

3.2 The Supplier shall not leave any installation, backup or archiving media or documentation for the PA BIS system which is the subject-matter of the supply hereunder unattended or freely available in the Site.

4. ACCESS CONTROL

4.1 The Supplier acknowledges and agrees that access to the PA BIS system may be provided only to the physical entity of Supplier’s (or Subcontractor’s) employees recorded in Identity Register kept by the Customer, on the basis of the Supplier’s access request.

4.2 The Supplier acknowledges and agrees that its employee must provide their personal data to the Customer in the scope required for opening such access, otherwise the Customer shall not be obliged to allow such Supplier’s employee to access the PA BIS system. Supplier’s employees with granted (physical, logical) access to the PA BIS system acknowledge and agree that the evaluation of movement and activities

[1] Migration procedures mean sets of steps defining the transfer of data between two or more systems of the PA BIS.

carried out in the Customer’s premises (e.g. monitoring using Security Information and Event Management) involves personal data processing.

4.3 The Supplier acknowledges and agrees that granting access privileges to any Supplier’s employee shall be governed by the principle of least privileges and that no Supplier’s employee is automatically entitled to such access.

4.4 The Supplier agrees that granted access may not be shared by multiple Supplier’s or Subcontractor’s employees.

4.5 The Supplier agrees that any remote access to the PA BIS system shall always be carried out through secure VPN connection.

4.6 Prior to connecting any terminal equipment, mobile terminal equipment or active network component, such as network switches, WiFi access points, routers or hubs, to the computer network, the Supplier shall request approval from the Customer’s Contact Person.

4.7 The Supplier undertakes to deactivate, without undue delay, any and all terminal equipment that is not used and/or any port of active network component that is not used.

4.8 The Supplier undertakes not to install or use any tools, such as Keylogger, Sniffer, Vulnerability Scanner, Port Scanner, Backdoor, rootkit and Trojan Horse or any other form of malware.

4.9 The Supplier undertakes to ensure that all its information systems that are connected to the Customer’s network infrastructure are and will be protected against malware.

4.10 The Supplier undertakes not to develop, compile or distribute any program code in any part of the PA BIS system which is intended to control, disrupt or compromise the PA BIS system illegally or to obtain data and information illegally.

4.11 The Supplier undertakes to ensure that no person engaged in the provision of supply for the Customer in the PA BIS:

4.12 stores or shares any data and information of ethically inappropriate contents contrary to morality or damaging the Customer’s reputation;

4.13 downloads, shares, stores, archives and/or installs any data or executable files in violation of the license conditions and/or copyright act;

4.14 sends chains emails.

4.15 The Supplier undertakes to ensure that security patches are applied and antivirus protections are installed, run and updated in any external devices (laptop/computer) of all the persons engaged in the provision of supply for the Customer and accessing the Customer’s internal network or PA BIS.

4.16 The Supplier undertakes to ensure that any person engaged in the provision of supply for the Customer and accessing the Customer’s internal and/or PA BIS system protect authentication means and details to the Customer’s PA BIS system. The Supplier acknowledges and agrees that if user authentication fails repeatedly, the applicable account may be blocked and considered a cybersecurity incident pursuant to the applicable documentation and applicable procedures for handling cyber security incidents may be applied (such as immediate access revocation to information assets for a natural person or an external entity). The Supplier handling a cybersecurity incident or Security Measure breach shall not be deemed Supplier's liability. With respect to any cybersecurity incident, Security Measure breach, loss of or damage to data, Supplier's sole obligations are as set forth in this Agreement and Supplier's own security processes.

5. MONITORING ACTIVITIES

5.1 The Supplier acknowledges and agrees that all its activities or supplies made or provided in the Customer's system environment shall be monitored and assessed by the Customer on a regular basis with respect to the contents of the agreement and the Customer's internal documents, of which the Supplier was made aware.

5.2 The Supplier shall monitor and record all its activities and supplies made or provided in connection with the subject-matter of the Agreement or closely relating to it. The Supplier shall provide records/logs containing results of such monitoring, successful and unsuccessful login to the PA BIS system and records on user administration, if available to the Supplier, at the Customer's request without undue delay throughout the term of the Agreement or after its termination.

6. ACCEPTANCE OF SUPPLY

6.1 The Supplier acknowledges and agrees that any failure of the Supplier to comply with the Security Measures, incl. the requirement to provide the entire System and operational documentation for the Systems operated by the Customer, is a defect preventing the acceptance of the subject-matter of the Agreement and the Customer shall not be obliged to accept the supply until such defect is removed.

6.2 The Supplier is responsible to ensure that systems supplied to the PA BIS contain most recent security patches[2].

7. INFORMATION EXCHANGE

7.1 If the subject-matter of the Agreement includes information exchange between the parties, the parties agree to negotiate in good faith to sign an agreement to protect such information, in particular in terms of its exchange, storing, archiving and in the event of agreement termination.

7.2 The Supplier undertakes to ensure that any transfers of data and information must be sufficiently secured using the most recent resilient cryptographic algorithms and cryptographic keys.

7.3 The Supplier undertakes to ensure that online transactions made using web technologies shall be protected by SSL certificates.

7.4 The Supplier is obliged to give the Customer any and all requested data, operating data and information without undue delay after the Customer's request, in systematic and machine readable form.

[2] Software updates to a higher version.

8. HANDLING CYBER SECURITY INCIDENTS

8.1 When providing supplies under the Agreement for the Customer, the Supplier undertakes to determine activities, roles and their responsibilities and powers leading to handling cyber security incidents and events rapidly and effectively. The Supplier shall proceed in accordance with such determined and described rules, and shall report any cyber security incidents and events, incl. cases of personal data security breaches to the Customer and, where feasible, after having become aware of it and having sufficient information to notify Customer. Furthermore, the Supplier shall evaluate information about cyber security incidents and events, and shall keep records about such information, cyber security incidents arisen, incl. short-term and long-term corrective measures applicable to all parts of the solution managed by the Supplier, and about risks relating to the business continuity and to keep such records for future reference with regard to the Customer's requirements.

8.2 The rules for handling cyber security incidents determined by the Supplier shall respect the requirement for the legality of collecting clues, i.e. the origin of such clues and the lawfulness of their collecting must be in compliance with the applicable legislation applicable to the Supplier generally as a provider of information technology services_so that such evidence may be used in forensic analysis and as evidence, if need be.

8.3 The Supplier shall propose such a solution so that the system of detecting and handling cyber security incidents and events is integrated in the Customer's processes and systems (*inter alia*, so that the Customer's requirements for crisis management are respected) and the Supplier shall implement measures to increase the resiliency of the information system against cyber security incidents and to limit accessibility, taking account of requirements stipulated by Supplier's own security policies.

8.4 The Supplier is obliged to notify the Customer, without delay, of any and all cyber security incidents relating to the supply under this Agreement. Such notice shall contain the description of the nature of such cyber security incident.

8.5 If a cyber security incident, or cyber security event occurs and such cyber security incident is handled and evaluated as a security incident of the Customer, the Supplier shall assist the Customer for instance by providing logs and identification details (such as IP address, MAC address, HW type, serial number, or IMEI) of the terminal equipment or mobile terminal equipment concerned, for contents analysis, and/or the Supplier shall implement measures required by the Customer, if any).

8.6 The Supplier is obliged to analyse the causes of a cyber security incident or event and to propose measures aiming to avoid its repetition if the Supplier caused such security incident or contributed to its occurrence.

9. COPYRIGHT

9.1 When performing the subject-matter of the Agreement for the Customer, the Supplier undertakes to comply with the conditions stipulated by Act No. 121/2000 Sb., on copyright and rights related to copyright and on amendments to some other acts (Copyright Act), as amended.

9.2 Further requirements are stated in the Agreement (Intellectual Property Rights).

10. AUTHORIZATION TO USE DATA

10.1 When performing the subject-matter of the Agreement for the Customer, the Supplier is entitled to use data provided by the Customer to the Supplier for the purposes of the performance of this Agreement, however only to the extent necessary to perform the subject-matter of this Agreement.

10.2 When performing the subject-matter of the Agreement for the Customer, the Supplier shall treat data in strict compliance with the Agreement and applicable legislation applicable to it (the Act, Regulation) and other related legislation applicable to the Supplier generally as a provider of information technology services.

11. CHANGE MANAGEMENT

11.1 The Customer shall review any impact of changes as part of the PA BIS change management and subject to agreement with Supplier to which will be included into Annex 4, shall determine significant changes pursuant to the Regulation.

