

**ACS CLOUD SERVICE SCHEDULE  
("EULA Acceptance Form")**

THIS SERVICE SCHEDULE AGREEMENT (the "Agreement") dated \_\_11\_\_/\_January\_/2019 (the "Commencement Date")

BETWEEN:

AeroCloud Systems Inc of Registered Florida office 1900 Main Street Suite 801, Sarasota, Florida,  
34263, USA  
("ACS")

-AND-

Northwest Florida Beaches International Airport of the Panama City-Bay County Airport &  
Industrial District of 6300 W Bay Pkwy, Panama City, FL 32409, USA  
(the "Customer")

**1. BACKGROUND**

The Customer wishes to enter into an agreement with ACS for the provision of a subscription to use the ACS Cloud Service under the terms and conditions defined below and that in the ACS Cloud End User Licence Agreement ("Cloud EULA")

**2. SUBSCRIPTION**

The Customer is granted a subscription to access and use:

- ACS Intelligent Airport Management Cloud Platform ("IAM")
- IAM Modules – Flight Management, Dashboard, Asset Management, GIS, Inspection Management, Document Management, Gate Visualisation, Reference Data Management, Messaging and Notifications, Historical Flight Query.
- AeroCloud Lease Management

**3. SERVICES**

The following services are to be provided as part of this agreement:

- Access to the Cloud Service Platform
- On boarding of the Clients Configuration within the Cloud Service
- Setup of Customers Authorised Users
- Integration with OAG data for real time Flight Schedule Data acquisition

**4. DEPENDENCIES**

The cloud service is dependent on the Customer providing the following:

- Access to the Customers OAG data feed during the term of this subscription.
- Customer having suitable network access to the internet and the Cloud Service

**5. SUBSCRIPTION TERM**

The initial annual subscription term is 3 years from the commencement date, with an option to renew 1 year at a time for a period of 5 years.

*Guil*

## 6. COSTS

Year	Cost Per Year	Subject to increase
1	\$29,100	No increase
2	\$29,100	No increase
3	\$29,100	No increase
4	\$29,100	Subject to CPI Increase
5	\$29,100	Subject to CPI Increase

## 7. USAGE METRICS & RESTRICTIONS

1. Access to the Cloud Service via the subscription is provided for the exclusive use of the Customer and its direct employees.
2. ACS may, at its discretion, grant access to users outside the Customers organisation upon receipt and acceptance of a written request from the Customer stating the nature and reason for such access.
3. Authorised User limit : Unlimited
4. Customer is allocated up to 2GB of Cloud Service storage for the uploading and holding of related documents and images. ACS may increase this limit for the Customer at ACS's sole discretion and may or may not charge an additional fee for the provision of this extra storage. This limit represents approximately 2000 documents and images and is allocated across all Authorised Users.

## 8. DATA PROCESSING

Please refer to separate Data Policy in respect of data usage and privacy whilst using the Cloud Service

## 9. PARTNER

NOT APPLICABLE

## 10. POLICIES

### a) SUPPORT POLICY

Support is provided via a dedicated support email address, to raise a support request please email ACS at [support@aerocloudsystems.com](mailto:support@aerocloudsystems.com). A response to support requests will be provided based upon the agreed issue severity and the SLA response times associated with that priority.

### b) SERVICE LEVEL AGREEMENT POLICY ("SLA")

The Cloud Service is hosted on the Amazon AWS platform and is made available to the Customer on the following basis:

1. Availability of the Cloud Service shall be no less than 99.9%
2. Priority 1 Issues will be responded to within 2 hours of the issue being logged with ACS Support with a target resolution time of 1 working day
3. Priority 2 Issues will be responded to within 12 hours of the issue being logged with ACS Support with a target resolution time of 2 working days.
4. Priority 3 Issues will be responded to within 1 working day of the issue being logged with ACS Support with a target resolution time of 5 working days.
5. Priority 4 Issues will be responded to within 3 working days of the issue being logged with ACS Support with a target resolution time of 10 working days.
6. ACS will determine the priority level of an issue in consultation with the



7. Where an issue is as a result of a fault outside the control of ACS, then ACS will use best endeavours to restore the service as soon as is practically possible in conjunction with the responsible party.
8. In the event of a Priority 1 Issue the Customer will have first ensured that all necessary checks have been performed within their own environments and network to ascertain that the fault does not rest within their own infrastructure.
9. Where a support Issue is raised with ACS Support and the Customer has not performed it's own checks and ACS later finds out that the fault rests with the Customers own infrastructure or network, then ACS reserves the right to charge an Incident Support Fee for this Support Issue. The maximum cap on this charge is \$1000 per incident of this nature.

## 11. NOTICES

All notices to the parties under this agreement are to be provided at the following addresses, or at such addresses as may be later provided in writing:

**AeroCloud Systems Inc** - Registered Florida office  
1900 Main Street Suite 801,  
Sarasota, Florida,  
34263,  
USA

**Northwest Florida Beaches International Airport of the Panama City-Bay County Airport & Industrial District**  
6300 W Bay Pkwy,  
Panama City,  
FL 32409,  
USA

**IN WITNESS WHEREOF** the parties have duly affixed their signature under hand and seal or stamp on this Day 11 of the month of January the year 2019

On behalf of  
(ACS)



Name

GEORGE W. RICHARDSON

Stamp/Seal

(ACS)



On Behalf of  
(Customer)



Name

PARKER W. MCCLELLAN, JR.