11.2 With respect to significant changes, the Customer documents their management, makes a risk analysis, implements measures to reduce adverse impacts of significant changes, makes updates to security policy and security documentation, ensures PA BIS testing and ensures the option of returning to the original condition.

11.3 The Customer is obliged to inform the Supplier of the results of the management of changes which have impacts on the performance of the subject-matter of the Agreement by the Supplier.

11.4 The Supplier is obliged to take effective measures in order to reduce adverse impact in compliance with the results of the management of changes referred to in cl. 11.3 which have been agreed with Supplier.

11.5 The Supplier shall provide the Customer with any reasonable assistance necessary for analysing relating risks, in implementing measures to reduce all adverse impacts relating with changes, in updating security documentation, relating testing and in ensuring the ability of returning to the original condition. The procedure described in Article 9 (Adaptations) of the Agreement will apply for these Services.

11.6 Subject to article 4.6 (Penetration Test) of the Agreement and unless otherwise provided in article 1.37 of the Agreement, the Supplier shall provide the Customer with any assistance necessary for penetration testing or solution vulnerability testing, if applicable.

12. BUSINESS CONTINUITY MANAGEMENT

12.1 The Customer is authorized to integrate the Supplier in the business continuity management, including the authorization to integrate the Supplier in the business continuity plan relating to the PA BIS and relating services and/or to integrate the Supplier in the Customer’s emergency plan.

12.2 The Customer is obliged to inform the Supplier about the manner of the Supplier’s integration in accordance with cl. 12.1.

12.3 With respect to Supplier Services, the Supplier shall provide the Customer with Supplier’s data backup and recovery methodology in the form of a backup plan, data recovery testing scenario, recording system, and the methodology of ensuring the integrity and authenticity of the backup media. All backup data shall be encrypted. The Supplier shall also supply and launch a corresponding technological solution on which the data backup and recovery shall be carried out. Supplier's current backup and recovery methodology is included in Supplier's response to Customer's request for proposal in connection with this Agreement.

13. Supplier's INFORMATION requirements

13.1 The Supplier is obliged to inform the Customer, without undue delay, about any significant change in the Supplier's control pursuant to Act No. 90/2012 Sb., on business corporations and cooperatives (Business Corporations Act) and/or any change of the ownership of basic assets, as well as any change of the Supplier's authorization to dispose of the assets that are used to provide the supply hereunder.

13.2 The Supplier is obliged to inform the Customer about the risk management method, as well as any residual risks relating to the performance of the subject-matter of this Agreement at the Customer's written request.

14. SUBCONTRACTORS

14.1 The Supplier may engage any other subcontractor in providing the supply hereunder without the Customer's previous specific or general approval. Supplier will notify Customer of Supplier's subcontractors.

14.2 The Supplier undertakes to fulfil the requirements for information security management and shall provide all reasonably necessary assistance to the Customer in the issues of information security management of Supplier's Services, and if the Supplier provides the supply hereunder through subcontractors, all such necessary assistance in the issues of information security management shall also be provided by such subcontractors.

14.3 The Supplier is obliged to give the Customer contact details of the lead persons providing system and technical support services for the solution.

14.4 If the Supplier provides the supply hereunder through a subcontractor, any contract between the Supplier and such subcontractor must contain sufficient obligations to fulfil contractual provisions as contained in this Annex between the Customer and the Supplier.

14.5

14.6 The Supplier is obliged to ensure that the subcontractor shall be in compliance with the requirements imposed on the Supplier by the Customer hereunder.

14.7 The Supplier shall be responsible if its subcontractors fail to comply with the Security Measures arising from this Annex; any failure to fulfil such requirements by any Supplier's subcontractors shall be deemed the Supplier's breach of obligations hereunder.

15. DATA DESTRUCTION

15.1 If the Supplier is obliged by Customer to delete Customer data and destroy Customer technical carriers and/or operating data and/or information and any copies thereof as part of the supply hereunder, the Supplier shall act in strict compliance with the reasonable rules of data deletion and in compliance with the methods of destruction of technical carriers, operating data, information and any copies thereof as prescribed by the Customer or applicable law as may be required.

15.2 The Customer undertakes to set forth rules of data deletion and destruction of technical carriers, operating data and/or information and any copies thereof in proportion to the value and significance of the assets.

15.3 The Customer hereby sets forth that methods of destruction of technical carriers and/or operating data and/or information and any copies thereof hereunder may include, in compliance with the regulation applicable to it, removal, overwrite or physical destruction of the data carrier.

16. inspection and audit of supplier

16.1 The Supplier shall make available to Customer information reasonably necessary to demonstrate compliance with Suppliers' Personal Data Processing obligations under this Agreement by making available certificates concerning data protection and/or information security (e.g. ISO 27001) or through attestation, reports, or report excerpts by independent authorities (e.g. auditors, data protection auditors).

If Customer, acting reasonably, considers that Supplier has not provided sufficient evidence of its compliance, Customer must notify Supplier in writing providing evidence of such concerns and Supplier shall use reasonable endeavors to resolve Customer's concerns.

If Supplier is unable to resolve Customer's concerns, Customer may, as required under mandatory data protection law, audit Suppliers' control environment and security practices relevant to the Personal Data processed under this Agreement for Customer. Any audits conducted by Customer pursuant to this provision shall be subject to the following and unless required otherwise by request from a regulator:

16.2 shall be limited no more than one (1) audit per calendar year;

16.3 audits will be carried out during normal working hours, without disturbing business operations;

16.4 at least sixty (60) days prior written notice is provided;

16.5 the auditor will be required to sign an appropriate confidentiality agreement with Supplier and comply with Suppliers' on-site security policies;

16.6 if conducted by a third party auditor appointed by Customer, Supplier may reject the auditor appointed by Customer if the auditor is a competitor of Supplier, or otherwise manifestly unsuitable; and

16.7 Customer will provide Supplier with a copy of the audit report

17. NON-DISCLOSURE OBLIGATION

17.1 The Parties undertake not to disclose any information, personal data or messages received by them in connection with the preparation and performance of this Agreement (hereinafter referred to as the “**Confidential Information**”), including the subject-matter of the Agreement and internal affairs of the Parties.

17.2 The Confidential Information pursuant to this Agreement does not include information classified as “confidential” in accordance with Act No. 412/2005 Sb., on the protection of classified information and on security eligibility, as amended.

17.3 The Parties undertake to ensure that all persons authorized to process confidential information agree to be bound by non-disclosure duty or that such persons are bound by non-disclosure duty by law. Such duty of non-disclosure and confidential information protection shall survive the termination of this Agreement.

18. OBLIGATIONS UPON TERMINATION

18.1 The Supplier undertakes to provide the Customer with all necessary assistance, documentation and information, to participate in discussions with the Customer and/or third parties in order to transfer smoothly and properly any and all activities relating to the operation, maintenance and development of the subject-matter of the Agreement to the Customer and/or to the new Supplier according to the Customer’s instructions which shall take place after the termination of this Agreement (hereinafter referred to as the “**Termination**”). Notwithstanding anything above to the contrary, Supplier’s assistance as described above or in this Section 18 will be limited to assisting the Customer only. The scope and timeline describing how the Services will be terminated will be provided by Supplier to the Customer.

18.2 The Supplier undertakes to prepare documentation which contains a procedure for the Termination (hereinafter referred to as the “**Plan**”) and to provide it to the Customer no later than on the day of providing operating documentation for each partial supply to the Customer. The Supplier shall update the Plan throughout the duration of this Agreement on a regular basis and shall provide such updated version of the Plan to the Customer in case of any change of any fact contained in the Plan.

18.3 The Supplier is obliged to make acts and activities necessary to implement such Plan, taking account of the corresponding provisions of this Agreement. The obligation set forth in this sub-clause shall survive the termination of this Agreement.

18.4 The Parties agree that the price for the preparation of the Plan and supply necessary to implement the Plan is included in the price hereunder.

19. COMMON AND CONCLUDING PROVISIONS

19.1 This Annex is in compliance with the applicable legislation of the Czech Republic. If any provision of this Annex becomes invalid or unenforceable, this shall be without prejudice to the effectiveness and enforceability of the remaining provisions of this Annex and the Agreement. The Parties undertake to replace any such invalid or unenforceable provision with a new provision the effect of which comes as close as possible to the original provision and this Annex as a whole.

19.2 This Annex may not be altered or amended unless by written numbered amendments signed by both Parties.

Annex No. 5 – CUPPS/CUSS System description

AirportConnect Open Platform

1. Introduction

AirportConnect Open is specifically designed for airports, airlines and ground handling agents, providing a common use platform to facilitate airlines' agent-facing passenger check-in and boarding processes. Customers selecting a common use platform choose AirportConnect Open as it is designed to address the needs to optimize limited terminal infrastructure, expand capacity for growth in passenger traffic, and overcome passenger flow and service level issues in a cost-effective manner.

The AirportConnect platform provides:

- The ability to run both CUPPS and CUTE applications on common use workstations – enabling airports to maximize the use of their terminal infrastructure. Airlines have the option to use their existing CUTE applications, and/or to use their CUPPS applications developed by the airline using the CUPPS IATA Recommended Practice 1797 specification;
- Access to applications in real time, at any location at an airport, on equipment shared by all users, and using an array of the latest technologies;
- An integrated blend of CUPPS, CUTE and CUSS applications supported by one management system;
- Extensive reporting capabilities to ensure that the most effective use is made of infrastructure to enable improved customer flow and better service levels;
- The flexibility to add kiosks, self-bag drop, self-boarding gates, biometric identity management, business intelligence tools, and other products which are integrated and can operate based upon the same infrastructure.

AirportConnect platform is fully compliant with key common use IATA standards, and many more IATA Recommended Practices (RP) adopted by other SITA products. For example,

- Common Use Passenger Processing (CUPPS) – IATA RP 1797;
- Common Use Self-Service (CUSS) – RP 1706;
- IATA/ACI Common Use Web Services RP 1741.

2. The AirportConnect Platform Benefits:

- Enables a single platform to host CUTE, CUPPS and CUSS applications. As few airlines have created an IATA CUPPS compliant application, AirportConnect enables airlines operating at the airport a choice of using their CUTE or CUPPS application;
- Enables airports to quickly add new airlines to a common use environment. Airports permit airlines to use their CUPPS applications, the same as used at any airport with a CUPPS-compliant, common use system. In addition, airlines that operate at one of the

450+ SITA managed airports can use their same CUTE application deployed at these airports;

- Allows airports to maximize the utilization of check-in counter and gate resources, which enables airlines to expand and contract to meet seasonal traffic demands;

Allows new carriers to rapidly begin service with minimal expense;

- Allows dedicated airline counters and space to be used as common use, thereby freeing up under-utilized resources, allowing the airport to increase passenger and airline capacity, with little our now terminal construction expense;
- Provides a consistent, airport-wide passenger processing environment that can be tailored for each airline;
- Enables airports to maximize all available space, improving the overall return on investment;
- Enables growth, as there is no limit on the applications that can be loaded and available for airline and ground handler use. Each application is interdependent, and does not affect the productivity of other applications, regardless of the number used;
- Enables the airport to adopt and offer tenants cutting edge technologies, increasing airline satisfaction and improving the passenger experience.

3. Redundancy and Resilience allows for high availability and speedy recovery

Ensuring to allow users to benefit from uninterrupted, continuous service, all AirportConnect Open components are redundant. From multi-path wiring to multiple gateways, redundant switches and servers to RAID disk arrays on servers and interleaved workstations across multiple VLANs, your AirportConnect Open installation is protected to ensure that no single component failure can compromise the overall service and ensures 24x7 system operation.

In addition to providing a fully redundant system, software resilience ensures that, for example, should a server or gateway fail, your users may continue to check-in passengers. Users are able to control the system’s resiliency to meet their own needs if required – for example, they will be able to select and direct printing to an alternate boarding pass or bag tag printer in case the original printer jams or becomes inoperable.

Regular backups and replications are a component of AirportConnect Open’s overall recovery strategy and can take place without causing any interruption to service. The system is protected with a network backup server that employs a ‘one-touch’ restore function to ensure optimized recovery in the event of failure.

4. Multiple Concurrent Applications

AirportConnect Open allows a workstation or kiosk to run several applications simultaneously. For example, a handling agent may operate two or more airlines’ terminal emulators (TE) at the same time, or an airline agent might use a TE and a separate application to update the FIDS system at the same time. Providing a user-friendly interface, AirportConnect Open ensures that when a user swaps between applications, any peripherals associated with the application also swap – instantly. This means that there is no need for the user to wait while a printer is reloaded with the parameters for the new session, thereby resulting in increased productivity and better passenger service.

5. Flexible Operating Environments and Software Development Capabilities

Whether developing for web browsers, native IP applications, or Windows applications, AirportConnect platform is unique among common use systems in providing a fully supported, flexible development environment. TCP/IP is used exclusively as the network transport protocol, and a full API and Java class library support is provided to the developers for interfacing to virtual peripherals from any sort of application.

5. System Security

Login authentication and network communications are secured using the services of Windows 10 and Windows Server 2016. All network components from the workstations to the wiring closets are kept physically locked and secure. Anti-virus and firewall protection is integrated into both the AirportConnect Open platform and LAN architecture.

Access Management is key to limiting access to systems to only those that have permissions. The profiles that describe workstation appearance and behavior can be assigned for use as a group or with individual login credentials. For the tightest security, individuals separate credentials can be given while sharing a group-wide profile.

SITA AirportConnect uses Windows Server profiles and policies to provide each user with a secure desktop. Airline user accounts have limited privileges and can access only their respective applications. Only administrator accounts have privileges that grant access to troubleshooting and configuration utilities to enable the management of user accounts.

AirportConnect Platform is isolated from untrusted domain by the External Services Firewalls. URL whitelisting is the part of the platform, so the system allows users to access defined and certified internet pages as well as SharePoint platform from the end-user workstations.

The retention period for user and administrator related activities and events in the system is set at 12 months. The data are collected from DC's and Firewalls. Beats/agents are installed to DC's (Winlogbeat and Packetbeat), beats are sending data to Logstash SIEM server in LKPR. Firewalls are also configured to send syslogs to Logstash SIEM server in LKPR. Logstash filters/parse these logs and it sends to Elasticsearch in ATI Cloud via Kibana interface. Analysts are then able to monitor, analyze all that data from Elasticsearch. Also, port mirroring is configured at the Core Switch for being able to implement later IDS.

6. Administration and Monitoring

AirportConnect Open provides tools for remotely administering and configuring a site. Site administrators will be able to perform software installation, inventory collection, network analysis and troubleshooting, and user/group creation and management.

All shared hardware and software components of the AirportConnect Open installation comply with the Simple Network Management Protocol (SNMP) standard for operational monitoring and control. SNMP additions to AirportConnect Open software components allow SITA PRG administrators to see what applications are doing. All monitoring can be performed either via a workstation on the LAN or via SITA's Global Command Center for ultimate coverage and control.

7. The CUTE Intelligent Workstation (IWS)

The CUTE Intelligent Workstation (IWS) is a standard PC capable of hosting all the required platform and application software, together with their associated peripherals. Each IWS has a hard drive and a network interface and is pre-configured so that booting the IWS enables network communications and establishes communications with the CUTE/CUPPS server. IWS hard drives do not, in general, host user software which is loaded from the CUTE/CUPPS server once a user has been authenticated.

IWS configurations can be customized in order to allow to create unique end user workplaces like check-in, gate, back-office, training etc. to fully reflect the user's needs. The AirporConnect Open offers maximum flexibility that allows to share the resources physically connected to any of the IWS using the platform.

Item	Model	Quantity
IWS	DELL OptiPlex 3070 SFF Intel® Core™ i5-9500 (6 Cores/9MB/6T/3.0GHz to 4.4GHz/65W) 16GB DDR4 2666MHz RAM	425
Mouse	Dell Optical Mouse MS116	425
Standard Keyboard	Dell Multimedia Keyboard KB216	95
LCD 24''	Dell UltraSharp 24 Monitor U2412M	4
LCD 19''	Dell 19 Monitor - P1917S	351
LCD 17''	Dell 17 Monitor E1715S	70

8. Peripherals

AirportConnect Open peripherals are driven through VPS32, SITA's Virtual Peripheral Service. This ensures that airlines of other host systems, as well as application developers, do not need to be familiar with specific device characteristics or whether another application is already using the peripheral.

Item	Model	Quantity
MSR/OCR Keyboard	Access AKB500-G	330
BGR	Access BGR750	135
LSR	Access IT 1950g	190
ATB	Custom TK180	275
BTP	Custom TK180 BTP	250

BTP with RFID	Custom TK180 BTP RFID	10
DCP	OKI ML3320	85

9. AirportConnect Platform Core System Design

System architecture is designed to provide a robust system to be able to host more than 500 clients with no need to upgrade any equipment in 5 years and with no effect on system performance.