Stamp/Seal

(Customer)

NOTE: Capitalized terms used in this document are defined in the Glossary.

## Glossary

- 1.1. **"ACS"** AeroCloud Systems Incorporated.
- 1.2. **"Authorised User"** means any individual to whom Customer grants access authorization to use the Cloud Service that is an employee, contractor or representative of
  - a) Customer
- 1.3. **"Cloud Service"** means any subscription-based, ACS hosted, supported and operated on-demand solution provided to the Customer under the terms of the Cloud Service EULA and this agreement.
- 1.4. **"Cloud EULA"** means a document governing the general terms and conditions for the provision of the Cloud Service.
- 1.5. **"Priority 1 Issues"** are defined as a fault with the Cloud Service that renders the service totally inaccessible or unavailable to the Customer. Issues of this priority are of the highest severity and are issues that render the Cloud Service unavailable to the Customer.
- 1.6. **"Priority 2 Issues"** are defined as a fault with the Cloud Service that renders major areas of the Cloud Services functionality inoperable or unavailable and offer the user no option to operate a workaround to the problem.
- 1.7. **"Priority 3 Issues"** are defined as a fault with the Cloud Service that renders minor areas of the Cloud Services functionality inoperable or unavailable, but the user is able still operate the majority of the system and use a workaround to the problem.
- 1.8. **"Priority 4 Issues"** are defined as a cosmetic issue with the Cloud Service that although not strictly faults with the Cloud Service do present minor usability issues to the Authorised User.
- 1.9. **"Customer Data"** means any content, materials, data and information that Authorised Users enter into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g. Customer-specific reports). Customer Data and its derivatives will not include ACS's Confidential Information.
- 1.10. **"Data Processing Agreement"** is defined in the Cloud EULA Acceptance Form.
- 1.11. **"Documentation"** means ACS's then-current technical and functional documentation as well as any roles and responsibilities descriptions, if applicable, for the Cloud Service which is made available to Customer with the Cloud Service.
- 1.12. **"Partner"** is defined in the Cloud EULA Acceptance Form.
- 1.13. **"ACS Policies"** means the operational guidelines and policies applied by ACS to provide and support the Cloud Service as defined in this agreement and the Cloud EULA.
- 1.14. **"Services"** means professional services related to a Cloud Service, such as implementation, configuration, custom development and training, performed by ACS's employees.
- 1.15. **"SLA"** is the defined Service Levels to be used the provision of this Cloud Service to the Customer.
- 1.16. **"Subscription Term"** means the term of a Cloud Service subscription of which the initial term is identified in this agreement, including all renewals.
- 1.17. **"Supplement"** is any additional supplementary information, service, offering or additional item recorded against the provision of the Cloud Service to the Customer.
- 1.18. **"Support Policy"** is the definition of what support will be provided to the Customer on the Cloud Service.
- 1.19. **"Usage Metric"** means the standard of measurement for determining the permitted use for a Cloud Service as set forth in this agreement.

*Gu*



**GENERAL TERMS AND CONDITIONS FOR AEROCLOUD CLOUD SERVICES  
("CLOUD EULA")**

**1. DEFINITIONS**

Capitalized terms used in this document are defined in the Glossary.

**2. USAGE RIGHTS AND RESTRICTIONS**

**2.1 Grant of Rights.**

Subject to all fees paid by the Partner to ACS, ACS grants to Customer on behalf of Partner a non-exclusive, non-transferable and world-wide right to use the Cloud Service (including its implementation and configuration), Cloud Materials and Documentation solely for Customer's and its Affiliates' internal business operations. Permitted uses and restrictions of the Cloud Service also apply to Cloud Materials and Documentation.

**2.2 Authorized Users.**

Customer may permit Authorized Users to use the Cloud Service. Usage is limited to the Usage Metrics and volumes stated in the Cloud EULA Acceptance Form. Access credentials for the Cloud Service may not be used by more than one individual, but may be transferred from one individual to another if the original user is no longer permitted to use the Cloud Service. Customer is responsible for breaches of the Agreement caused by Authorized Users.

**2.3 Acceptable Use Policy.**

With respect to the Cloud Service, Customer will not:

- (a) disassemble, decompile, reverse-engineer, copy, translate or make derivative works,
- (b) transmit any content or data that is unlawful or infringes any intellectual property rights, or
- (c) circumvent or endanger its operation or security.

**2.4 Verification of Use.**

Customer will monitor its own use of the Cloud Service and report any use in excess of the Usage Metrics and volume to Partner. ACS may monitor use to verify compliance with Usage Metrics, volume and the Agreement. ACS will be permitted to forward any data regarding use in excess of the Usage Metrics, volume and the Agreement by the Customer to Partner.

**2.5 Suspension of Cloud Service.**

ACS may suspend use of the Cloud Service if continued use may result in material harm to the Cloud Service or its users. ACS will promptly notify Customer of the suspension. ACS will limit the suspension in time and scope as reasonably possible under the circumstances.

**2.6 Third Party Web Services.**

The Cloud Service may include integrations with web services made available by third parties that are accessed through the Cloud Service and subject to terms and conditions with those third parties. These third party web services are not part of the Cloud Service and the Agreement does not apply to them.

**2.7 Mobile Access to Cloud Service.**

Authorized Users may access certain Cloud Services through mobile applications obtained from third-party websites such as Android or Apple app store. The use of mobile applications may be governed by the terms and conditions presented upon download/access to the mobile application and not by the terms of the Agreement.