The SITA proposed solution is built on the Microsoft Windows 10 and Windows Server 2016 software suite.

Item	Model	Quantity
Domain Controller Servers	HPE DL380 Gen10	2
Usage Servers	HPE DL380 Gen10	2
Backup Server	ReadyNAS 2304	1
Tape Backup	HPE LTO5 Ultrium 3000 SAS Tape Drive	1
External Services Switches	Cisco Catalyst 9200L	2
External Services Firewalls	Cisco Firepower 2110 ASA	2
SITA Services Switches	Cisco Catalyst 9300L	2

10. AirportConnect Kiosk

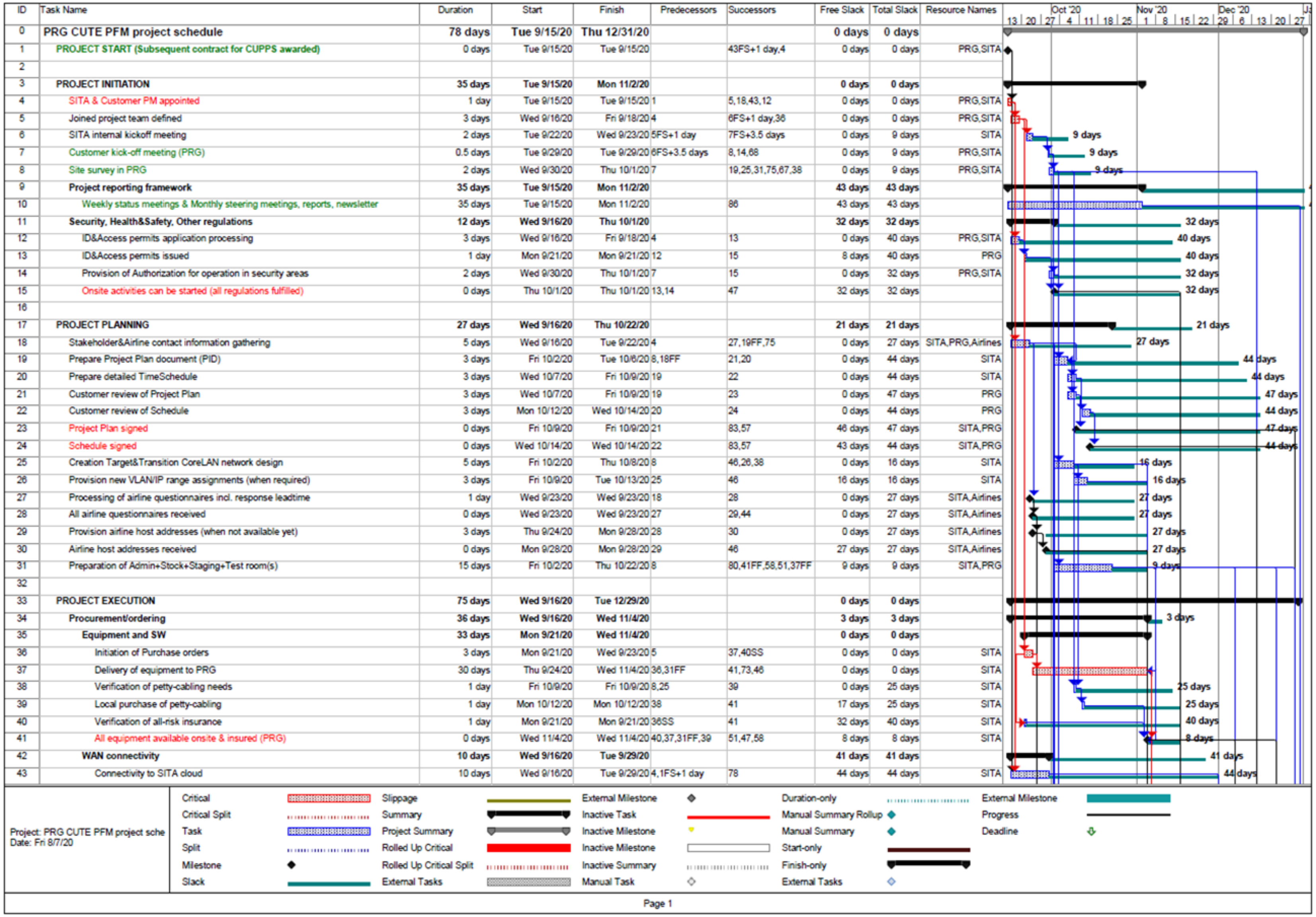
The SITA S6 Kiosk is a stand-alone, self-service kiosk that allows airline passengers to check in and print a boarding pass and bag tags. The kiosk runs CUSS compliant software and communicates with the airline network through a LAN connection. A passenger interacts with the kiosk software through the touch screen display.

The kiosk is designed with more hygienic and easy-to-clean materials and can be enhanced with temperature readers etc. to increase safe travel passenger experience.

The S6s kiosk specifications:

Item	Quantity
S6 kiosk ▪ Industrial PC; ▪ 17" Touch screen + Virtual Keyboard; ▪ OCR ID/passport/BC scanner; ▪ General Purpose Printer; ▪ BagTag printer; ▪ IP Addressable power management device; ▪ UPS; ▪ Card reader; ▪ Overhead Signage; ▪ Base plate; ▪ Top Arch LEDs indicating kiosk status – Green, Amber and Red.	35

Annex No. 6 – Implementation Time Schedule

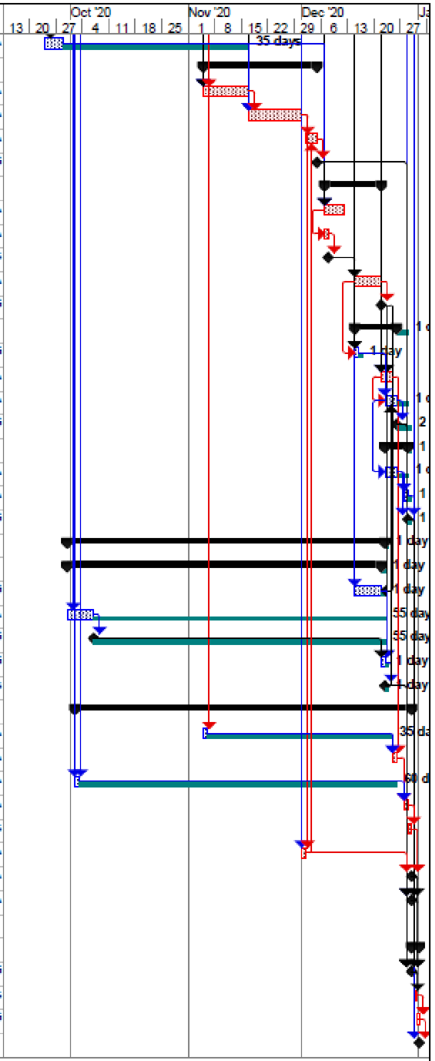


ID	Task Name	Duration	Start	Finish	Predecessors	Successors	Free Slack	Total Slack	Resource Names
0	**PRG CUTE PFM project schedule**	**78 days**	**Tue 9/15/20**	**Thu 12/31/20**			**0 days**	**0 days**	
1	**PROJECT START (Subsequent contract for CUPPS awarded)**	0 days	Tue 9/15/20	Tue 9/15/20		43FS+1 day,4	0 days	0 days	PRG,SITA
2									
3	**PROJECT INITIATION**	**35 days**	**Tue 9/15/20**	**Mon 11/2/20**			**0 days**	**0 days**	
4	SITA & Customer PM appointed	1 day	Tue 9/15/20	Tue 9/15/20	1	5,18,43,12	0 days	0 days	PRG,SITA
5	Joined project team defined	3 days	Wed 9/16/20	Fri 9/18/20	4	6FS+1 day,36	0 days	0 days	PRG,SITA
6	SITA internal kickoff meeting	2 days	Tue 9/22/20	Wed 9/23/20	5FS+1 day	7FS+3.5 days	0 days	9 days	SITA
7	Customer kick-off meeting (PRG)	0.5 days	Tue 9/29/20	Tue 9/29/20	6FS+3.5 days	8,14,68	0 days	9 days	PRG,SITA
8	Site survey in PRG	2 days	Wed 9/30/20	Thu 10/1/20	7	19,25,31,75,67,38	0 days	9 days	PRG,SITA
9	**Project reporting framework**	**35 days**	**Tue 9/15/20**	**Mon 11/2/20**			**43 days**	**43 days**	
10	Weekly status meetings & Monthly steering meetings, reports, newsletter	35 days	Tue 9/15/20	Mon 11/2/20		86	43 days	43 days	
11	**Security, Health&Safety, Other regulations**	**12 days**	**Wed 9/16/20**	**Thu 10/1/20**			**32 days**	**32 days**	
12	ID&Access permits application processing	3 days	Wed 9/16/20	Fri 9/18/20	4	13	0 days	40 days	PRG,SITA
13	ID&Access permits issued	1 day	Mon 9/21/20	Mon 9/21/20	12	15	8 days	40 days	PRG
14	Provision of Authorization for operation in security areas	2 days	Wed 9/30/20	Thu 10/1/20	7	15	0 days	32 days	PRG,SITA
15	Onsite activities can be started (all regulations fulfilled)	0 days	Thu 10/1/20	Thu 10/1/20	13,14	47	32 days	32 days	
16									
17	**PROJECT PLANNING**	**27 days**	**Wed 9/16/20**	**Thu 10/22/20**			**21 days**	**21 days**	
18	Stakeholder&Airline contact information gathering	5 days	Wed 9/16/20	Tue 9/22/20	4	27,19FF,75	0 days	27 days	SITA,PRG,Airlines
19	Prepare Project Plan document (PID)	3 days	Fri 10/2/20	Tue 10/6/20	8,18FF	21,20	0 days	44 days	SITA
20	Prepare detailed TimeSchedule	3 days	Wed 10/7/20	Fri 10/9/20	19	22	0 days	44 days	SITA
21	Customer review of Project Plan	3 days	Wed 10/7/20	Fri 10/9/20	19	23	0 days	47 days	PRG
22	Customer review of Schedule	3 days	Mon 10/12/20	Wed 10/14/20	20	24	0 days	44 days	PRG
23	Project Plan signed	0 days	Fri 10/9/20	Fri 10/9/20	21	83,57	46 days	47 days	SITA,PRG
24	Schedule signed	0 days	Wed 10/14/20	Wed 10/14/20	22	83,57	43 days	44 days	SITA,PRG
25	Creation Target&Transition CoreLAN network design	5 days	Fri 10/2/20	Thu 10/8/20	8	46,26,38	0 days	16 days	SITA
26	Provision new VLAN/IP range assignments (when required)	3 days	Fri 10/9/20	Tue 10/13/20	25	46	16 days	16 days	SITA
27	Processing of airline questionnaires incl. response leadtime	1 day	Wed 9/23/20	Wed 9/23/20	18	28	0 days	27 days	SITA,Airlines
28	All airline questionnaires received	0 days	Wed 9/23/20	Wed 9/23/20	27	29,44	0 days	27 days	SITA,Airlines
29	Provision airline host addresses (when not available yet)	3 days	Thu 9/24/20	Mon 9/28/20	28	30	0 days	27 days	SITA,Airlines
30	Airline host addresses received	0 days	Mon 9/28/20	Mon 9/28/20	29	46	27 days	27 days	SITA,Airlines
31	Preparation of Admin+Stock+Staging+Test room(s)	15 days	Fri 10/2/20	Thu 10/22/20	8	80,41FF,58,51,37FF	9 days	9 days	SITA,PRG
32									
33	**PROJECT EXECUTION**	**75 days**	**Wed 9/16/20**	**Tue 12/29/20**			**0 days**	**0 days**	
34	**Procurement/ordering**	**36 days**	**Wed 9/16/20**	**Wed 11/4/20**			**3 days**	**3 days**	
35	**Equipment and SW**	**33 days**	**Mon 9/21/20**	**Wed 11/4/20**			**0 days**	**0 days**	
36	Initiation of Purchase orders	3 days	Mon 9/21/20	Wed 9/23/20	5	37,40SS	0 days	0 days	SITA
37	Delivery of equipment to PRG	30 days	Thu 9/24/20	Wed 11/4/20	36,31FF	41,73,46	0 days	0 days	SITA
38	Verification of petty-cabling needs	1 day	Fri 10/9/20	Fri 10/9/20	8,25	39	0 days	25 days	SITA
39	Local purchase of petty-cabling	1 day	Mon 10/12/20	Mon 10/12/20	38	41	17 days	25 days	SITA
40	Verification of all-risk insurance	1 day	Mon 9/21/20	Mon 9/21/20	36SS	41	32 days	40 days	SITA
41	All equipment available onsite & insured (PRG)	0 days	Wed 11/4/20	Wed 11/4/20	40,37,31FF,39	51,47,58	8 days	8 days	SITA
42	**WAN connectivity**	**10 days**	**Wed 9/16/20**	**Tue 9/29/20**			**41 days**	**41 days**	
43	Connectivity to SITA cloud	10 days	Wed 9/16/20	Tue 9/29/20	4,1FS+1 day	78	44 days	44 days	SITA

Project: PRG CUTE PFM project sche
Date: Fri 8/7/20

Critical	▨	Slippage	▬	External Milestone	◆	Duration-only	┄	External Milestone	▬
Critical Split	┄	Summary	▬	Inactive Task	▬	Manual Summary Rollup	◆	Progress	▬
Task	▨	Project Summary	▬	Inactive Milestone	▼	Manual Summary	◆	Deadline	⇩
Split	┄	Rolled Up Critical	▬	Inactive Milestone	□	Start-only	▬		
Milestone	◆	Rolled Up Critical Split	┄	Inactive Summary	┄	Finish-only	▬		
Slack	▬	External Tasks	▨	Manual Task	◇	External Tasks	◇		