**3. ACS RESPONSIBILITIES**

**3.1 Provisioning.**

ACS provides access to the Cloud Service as described in the Agreement.

**3.2 Support.**

ACS provides support for the Cloud Service as referenced in the Cloud EULA Acceptance Form.

**3.3 Security.**

ACS uses reasonable security technologies in providing the Cloud Service. As a data processor, ACS will implement technical and organizational measures to secure personal data processed in the Cloud Service in accordance with applicable data protection law.

### **3.4 Modifications.**

The Cloud Service and ACS Policies may be modified by ACS at any time. Modifications may include optional new features for the Cloud Service, which Customer may use subject to the then-current Supplement and Documentation.

### **3.5 Analyses.**

ACS may create analyses utilizing, in part, Customer Data and information derived from Customer's use of the Cloud Service and Services. Analyses will anonymize and aggregate information, and will be treated as Cloud Materials. Examples of how analyses may be used include: optimizing resources and support; research and development; automated processes that enable continuous improvement, performance optimization and development of new ACS products and services; verification of security and data integrity; internal demand planning; and data products such as industry trends and developments, indices and anonymous benchmarking.

## **4. CUSTOMER AND PERSONAL DATA**

### **4.1 Customer Data.**

Customer is responsible for the Customer Data and entering it into the Cloud Service. Customer grants to ACS a non-exclusive right to process Customer Data solely to provide and support the Cloud Service.

### **4.2 Personal Data.**

Customer will collect and maintain all personal data contained in the Customer Data in compliance with applicable data privacy and protection laws.

### **4.3 Security.**

Customer will maintain reasonable security standards for its Authorized Users' use of the Cloud Service.

### **4.4 Access to Customer Data.**

- (a)** During the Subscription Term, Customer can access its Customer Data at any time. Customer may export and retrieve its Customer Data in a standard format. Export and retrieval may be subject to technical limitations, in which case ACS and Customer will find a reasonable method to allow Customer access to Customer Data.
- (b)** Before the Subscription Term expires, Customer may use ACS's export tools (as available) to perform a final export of Customer Data from the Cloud Service.
- (c)** At the end of the Agreement, ACS will delete the Customer Data remaining on servers hosting the Cloud Service unless applicable law requires retention. Retained data is subject to the confidentiality provisions of the Agreement.
- (d)** In the event of third party legal proceedings relating to the Customer Data, ACS will cooperate with Customer and comply with applicable law (both at Customer's expense) with respect to handling of the Customer Data.

## **5. PARTNER RELATIONSHIP**

### **5.1 Non-Payment by Partner**

ACS may at its sole discretion suspend Customer's use of the Cloud Service and/or terminate the Agreement if Partner fails to pay any fee or other amount payable by it on its due date.

### **5.2 Termination of partner relationship or orders relating to Customer**

If (i) Partner terminates all orders relating to the Customer or (ii) ACS terminates any of Partner's orders relating to the Customer for good cause or (iii) the partnership between ACS and Partner relating to the sale of subscription for the Cloud Services is terminated, ACS may (depending on Customer's choice):



- (a) directly provide the affected Cloud Service to the Customer pursuant to ACS's then-current General Terms and Conditions for ACS Cloud Services for mutually-agreed subscription fees; or
- (b) recommend to Customer other partners or third parties for the provision of the affected Cloud Service.

## **6. TERM AND TERMINATION**

### **6.1 Term.**

The initial Subscription Term is as stated in the Cloud EULA Acceptance Form.

### **6.2 Termination.**

- (a) A party may terminate the Agreement:
  - (i) upon thirty days written notice of the other party's material breach (including without limitation Customer's failure to pay Partner any fees due for the Cloud Service) unless the breach is cured during that thirty day period,
  - (ii) immediately, if the other party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors, or otherwise materially breaches Sections 11 or 12.6.
- (b) ACS may terminate the Agreement if the relevant Cloud Services that this Agreement pertains to were terminated between ACS and Partner.
- (c) Customer may terminate the Agreement by providing 60 days advanced written notice prior of annual renewal. In such event, Customer shall pay all costs that are due to ACS prior to the termination date but shall not be responsible for costs after for the terminated agreement.

### **6.3 Effect of Expiration or Termination.**

- (a) Customer's right to use the Cloud Service and all ACS Confidential Information will end,
- (b) Confidential Information of the disclosing party will be returned or destroyed as required by the Agreement, and
- (c) termination or expiration of the Agreement does not affect other agreements between the parties.

### **6.4 Survival.**

Sections 6.3, 6.4, 8, 9, 10, 11, and 12 will survive the expiration or termination of the Agreement.

## **7. WARRANTIES**

### **7.1 Compliance with Law.**

Customer warrants its current and continuing compliance with all laws and regulations applicable to it in connection with the Customer Data and Customer's use of the Cloud Service.

### **7.2 Good Industry Practices.**

ACS Warrants that:

- (a) the Cloud Service will substantially conform to the specifications contained in the Documentation during the Subscription Term for the Cloud Services.
- (b) the Service will materially conform to the specifications contained in the Documentation, Cloud EULA Acceptance Form, statement of work, deployment description or other documentation containing the scope and service description for the relevant Service in all cases agreed to by ACS at the point in time the relevant Service is performed by ACS and it will perform any Service in a workmanlike and professional manner using resources with the skills reasonably required to perform such Services.