ID	Task Name	Duration	Start	Finish	Predecessors	Successors	Free Slack	Total Slack	Resource Names
44	Airline WAN connections to hosts (when not existing)	3 days	Thu 9/24/20	Mon 9/28/20	28	51,47	35 days	35 days	Airlines,SITA
45	**Core room**	**22 days**	**Thu 11/5/20**	**Fri 12/4/20**			**0 days**	**0 days**	
46	Core equipment staging	8 days	Thu 11/5/20	Mon 11/16/20	25,26,30,37	47	0 days	0 days	SITA
47	Core equipment installation & Core network config in PRG	10 days	Tue 11/17/20	Mon 11/30/20	44,41,15,46	78,48	0 days	0 days	SITA
48	Core installation acceptance testing	3 days	Wed 12/2/20	Fri 12/4/20	78,47	49	0 days	0 days	SITA
49	Hand-over of Core acceptance sheets	0 days	Fri 12/4/20	Fri 12/4/20	48	51,83	0 days	0 days	SITA,PRG
50	**Airline TE applications**	**11 days**	**Mon 12/7/20**	**Mon 12/21/20**			**0 days**	**0 days**	
51	Stage/tune configuration of Test-wks & Install all TEs	5 days	Mon 12/7/20	Fri 12/11/20	49,44,41,31	52SS	0 days	0 days	Airlines,SITA
52	Creation of testing documentation (plan+scenarios)	1 day	Mon 12/7/20	Mon 12/7/20	51SS	53	0 days	0 days	SITA
53	Testing docs handed over to all stakeholders	0 days	Mon 12/7/20	Mon 12/7/20	52	54FS+5 days	0 days	0 days	SITA,PRG,Airlines
54	Series of TE testing by agents & tuning by SITA	5 days	Tue 12/15/20	Mon 12/21/20	53FS+5 days	55,57SS	0 days	0 days	Airlines,SITA
55	All TEs signed and acceptance sheets handed over	0 days	Mon 12/21/20	Mon 12/21/20	54	70,58,67FF	0 days	0 days	Airlines,SITA,PRG
56	**Roll-out shared end-user equipment**	**9 days**	**Tue 12/15/20**	**Fri 12/25/20**			**1 day**	**1 day**	
57	Schedule of counter modifications pre-agreed with Flight planning	1 day	Tue 12/15/20	Tue 12/15/20	23,24,54SS	59FS+5 days	0 days	1 day	SITA,PRG
58	Pre-staging of all wks incl. peripherals	3 days	Tue 12/22/20	Thu 12/24/20	31,41,55	59SS+1 day,74	0 days	0 days	SITA
59	Installation of wks incl. peripherals to counters	3 days	Wed 12/23/20	Fri 12/25/20	58SS+1 day,57FS	62SS,60	0 days	1 day	SITA
60	Hand-over of wks/counter acceptance sheets	0 days	Fri 12/25/20	Fri 12/25/20	59	83,80	2 days	2 days	SITA,PRG
61	**De-installation of old equipment**	**4 days**	**Wed 12/23/20**	**Mon 12/28/20**			**1 day**	**1 day**	
62	De-installation of shared end-user equipment	3 days	Wed 12/23/20	Fri 12/25/20	59SS	64,63	0 days	1 day	SITA
63	De-installation old Core equipment	1 day	Mon 12/28/20	Mon 12/28/20	62	64	0 days	1 day	SITA
64	De-installation completed and signed	0 days	Mon 12/28/20	Mon 12/28/20	62,63	83,80	1 day	1 day	SITA,PRG
65	**Training program**	**60 days**	**Wed 9/30/20**	**Tue 12/22/20**			**1 day**	**1 day**	
66	**Training preparation**	**59 days**	**Wed 9/30/20**	**Mon 12/21/20**			**1 day**	**1 day**	
67	Preparation of Training room and wks	5 days	Tue 12/15/20	Mon 12/21/20	8,55FF	70	0 days	1 day	SITA,PRG
68	Definition of Training program curricullum	5 days	Wed 9/30/20	Tue 10/6/20	7	69	0 days	55 days	SITA
69	Approval for Training program provided	0 days	Tue 10/6/20	Tue 10/6/20	68	70	54 days	55 days	PRG
70	Airline supervisor training onsite	1 day	Tue 12/22/20	Tue 12/22/20	69,55,67	71	0 days	1 day	SITA,Airlines,PRG
71	Training program(s) completed & Acceptance sheet signed	0 days	Tue 12/22/20	Tue 12/22/20	70	83,59,80	0 days	1 day	SITA,PRG,Airlines
72	**Operations set-up**	**63 days**	**Fri 10/2/20**	**Tue 12/29/20**			**0 days**	**0 days**	
73	Asset data gathering for ServiceDesk started	1 day	Thu 11/5/20	Thu 11/5/20	37	74	35 days	35 days	SITA
74	Asset data gathering for ServiceDesk completed	1 day	Fri 12/25/20	Fri 12/25/20	73,58	76	0 days	0 days	SITA
75	Contact data for ServiceDesk gathered	1 day	Fri 10/2/20	Fri 10/2/20	18,8	76	60 days	60 days	SITA
76	Tools set-up (Montreal)	1 day	Mon 12/28/20	Mon 12/28/20	75,74	77	0 days	0 days	SITA
77	ServiceDesk Call flow testing	1 day	Tue 12/29/20	Tue 12/29/20	76	79	0 days	0 days	SITA,PRG,Airlines
78	Remote mgmt connection testing	1 day	Tue 12/1/20	Tue 12/1/20	47,43	48,79	0 days	0 days	SITA
79	ServiceDesk & Operational solution ready	0 days	Tue 12/29/20	Tue 12/29/20	77,78	83,80	0 days	0 days	SITA
80	Formal hand-over to SITA Regional Ops signed	0 days	Tue 12/29/20	Tue 12/29/20	31,79,60,71,64	83	0 days	0 days	SITA
81									
82	**PROJECT CLOSURE**	**2 days**	**Tue 12/29/20**	**Thu 12/31/20**			**0 days**	**0 days**	
83	OFFICIAL CUTOVER TO PRODUCTION (Acceptance signed)	0 days	Tue 12/29/20	Tue 12/29/20	49,71,60,23,24,64,	84FS+1 day	0 days	0 days	SITA,PRG
84	Post-cutover workshop to agree Work procedure for Ops stage	0.5 days	Thu 12/31/20	Thu 12/31/20	83FS+1 day	85	0 days	0 days	SITA,PRG,Airlines
85	Project closure and lessons learned meeting	0.5 days	Thu 12/31/20	Thu 12/31/20	84	86	0 days	0 days	SITA,PRG
86	PROJECT END	0 days	Thu 12/31/20	Thu 12/31/20	85,10		0 days	0 days	



Project: PRG CUTE PFM project sche
Date: Fri 8/7/20

Critical	▨	Slippage	▬	External Milestone	◆	Duration-only	┈	External Milestone	▬
Critical Split	┈	Summary	▬	Inactive Task	▬	Manual Summary Rollup	◆	Progress	▬
Task	▨	Project Summary	▬	Inactive Milestone	◆	Manual Summary	◆	Deadline	⇩
Split	┈	Rolled Up Critical	▬	Inactive Milestone	□	Start-only	▬		
Milestone	◆	Rolled Up Critical Split	┈	Inactive Summary	┈	Finish-only	▬		
Slack	▬	External Tasks	▨	Manual Task	◇	External Tasks	◇		

Annex No. 7 – List of airline systems to implement

Airline	Product	Basename
3U		
	Angel Lite Overseas V2.0.0	Angel Lite Overseas
4U		
	LH Cute Future GoNow V1.7.3.3 for LH, 4U	LH Cute Future GoNow
	4U GoNow V1.5.0.83	4U GoNow
	LH ICB4U V1.0	LH ICB4U
	LH Cute Future 2019.09.20	LH Cute Future
7X		
	SFEB V7.0.4	SFEB
A3		
	A3 CUSS V4.1.5	A3 CUSS
	Amadeus StandalonePrintEmulator v2.43.0	StandalonePrintEmulator
	Amadeus Flight Management V20.1.01	Amadeus Flight Management
	Amadeus CustomerManagement v65.4.2	Amadeus CustomerManagement
A9		
	SFEB V7.0.4	SFEB
AA		
	Microsoft .NET Framework V4.6.2	Microsoft .NET Framework
	AA CUSS V4.2_R_8_5_6	AA CUSS
	AA Hub V8.0/3.7	AA Hub
	aim: American Hub Launcher 8.0 (6)	American Hub Launcher
AC		
	AC QIKCHECK v0014A_BGR	AC QIKCHECK
	AC QIKCHECK for CUTE/NT and APC 00.20A_6.2	AC QIKCHECK for CUTE/NT and APC
	AC Suite V6.2	AC Suite
	AC CUSS 4.1.9	AC CUSS
AF		
	Amadeus Flight Management V17.1.01	Amadeus Flight Management
	AF CUSS V13.0.28	AF CUSS
	KL Webkiosk V18.05	KL Webkiosk
	AF VEGA V4.5	AF VEGA
	AF/KL NGKA 2018.1	AF/KL NGKA
	Amadeus CustomerManagement v64.3.5	Amadeus CustomerManagement
	Amadeus StandalonePrintEmulator V2.42.0	StandalonePrintEmulator
	aim: VEGA4 4.5 (7)	VEGA4
AY		
	AY Citrix V1.0	AY Citrix
	AY CUSS V4.1.5	AY CUSS
	AY AYRES V10.5.46	AY AYRES
	Amadeus CustomerManagement v64.3.5	Amadeus CustomerManagement
	Amadeus StandalonePrintEmulator V2.42.0	StandalonePrintEmulator
	Amadeus Flight Management V19.4.01	Amadeus Flight Management
AZ		
	LoadManager V1.2	LoadManager
	Horizon Weight & Balance V3.2.419	Horizon Weight & Balance
	AZ CUSS V1.0	AZ CUSS
	Sabre Interact V10.4.2v9.1 for Multiple Airlines	Sabre Interact
B2		
	SFEB V6.15.7 Windows7	SFEB
	B2 CUSS V7.9	B2 CUSS
	Sabre Interact V10.3.0v9.0 for Multiple Airlines	Sabre Interact
BA		
	Amadeus Flight Management V18.3.01	Amadeus Flight Management
	Amadeus CustomerManagement v62.3.6	Amadeus CustomerManagement
	Amadeus StandalonePrintEmulator V2.40.0	StandalonePrintEmulator
	BA Fly V2.5.1	BA Fly
BT		
	Amadeus Flight Management V19.3.01	Amadeus Flight Management
	Amadeus StandalonePrintEmulator V2.42.0	StandalonePrintEmulator
	Amadeus CustomerManagement v64.3.5	Amadeus CustomerManagement
KL		
	Amadeus Flight Management V16.3.01	Amadeus Flight Management
	KL CUSS V1511.1	KL CUSS
	KL Alpha V3.6	KL Alpha
	KL Webkiosk V18.05	KL Webkiosk
	AF VEGA V4.5	AF VEGA
	AF/KL NGKA 2018.1	AF/KL NGKA
	Amadeus StandalonePrintEmulator V2.42.0	StandalonePrintEmulator
	Amadeus CustomerManagement v64.3.5	Amadeus CustomerManagement
	aim: Customer Management V62.3.6 (58)	Customer Management
KM		
	SFEB V6.15.7 Windows7	SFEB
	Horizon Weight & Balance V3.2.419	Horizon Weight & Balance
LG		
	SFEB V6.15.7 Windows7	SFEB
LH		
	LH Guide CKI V2006.1.3/3.11 Java CF	LH Guide CKI Java CF
	LH_CF_GONOW V3.1.0.44 for Multiple Airlines	LH_CF_GONOW
	LH Cute Future 2020.01.10	LH Cute Future
	LH CUSS V2.19.2.6	LH CUSS
	LH cFront V4.1 for Multiple Airlines	LH cFront
	aim: cFront V3.2 (1)	cFront
	aim: cFront V3.5 (19)	cFront
LO		
	LH Cute Future 2014.03.31 Delta	LH Cute Future
	LH Guide CKI V2006.1.3/3.11 Java CF	LH Guide CKI Java CF
	Amadeus CustomerManagement v65.4.2	Amadeus CustomerManagement
	Amadeus StandalonePrintEmulator v2.43.0	StandalonePrintEmulator
	Amadeus Flight Management V20.1.01	Amadeus Flight Management
LS		
	SFEB V7.0.1	SFEB
LX		
	Amadeus Flight Management V16.3.01	Amadeus Flight Management
	Amadeus CustomerManagement V56.3.2	Amadeus CustomerManagement
	LH Cute Future 2019.09.20	LH Cute Future
	LH cFront V4.1 for Multiple Airlines	LH cFront
LY		
	Amadeus StandalonePrintEmulator V2.36.0	StandalonePrintEmulator
	LY CUSS V4.1.5	LY CUSS
	Amadeus Flight Management V19.1.01	Amadeus Flight Management
	Amadeus CustomerManagement v62.3.6	Amadeus CustomerManagement
MU		
	Angel Lite Overseas V2.0.0	Angel Lite Overseas
OK		
	OK ARDW(URL) V1.0	OK ARDW(URL)
	OK CUSS V4.2.1	OK CUSS
	Amadeus Flight Management V20.1.01	Amadeus Flight Management
	Amadeus StandalonePrintEmulator v2.43.0	StandalonePrintEmulator
	Amadeus CustomerManagement v65.4.2	Amadeus CustomerManagement
OS		
	Amadeus StandalonePrintEmulator V2.31.0	StandalonePrintEmulator
	Amadeus Flight Management V16.3.01	Amadeus Flight Management
	OS CUSS V2.5.4.1	OS CUSS
	Amadeus CustomerManagement V56.3.2	Amadeus CustomerManagement
	LH Cute Future 2019.09.20	LH Cute Future
	LH cFront V4.1 for Multiple Airlines	LH cFront
OU		
	Amadeus Flight Management V16.3.01	Amadeus Flight Management
	Amadeus StandalonePrintEmulator V2.40.0	StandalonePrintEmulator
	Amadeus CustomerManagement v62.3.6	Amadeus CustomerManagement

CX		
	Amadeus Flight Management V19.2.01	Amadeus Flight Management
	Amadeus StandalonePrintEmulator v2.43.0	StandalonePrintEmulator
	Amadeus CustomerManagement v65.4.2	Amadeus CustomerManagement
CY		
	Amadeus StandalonePrintEmulator V2.41.0	StandalonePrintEmulator
	Amadeus CustomerManagement v63.4.2	Amadeus CustomerManagement
	Amadeus Flight Management V19.2.01	Amadeus Flight Management
DL		
	DL CUSS V16.11.01	DL CUSS
	DL Lite V1.1.7.0	DL LITE
	DL_APM VPN access	DL_APM VPN access
	DL Lite V1.1.7.0 Update 11092010	DL LITE Update
	RFID Query Tool V1.0.2 _ DL	RFID Query Tool
	DL SNAPP Ver3.0.4.5	DL SNAPP
	aim: SNAPP v3.0.4.5 (2)	SNAPP
DV		
	SFEB V7.0.4.1	SFEB
DY		
	Amadeus CUSS V3.5	Amadeus CUSS
	Amadeus StandalonePrintEmulator V2.42.0	StandalonePrintEmulator
	Amadeus Flight Management V19.4.01	Amadeus Flight Management
	Amadeus CustomerManagement v65.4.2	Amadeus CustomerManagement
EK		
	EK MATIP Configuration Services V1.4	EK MATIP Configuration Service
	XSJTE Ver. 5.07.02 for EK	XSJTE FOR EK
	EK TSCA V2.0.5.88	EK TSCA
	ASConnect V3.0.0 for EK	ASConnect
	EK ECUSEASCONNECT V3.0.0.4	EK ECUSEASCONNECT
	aim: ECUSEASCONNECT 3.0.0.3 (24)	ECUSEASCONNECT
	aim: ECUSEASCONNECT 3.0.0.4 (7)	ECUSEASCONNECT
EW		
	LH Cute Future 2019.09.20	LH Cute Future
	LH cFront V4.1 for Multiple Airlines	LH cFront
FB		
	Amadeus StandalonePrintEmulator V2.41.0	StandalonePrintEmulator
	Amadeus CustomerManagement v63.4.2	Amadeus CustomerManagement
	Amadeus Flight Management V19.3.01	Amadeus Flight Management
FR		
	GoNow V4.0.0.29 for Multiple Airlines	GoNow
FV		
	SFEB V6.15.7	SFEB
FZ		
	SFEB V7.0.1	SFEB
	EK MATIP Configuration Services V1.4	EK MATIP Configuration Service
	XSJTE Ver. 5.08.01 for EK	XSJTE FOR EK
	SprintCheckin V2.4.0 for FZ	SprintCheckin
G9		
	Horizon Weight & Balance V3.8.26	Horizon Weight & Balance
	SFEB V7.0.4	SFEB
	G9 Horizon DCS v15.9.98	G9 Horizon DCS
	Horizon DCS v15.10.122	Horizon DCS
HU		
	Angel Lite Overseas V2.0.0	Angel Lite Overseas
HV		
	GoNow V4.0.0.29 for HV	GoNow
	aim: GoNow 4.0.0.29 (84)	GoNow
IB		
	IB TSGate V4.20b	IB TSGate
	IB CUSS V4.04	IB CUSS
IZ		
	SFEB V7.0.1	SFEB
J2		
	SFEB V6.15.7	SFEB
JU		
	LoadManager V1.2	LoadManager
	Sabre Interact V10.4.2v10.0 for Multiple Airlines	Sabre Interact
	aim: Sabre Interact V10.4.2v10.0 (22)	Sabre Interact
KE		
	Amadeus Flight Management V16.3.01	Amadeus Flight Management
	Amadeus StandalonePrintEmulator V2.31.0	StandalonePrintEmulator
	Amadeus CustomerManagement v64.3.5	Amadeus CustomerManagement
PC		
	CraneDCS V3.6 for Multiple Airlines	CraneDCS
	PC KeyPortal V8.0	PC KeyPortal
PS		
	SFEB V7.0.1	SFEB
	Amadeus Flight Management V19.3.01	Amadeus Flight Management
	Amadeus StandalonePrintEmulator V2.42.0	StandalonePrintEmulator
	Amadeus CustomerManagement v64.3.5	Amadeus CustomerManagement
QR		
	Amadeus StandalonePrintEmulator V2.40.0	StandalonePrintEmulator
	Amadeus Flight Management V19.2.01	Amadeus Flight Management
	Amadeus CustomerManagement v62.3.6	Amadeus CustomerManagement
QS		
	SFEB V7.0.1	SFEB
	QS CUSS V4.1.5	QS CUSS
	Amadeus StandalonePrintEmulator v2.43.0	StandalonePrintEmulator
	Amadeus CustomerManagement v65.4.2	Amadeus CustomerManagement
	Amadeus Flight Management V20.1.01	Amadeus Flight Management
RO		
	SFEB V7.0.4	SFEB
	Amadeus CustomerManagement v64.3.5	Amadeus CustomerManagement
	Amadeus Flight Management V19.3.01	Amadeus Flight Management
	Amadeus StandalonePrintEmulator V2.41.0	StandalonePrintEmulator
	RO ARDWEB V1.0	RO ARDWEB
S7		
	Horizon Weight & Balance V3.4.49	Horizon Weight & Balance
	SFEB V7.0.1	SFEB
	Amadeus CustomerManagement v64.3.5	Amadeus CustomerManagement
	Amadeus StandalonePrintEmulator V2.42.0	StandalonePrintEmulator
	Amadeus Flight Management V19.4.01	Amadeus Flight Management
SK		
	SK CUSS V1.5.0	SK CUSS
	Amadeus CustomerManagement v64.3.5	Amadeus CustomerManagement
	Amadeus StandalonePrintEmulator V2.42.0	StandalonePrintEmulator
	Amadeus Flight Management V19.3.01	Amadeus Flight Management
SN		
	HP OPAT V5.5	EDS OPAT
	SN CUSS V2.0.0	SN CUSS
	1C CUSS V3.1	1C CUSS
	LH Cute Future 2019.09.20	LH Cute Future
	LH cFront V4.1 for Multiple Airlines	LH cFront
SU		
	Sabre Interact V10.1.3v8.2.1 for Multiple Airlines	Sabre Interact
	Amadeus Flight Management V18.2.01	Amadeus Flight Management
	SU CUSS V7.9	SU CUSS
	Sabre Interact V10.4.2v10.0 for Multiple Airlines	Sabre Interact
TK		
	XSJTE Ver. 5.03.02a for TK	XSJTE FOR TK
	TK WEB_GUI_DCS V1.4.0	TK WEB_GUI_DCS
	TK CUSS V2.0.00	TK CUSS
	TK Quick Checkin 2.3.1	Quick Checkin
	aim: Quick Checkin 2.3.1 (13)	Quick Checkin
TO		
	SFEB V7.0.1	SFEB
	GoNow V3.1.0.34.2 for Multiple Airlines	GoNow
TP		
	Amadeus CustomerManagement v63.4.2	Amadeus CustomerManagement
	Amadeus StandalonePrintEmulator V2.41.0	StandalonePrintEmulator
	Amadeus Flight Management V19.3.01	Amadeus Flight Management
TS		
	Amadeus Flight Management V16.3.01	Amadeus Flight Management
	Amadeus CustomerManagement v65.4.2	Amadeus CustomerManagement
	Amadeus StandalonePrintEmulator v2.43.0	StandalonePrintEmulator
U2		
	XSJTE FOR U2 Ver. 5.05.01	XSJTE FOR U2
U6		
	Amadeus CustomerManagement v65.4.2	Amadeus CustomerManagement
	Amadeus Flight Management V20.1.01	Amadeus Flight Management
	Amadeus StandalonePrintEmulator v2.43.0	StandalonePrintEmulator
UA		
	UA CUSS V2.7 for CUSS Standard 1.3(V7.0)	UA CUSS
	UA AERO V1.1.5.3	UA AERO
	UA Airport Apps Portal V4.6u	UA Airport Apps Portal
	UA Infoconnect V9.1b	UA Infoconnect
	UA Suite V2019.08.19	UA Suite
V7		
	SFEB V7.0.1	SFEB
	XSJTE Ver. 5.03.01 for V7	XSJTE FOR V7
VY		
	GoNow V4.1.1.2 for Multiple Airlines	GoNow
	aim: GoNow 4.1.1.2 (23)	GoNow
XH		
	Horizon Weight & Balance V3.3.39	Horizon Weight & Balance
	SFEB V7.0.1	SFEB