### **7.3 Remedy.**

- (a)** Provided Customer (and/or Partner on Customer's behalf) notifies ACS in writing with a specific description of the Cloud Service's or the Service's nonconformance with the warranty in Section 7.2 within the warranty period without undue delay and ACS validates the existence of such nonconformance, ACS will, at its option:
  - (i)** with regard to the Cloud Services:
    - (a)** correct or replace the nonconforming Cloud Service, or
    - (b)** if ACS fails to correct the nonconformance after using reasonable commercial efforts, terminate the access to the nonconforming Cloud Service.
  - (ii)** with regard to the Services, re-perform the nonconforming Service.
- (a)** This does not apply to trivial or non-material cases of nonconformance and is Customer's sole and exclusive remedy under the warranty in Section 7.2. The written notification of any nonconformance by Customer (and/or Partner on Customer's behalf) must include sufficient detail for ACS to analyse the alleged nonconformance. Customer must provide commercially reasonable assistance to ACS in analysing and remediating any nonconformance of the Cloud Service and Service.
- (b)** For clarification purposes, ACS will,
  - (i)** with regard to the Cloud Services: in all cases; and
  - (ii)** with regard to the Services: if ACS fails to correct the nonconformance of the Service after using reasonable commercial effort, consult with Partner to define a reasonable amount **(a)** by which Partner may reduce the subscription fees or the fees for the nonconforming Service, in case Partner has not already paid them, or **(b)** if Partner has already paid the subscription fees or the fees for the nonconforming Service, which ACS will refund to Partner to reflect the nonconformance.
- (c)** ACS may fulfill its warranty obligations vis-à-vis Partner or Customer. To the extent that ACS fulfills its warranty obligations vis-à-vis Partner, Customer will not have any claim against ACS for a breach of the warranty in Section 7.2.

### **7.4 System Availability.**

- (a)** ACS warrants to maintain an average monthly system availability for the production system of the Cloud Service as defined in the SLA or Supplement.

### **7.5 Warranty Exclusions.**

The warranties in Sections 7.2 and 7.4 will not apply if:

- (a)** the Cloud Service is not used in accordance with the Agreement or Documentation,
- (b)** the nonconformance is caused by Partner, Customer, another third party, or by any product, database, content or service not provided by ACS, or
- (c)** the Cloud Service was provided for no fee or is a trial license of the Cloud Service or both.

### **7.6 Disclaimer.**

Except as expressly provided in the Agreement, neither ACS nor its subcontractors make any representation or warranties, express or implied, statutory or otherwise, regarding any matter, including the merchantability, suitability, originality, or fitness for a particular use or purpose, non-infringement or results to be derived from the use of or integration with any products or services provided under the Agreement, or that the operation of any products or services will be secure, uninterrupted or error free. Customer agrees that it is not relying on delivery of future functionality, public comments or advertising of ACS or product roadmaps in obtaining subscriptions for any Cloud Service.



## **8. THIRD PARTY CLAIMS**

### **8.1 Claims Brought Against Customer.**

- (a)** ACS will defend Customer against claims brought against Customer by any third party alleging that Customer's use of the Cloud Service infringes or misappropriates a patent claim, copyright or trade secret right. ACS will indemnify Customer against all damages finally awarded against Customer (or the amount of any settlement ACS enters into) with respect to these claims.
- (b)** ACS's obligations under Section 8.1 will not apply if the claim results from (i) Customer's breach of Section 2, (ii) use of the Cloud Service in conjunction with any product or service not provided by ACS, or (iii) use of the Cloud Service provided for no fee.
- (c)** In the event a claim is made or likely to be made, ACS may (i) procure for Customer the right to continue using the Cloud Service under the terms of the Agreement, or (ii) replace or modify the Cloud Service to be non-infringing without a material decrease in functionality. If these options are not reasonably available, ACS may terminate Customer's subscription to the affected Cloud Service upon written notice.

### **8.2 Claims Brought Against ACS.**

Customer will defend ACS against claims brought against ACS by any third party related to Customer Data. Customer will indemnify ACS against all damages finally awarded against ACS (or the amount of any settlement Customer enters into) with respect to these claims.

### **8.3. Third Party Claims Procedure.**

- (a)** The party against whom a third party claim is brought will timely notify the other party in writing of any claim, reasonably cooperate in the defense and may appear (at its own expense) through counsel reasonably acceptable to the party providing the defense.
- (b)** The party that is obligated to defend a claim will have the right to fully control the defense.
- (c)** Any settlement of a claim will not include a financial or specific performance obligation on, or admission of liability by, the party against whom the claim is brought.

### **8.4 Exclusive Remedy.**

The provisions of Section 8 state the sole, exclusive, and entire liability of the parties, their Business Partners and subcontractors to the other party, and is the other party's sole remedy, with respect to covered third party claims and to the infringement or misappropriation of third party intellectual property rights.

## **9. LIMITATION OF LIABILITY**

### **9.1 Not Responsible.**

ACS and its licensors will not be responsible under this Agreement (i) if a Cloud Service is not used in accordance with the Documentation, or (ii) if the defect or liability is caused by Partner, Customer, any third-party product or service or use of the Cloud Service in conjunction with any product or service not provided by ACS, or (iii) for any Customer activities not permitted under this Agreement. ACS AND ITS LICENSORS WILL NOT BE LIABLE FOR ANY CLAIMS OR DAMAGES ARISING FROM INHERENTLY DANGEROUS USE OF ANY OF THE CLOUD SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT.

### **9.2 Exclusion of Damages; Limitation of Liability.**

Anything to the contrary herein notwithstanding, except for (a) damages resulting from (i) unauthorized use or disclosure of confidential information; and (ii) death or personal injury arising from either party's gross negligence or arising from either party's willful misconduct, or (b) ACS's obligations under Section 8.1 or (c) Customer's obligations under Section 8.2, under no circumstances and regardless of the nature of any claim will ACS its licensors or Customer be liable to each other or any other person or entity for an amount in excess of the subscription fees paid by Customer to Partner in the twelve months period immediately preceding the events giving rise to the claim for the Cloud Services directly causing the damages or be liable in any amount for special, incidental, consequential or indirect damages, loss of good will or profits, work stoppage, data loss, computer failure or malfunction, attorney's fees, court costs, interest or exemplary or punitive damages.

### **9.3 Risk Allocation.**

This Agreement allocates the risks between ACS and Customer. The subscription fees paid by Customer reflect this allocation of risk and limitations of liability. It is expressly understood and agreed that each and every provision of this Agreement which provides for a limitation of liability, disclaimer of warranties or exclusion of damages, is intended by the parties to be severable and independent of any other provision and to be enforced as such.

## **10. INTELLECTUAL PROPERTY RIGHTS**

### **10.1 ACS Ownership.**

ACS own all intellectual property rights in and related to the Cloud Service, Cloud Materials, Documentation, Services, design contributions, related knowledge or processes, and any derivative works of them. All rights not expressly granted to Customer are reserved to ACS.

### **10.2 Customer Ownership.**

Customer retains all rights in and related to the Customer Data. ACS may use Customer provided trademarks solely to provide and support the Cloud Service.

### **10.3 Non-Assertion of Rights.**

Customer covenants, on behalf of itself and its successors and assigns, not to assert against ACS any rights, or any claims of any rights, in any Cloud Service, Cloud Materials, Documentation, or Services.

## **11. CONFIDENTIALITY**

### **11.1 Use of Confidential Information.**

- (a) The receiving party will protect all Confidential Information of the disclosing party as strictly confidential to the same extent it protects its own Confidential Information, and not less than a reasonable standard of care. Receiving party will not disclose any Confidential Information of the disclosing party to any person other than its personnel, representatives or Authorized Users whose access is necessary to enable it to exercise its rights or perform its obligations under the Agreement and who are under obligations of confidentiality



substantially similar to those in Section 11. Customer will not disclose the Agreement or the pricing to any third party.

- (b) Confidential Information of either party disclosed prior to execution of the Agreement will be subject to Section 11.
- (c) In the event of legal proceedings relating to the Confidential Information, the receiving party will cooperate with the disclosing party and comply with applicable law (all at disclosing party's expense) with respect to handling of the Confidential Information.

#### **11.2 Exceptions.**

The restrictions on use or disclosure of Confidential Information will not apply to any Confidential Information that:

- (a) is independently developed by the receiving party without reference to the disclosing party's Confidential Information,
- (b) is generally available to the public without breach of the Agreement by the receiving party,
- (c) at the time of disclosure, was known to the receiving party free of confidentiality restrictions, or
- (d) the disclosing party agrees in writing is free of confidentiality restrictions.
- (e) is required to be disclosed by applicable law.

#### **11.3 Publicity.**

Neither party will use the name of the other party in publicity activities without the prior written consent of the other, except that Customer agrees that ACS may use Customer's name in customer listings or quarterly calls with its investors or, at times mutually agreeable to the parties, as part of ACS's marketing efforts (including reference calls and stories, press testimonials, site visits, ACS participation). Customer agrees that ACS may share information on Customer with its Affiliates for marketing and other business purposes and that it has secured appropriate authorizations to share Customer employee contact information with ACS.

### **12. MISCELLANEOUS**

#### **12.1 Severability.**

If any provision of the Agreement is held to be invalid or unenforceable, the invalidity or unenforceability will not affect the other provisions of the Agreement.

#### **12.2 No Waiver.**

A waiver of any breach of the Agreement is not deemed a waiver of any other breach.

#### **12.3 Electronic Signature.**

Electronic signatures that comply with applicable law are deemed original signatures.

#### **12.4 Regulatory Matters.**

- (a) ACS Confidential Information is subject to export control laws of various countries, including the laws of the United States, EU, Ireland and Germany. Customer will not submit ACS Confidential Information or parts thereof to any government agency for licensing consideration or other regulatory approval, and will not export, re-export or import any ACS Confidential Information or parts thereof to countries, persons or entities if prohibited by export laws.
- (b) ACS assumes no responsibility or liability:
  - (i) for any delay caused in the delivery and/or granting of access to any or all ACS Confidential Information of parts thereof due to export or import authorizations or both having to be obtained from the competent authorities;

- (ii) if any required authorization, approval or other consent for the delivery of and/or granting of access to any or all ACS Confidential Information or parts thereof cannot be obtained from the competent authorities;
- (iii) if the delivery of and/or granting of access to any or all ACS Confidential Information or parts thereof is prevented due to applicable Export Laws; and
- (iv) if access to Cloud Services, Services or other services has to be limited, suspended or terminated due to applicable Export Law.

#### **12.5 Notices.**

All notices will be in writing and given when delivered to the address set forth in an Cloud EULA Acceptance Form with copy to the legal department. Notices by ACS relating to the operation or support of the Cloud Service may be in the form of an electronic notice to Customer's authorized representative or administrator identified in the Cloud EULA Acceptance Form.