🟦	**airline applications to be implemented before 1st JAN 2021**
🟧	**airline applications that might be implemented after 1st JAN 2021**

Annex No. 8 – Standard warranty exclusions

Product	Manufacturer Warranty Details
Kiosk	**Damage caused by the following is not covered:**
	Normal wear and tear
	Abuse
	Misuse
	Operation of the product outside the environmental or electrical specification for the Product
	Unsuitable physical or operating environment
	Air conditioning, humidity control or other environmental conditions
	Damage by beverage and liquid spillage
	Accident
	Third party supplied hardware or interfacing, or reprogramming, which causes excessive repetition of electromechanical or electronic components // Failure or damage caused by other third party products // Damage caused by malfunction of another device to which the product is connected
	Third party provided software which may cause improper product function, operation and/or system failure Reloading of software also not covered
	Modifications not authorised by the manufacturer
	Accident or damage due to war or civil commotion or natural calamity including, but not limited to, lightning, fire, flood or earthquake, or force majeure
	Any other criteria specific to a model type that constitutes a customer-induced fault
	Hazard
	Failure or fluctuation of electric power, power surges
	Uses not in accordance with documentation
	Products modified, repaired or disassembled by unauthorised persons
	Damage from the use of unapproved cleaning chemicals
	Failure or damage caused by use of Operational Consumables with specifications not recommended by manufacturer
	The following are not within the scope of the warranty:
	Replacement of consumable items (e.g. batteries, printer media, ink heads) unless specifically included in scope of services
	Uninterrupted to error free operation

Product	Manufacturer Warranty Details
	Loss of or damage to data by the product
Kiosk	Firmware upgrade, or product re-configuration, unless necessary to repair the product SW programs
	Scratched optical components
	Missing parts or screws
	Prototype products or customised products supplied for evaluation only
LSR	**The warranty does not cover:**
	Software or damage to the product caused by modification, alteration, misapplication, misuse of, or physical abuse to the product
	Damage due to repair or service to the product by anyone other than a manufacturer authorised center
	This warranty also excludes any damage to the product caused by circumstances outside of manufacturer's control, such as, but not limited to, lightning or fluctuation in electrical power
MSR/OCR	**The warranty does not cover:**
	Normal wear and tear. Manufacturer is not responsible for damages outside of Manufacturer control including, but not limited to, physical damage, modifications to the product, or improper packaging. In particular, the warranty becomes void if - the product has been opened, - the product has been altered, - the product data have been removed, - the guide frame has been damaged through inexpert exchange of the key covers, or - by an operating error
DCP	**The warranty does not cover:**
	For software products, the Warranty applies only to a failure to execute programming instructions. Manufacturer does not warrant that the operation of any product will be uninterrupted, error free, or to the satisfaction of the Customer.
	The Warranty covers only those defects which arise as a result of normal use of the product, and in no way will apply to any fault or malfunction caused by: - Improper or inadequate installation, maintenance, repair or modification to the product other than by OEL or its authorized representatives, - Software, media, parts (including consumables), supplies or interfacing components not supplied by OEL - Misuse of the product or any operation or attempted operation of the product outside its written specifications and instructions -Negligence or accidental damage
	Manufacturer consumables (including but not limited to toner, ribbons, ink and drum cartridges) are specifically designed for manufacturer machines, and the use of non-manufacturer products may result in degradation of print quality, loss of advanced functionality (such as colour balancing) and even, in some cases, damage to your printer, fax or multi-function machine. This Warranty does not extend to any print

Product	Manufacturer Warranty Details
	quality degradation, machine malfunction, or damage caused by the use of non-Vendor consumables or refilled Vendor toner or ink cartridges.
ATB, BTP and BTP RFID	**The warranty does not cover:**
	Repair of equipment with no fault found. Additional charges may apply.
	Repair of equipment considered dirty or being beyond economical repair in compliance with common practice including in terms of preventative maintenance. Equipment considered beyond economical repair is equipment presenting simultaneously several failures or equipment that has been repaired with used parts from other equipment (cannibalized equipment).
	Repair of Equipment returned with parts missing, equipment subject to attempted repairs by a third party or equipment not used according to the manufacturer specifications. Equipment used with non-manufacturer parts or non-manufacturer consumables.
	Any refurbishment or retrofit of the equipment
	Technical Consumables (thermal heads, magnetic heads, ribbons…)
BGR	**The warranty does not apply where damage is caused by other factors, including without limitation:**
	• Normal wear and tear
	• Abuse, mishandling, accident or failure to follow operating instructions
	• Damage caused by heavy impact or drop
	• Leaking batteries, exposure to liquid or infiltration of foreign particles
	• Servicing or modification of the product other than by the manufacturer or their authorized service agents
	• Use of the product with other accessories, attachments, product supplies, parts or devices (including batteries) that do not conform to the manufacturer specifications.
	• Dirt and transportation damages due to improper packing of return shipment to manufacturers repair center.
WS, Monitor and Keyboard	**The warranty does not cover:**
	Normal wear and tear
	Repair of damage or defects in supported Products which are purely cosmetic and do not affect device functionality.
	Service for equipment damaged by misuse, accident or abuse of the product and components (such as, but not limited to, use of incorrect line voltages, use of incorrect fuses, use of incompatible devices and accessories, improper or insufficient ventilation or failure to follow operating instructions), modification, unsuitable physical or operating environment, improper maintenance by the Customer (or Customer's agent).

Product	Manufacturer Warranty Details
	Repairs necessitated by software problems, or because of alteration, adjustment, or repair by anyone other than the manufacturer or manufacturer’s authorized representative or by customers utilizing Customer Self Replaceable (CSR) parts.