#### **12.6 Assignment.**

Without ACS's prior written consent, Customer may not assign or transfer the Agreement (or any of its rights or obligations) to any party.

#### **12.7 Subcontracting.**

ACS may subcontract parts of the Cloud Service or Services to third parties. ACS is responsible for breaches of the Agreement caused by its subcontractors.

#### **12.8 Relationship of the Parties.**

The parties are independent contractors, and no partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties is created by the Agreement.

#### **12.9 Force Majeure.**

Any delay in performance (other than for the payment of amounts due) caused by conditions beyond the reasonable control of the performing party is not a breach of the Agreement. The time for performance will be extended for a period equal to the duration of the conditions preventing performance.

#### **12.10 Governing Law.**

The Agreement and any claims relating to its subject matter will be governed by and construed under the laws of the State of Florida, without reference to its conflicts of law principles. All disputes will be subject to the exclusive jurisdiction of the courts located in the Commonwealth of Delaware. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act (where enacted) will not apply to the Agreement. Either party must initiate a cause of action for any claim(s) relating to the Agreement and its subject matter within one year from the date when the party knew, or should have known after reasonable investigation, of the facts giving rise to the claim(s).

#### **12.11 Entire Agreement.**

The Agreement constitutes the complete and exclusive statement of the agreement between ACS and Customer in connection with the parties' business relationship related to the subject matter of the Agreement. All previous representations, discussions, and writings (including any confidentiality agreements) are merged in and superseded by the Agreement and the parties disclaim any reliance on them. The Agreement may be modified solely in writing signed by both parties, except as permitted under Section 3.4. An Agreement will prevail over terms and conditions of any Customer-issued purchase order, which will have no force and effect, even if ACS accepts or does not otherwise reject the purchase order.



## Glossary

- 1.1 **"ACS"** AeroCloud Systems Incorporated.
- 1.2 **"Affiliate"** of a party means any legal entity in which a party, directly or indirectly, holds more than fifty percent (50%) of the entity's shares or voting rights. Any legal entity will be considered an Affiliate as long as that interest is maintained.
- 1.3 **"Agreement"** is defined in the Cloud EULA Acceptance Form.
- 1.4 **"Authorized User"** means any individual to whom Customer grants access authorization to use the Cloud Service that is an employee, agent, contractor or representative of
  - (a) Customer,
  - (b) Customer's Affiliates, and/or
  - (c) Customer's and Customer's Affiliates' Business Partners.
- 1.5 **"Business Partner"** means a legal entity that requires use of a Cloud Service in connection with Customer's and its Affiliates' internal business operations. These may include customers, distributors, service providers and/or suppliers of Customer.
- 1.6 **"Cloud EULA Acceptance Form"** means the "ACS Cloud Service Schedule (for indirect sales)" concluded between ACS and the Customer that references the CLOUD EULA.
- 1.7 **"Cloud Service"** means any subscription-based, ACS hosted, supported and operated on-demand solution provided by ACS on behalf of the Partner to the Customer under the Cloud EULA Acceptance Form.
- 1.8 **"Cloud Materials"** mean any materials provided or developed by ACS (independently or with Partner's and/or Customer's cooperation) in the course of performance under the Agreement, including in the delivery of any support or Services to Customer. Cloud Materials do not include the Customer Data, Customer Confidential Information or the Cloud Service.
- 1.9 **"Confidential Information"** means
  - (a) with respect to Customer: (i) the Customer Data, (ii) Customer marketing and business requirements, (iii) Customer implementation plans, and/or (iv) Customer financial information, and
  - (b) with respect to ACS: (i) the Cloud Service, Documentation, Cloud Materials and analyses under Section 3.5, and (ii) information regarding ACS research and development, product offerings, pricing and availability.
  - (c) Confidential Information of either ACS or Customer also includes information which the disclosing party protects against unrestricted disclosure to others that (i) the disclosing party or its representatives designates as confidential at the time of disclosure, or (ii) should reasonably be understood to be confidential given the nature of the information and the circumstances surrounding its disclosure.
- 1.10 **"Customer Data"** means any content, materials, data and information that Authorized Users enter into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g. Customer-specific reports). Customer Data and its derivatives will not include ACS's Confidential Information.
- 1.11 **"Data Processing Agreement"** is defined in the Cloud EULA Acceptance Form.
- 1.12 **"Documentation"** means ACS's then-current technical and functional documentation as well as any roles and responsibilities descriptions, if applicable, for the Cloud Service which is made available to Customer with the Cloud Service.
- 1.13 **"Partner"** is defined in the Cloud EULA Acceptance Form.
- 1.14 **"ACS Policies"** means the operational guidelines and policies applied by ACS to provide and support the Cloud Service as incorporated in an Cloud EULA Acceptance Form.
- 1.15 **"Services"** means professional services related to a Cloud Service, such as implementation, configuration, custom development and training, performed by ACS's employees or subcontractors as described in the Cloud EULA Acceptance Form and which are governed by the Consulting Services Supplement or similar agreement for Services.
- 1.16 **"SLA"** is defined in the Cloud EULA Acceptance Form.
- 1.17 **"Subscription Term"** means the term of a Cloud Service subscription of which the initial term is identified in the applicable Cloud EULA Acceptance Form, including all renewals.
- 1.18 **"Supplement"** is defined in the Cloud EULA Acceptance Form.

**1.19 "Support Policy"** is defined in the Cloud EULA Acceptance Form.

**1.20 "Usage Metric"** means the standard of measurement for determining the permitted use for a Cloud Service as set forth in a Cloud EULA Acceptance Form.



## **PERSONAL DATA PROCESSING AGREEMENT FOR ACS CLOUD SERVICES**

### **1. BACKGROUND**

#### **1.1 Purpose.**

This document is a data processing agreement ("DPA") between ACS and Customer and applies to Personal Data provided by Customer and each Data Controller in connection with their use of the Cloud Service. It states the technical and organizational measures ACS uses to protect Personal Data that is stored in the production system of the Cloud Service.

#### **1.2 Governance.**

Customer is solely responsible for administration of all requests from other Data Controllers. Customer will bind any other Data Controller it permits to use the Cloud Service to the terms of this DPA.

### **2. APPENDICES**

Customer and its Data Controllers determine the purposes of collecting and processing Personal Data in the Cloud Service. Appendix 1 states the measures ACS applies to the Cloud Service, unless the Agreement states otherwise.

### **3. ACS OBLIGATIONS**

#### **3.1 Instructions from Customer.**

ACS will follow instructions received from Customer (on its own behalf or on behalf of its Data Controllers) with respect to Personal Data, unless they are (i) legally prohibited or (ii) require material changes to the Cloud Service. ACS may correct or remove any Personal Data in accordance with the Customer's instruction. If ACS cannot comply with an instruction, it will promptly notify Customer (email permitted).

#### **3.2 Data Secrecy.**

To process Personal Data, ACS will only use personnel who are bound to observe data and telecommunications secrecy under the Data Protection Law.

#### **3.3 Technical and Organizational Measures.**

- (a) ACS will use the appropriate technical and organizational measures stated in Appendix 1.
- (b) Appendix 1 applies to the production system of the Cloud Service. Customer should not store any Personal Data in non-production environments.
- (c) ACS provides the Cloud Service to ACS's entire customer base hosted out of the same data center and receiving the same Cloud Service. Customer agrees ACS may improve the measures taken in Appendix 1 in protecting Personal Data so long as it does not diminish the level of data protection.

#### **3.4 Security Breach Notification.**

ACS will promptly inform Customer if it becomes aware of any Security Breach.

#### **3.5 Cooperation.**

At Customer's request, ACS will reasonably support Customer or any Data Controller in dealing with requests from Data Subjects or regulatory authorities regarding ACS's processing of Personal Data.

### **4. CERTIFICATIONS AND AUDITS**

#### **4.1 Customer Audits.**

Customer or its independent third party auditor may audit ACS's security practices relevant to Personal Data processed by ACS only if:

- (a) ACS has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate). Upon Customer's request ISO certifications are available through ACS;
- (b) A Security Breach has occurred;

- (c) Customer or another Data Controller has reasonable grounds to suspect that ACS is not in compliance with its obligations under this DPA;
- (d) An audit is formally requested by Customer's or another Data Controller's data protection authority; or
- (e) Mandatory Data Protection Law provides Customer with a direct audit right.

#### **4.2 Audit Restrictions.**

The Customer audit will be limited to once in any twelve month period, and limited in time to a maximum of 3 business days and scope as reasonably agreed in advance between the parties. Reasonable advance notice of at least sixty days is required, unless Data Protection Law requires earlier audit. ACS and Customer will use current certifications or other audit reports to minimize repetitive audits.

Customer and ACS will each bear their own expenses of audit, unless the Customer is auditing under Section 4.1 (c) (unless such audit reveals a breach by ACS in which case ACS shall bear its own expenses of audit), 4.1 (d) or 4.1 (e). In those cases, Customer will bear its own expense and the cost of ACS's internal resources required to conduct the audit. If an audit determines that ACS has breached its obligations under the Agreement, ACS will promptly remedy the breach at its own cost.

### **5. DEFINITIONS**

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

**"ACS"** means AeroCloud Systems Inc.

**"Data Center"** means the location where the production instance of the Cloud Service is hosted for the Customer in its region. The Cloud Service is hosted on Amazons AWS Cloud Infrastructure using Locations based in their North American Data Centers.

**"Data Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

**"Data Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**"Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

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

**"Personal Data"** means any information relating to a Data Subject For the purposes of this DPA, it includes only personal data entered by Customer or its Authorized Users into or derived from their use of the Cloud Service. It also includes personal data supplied to or accessed by ACS in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data.

**"Security Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, or disclosure of Customer Personal Data or Confidential Data, or (2) similar incident involving Personal Data for which a Data Processor is required under applicable law to provide notice to the Data Controller.



## **Appendix 1 – Technical and Organizational Measures**

### **1. TECHNICAL AND ORGANIZATIONAL MEASURES**

The following sections define the ACS's current security measures. ACS may change these at any time without notice so long as it maintains a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

#### **1.1 Physical Access Control.**

ACS's Cloud Infrastructure is hosted on Amazon's AWS and is access controlled by their own policies and procedures which can be found at <https://aws.amazon.com/compliance> and <https://aws.amazon.com/security/>

#### **1.2 System Access Control.**

Data processing systems used to provide the ACS Services must be prevented from being used without authorization.

##### Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. ACS controls the creation of users within the system to ensure only valid authorized users have the appropriate access.
- All users access ACS's systems with a unique identifier (user ID).
- ACS has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, his or her access rights are revoked.
- The ACS network is protected from the public network by firewalls.
- Security patch management is implemented to ensure regular and periodic deployment of relevant security updates.
- Full remote access to ACS's critical cloud infrastructure is protected by strong authentication.

#### **1.3 Data Access Control.**

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

##### Measures:

- Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing personal, confidential or other sensitive information are regularly checked.
- ACS does not allow the installation of personal software or other software that has not been approved by ACS.

#### **1.4 Data Transmission Control.**

Except as necessary for the provision of the Services in accordance with the relevant service agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Personal Data transfer over ACS internal networks are protected in the same manner as any other confidential data.

- When data is transferred between ACS and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of ACS-controlled systems (e.g. data being transmitted outside the firewall of the ACS Data Center).

### **1.5 Data Input Control.**

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from ACS data processing systems.

#### Measures:

- ACS only allows authorized persons to access Personal Data as required in the course of their work.
- ACS has implemented a logging system for input & modification, or blocking of Personal Data by ACS within ACS's Products and Services to the fullest extent possible.

### **1.6 Availability Control.**

Personal Data will be protected against accidental or unauthorized destruction or loss.

#### Measures:

- ACS employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary.
- The Data Centers use uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability.
- ACS has defined contingency plans as well as business and disaster recovery strategies for the provided Services.

### **1.7 Data Separation Control.**

Personal Data collected for different purposes can be processed separately.

#### Measures:

- ACS uses the technical capabilities of the deployed software (for example: multi-tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customers have access only to their own data.
- If Personal Data is required to handle a support incident from a specific customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

### **1.9 Data Integrity Control .**

Personal Data will remain intact, complete and current during processing activities.

#### Measures:

ACS has implemented a multi-layered defence strategy as a protection against unauthorized modifications.

In particular, ACS uses the following to implement the control and measure sections described above.

In particular:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;



**CONTRACT ADDENDUM**

**THIS CONTRACT ADDENDUM** dated this 10th day of MAY, 2021

**BETWEEN:**

AeroCloud Systems Inc of Registered office 1900 Main Street Suite 801, Sarasota, Florida, 34263, USA

**OF THE FIRST PART**

**-AND-**

Northwest Florida Beaches International Airport of the Panama City-Bay County Airport & Industrial District Of 6300 W Bay Pkwy, Panama City, FL 32409, USA

**OF THE SECOND PART****Background**

- A. AeroCloud Systems Inc and Northwest Florida Beaches International Airport (the "Parties") entered into the contract (the "Contract") dated 11<sup>th</sup> January 2019, for the purpose of ACS Cloud Service Subscription.
- B. The Parties desire to amend the Contract on the terms and conditions set forth in this Contract Addendum (the "Agreement").
- C. This Agreement is the first amendment to the Contract.
- D. References in this Agreement to the Contract are to the Contract previously amended or varied.

**IN CONSIDERATION OF** the Parties agreeing to amend their obligations in the existing Contract, and other valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to keep, perform, and fulfil the promises, conditions and agreements below:

**Amendments**

1. The contract is amended as follows:
  - a. **Subscription.** Addition of AeroCloud GMS with Forward Planning Subscription and extension of overall current contract till 11<sup>th</sup> January 2027.
  - b. **Subscription Term + Costs**

Year (Effective Date)	Cost	Subject to Increase
11 <sup>th</sup> January 2022- 11 <sup>th</sup> January 2023	\$39,987	No Increase
11 <sup>th</sup> January 2023- 11 <sup>th</sup> January 2024	\$39,987	No Increase
11 <sup>th</sup> January 2024- 11 <sup>th</sup> January 2025	\$39,987	No Increase
11 <sup>th</sup> January 2025- 11 <sup>th</sup> January 2026	\$39,987	Subject to CPI Increase
11 <sup>th</sup> January 2026- 11 <sup>th</sup> January 2027	\$39,987	Subject to CPI Increase

**No Other Change**

- c. Except as otherwise expressly provided in this Agreement, all of the terms and conditions of the Contract remain unchanged and in full force and effect.

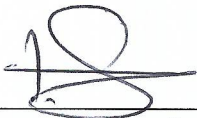
**Miscellaneous Terms**

- d. Capitalised terms not otherwise defined in this Agreement will have the meanings ascribed to them in the Contract. Headings are inserted for convenience of the parties only and are not to be considered when interpreting this Agreement. Words in the singular mean and include the plural and vice versa. No regard for gender is intended by the language in this Agreement.



**Governing Law**

- e. The Agreement and any claims relating to its subject matter will be governed by and construed under the laws of the state of Florida, without reference to its conflicts of law principles. All disputes will be subject to the exclusive jurisdiction of the courts located in the state of Florida.

IN WITNESS WHEREOF the Parties have duly affixed their signatures under hand and seal on this 10<sup>th</sup> day of MAY, 2021.

  
WITNESS: IAN FULDE - SMITH  
ADDRESS: 1900 MAIN STREET  
SUITE 801, SARASOTA, FLORIDA  
34263, USA

\_\_\_\_\_  
WITNESS: \_\_\_\_\_  
ADDRESS: \_\_\_\_\_

  
  
AEROCLLOUD SYSTEMS INC CEO AEROCLLOUD SYSTEMS INC  
Reg. EL Office (Party)  
1900 Main Street Suite 801  
Sarasota, Florida  
34263, USA

\_\_\_\_\_  
\_\_\_\_\_(Party)