# PERSONAL DATA PROCESSING AGREEMENT FOR ACS CLOUD SERVICES

1. **BACKGROUND**
	1. **Purpose.**

This document is a data processing agreement (“**DPA**”) between the GSA Multiple Award Schedule (MAS) Contractor acting on behalf of 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.

# 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.

# 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.

# ACS OBLIGATIONS

* 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).

# 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.

# Technical and Organizational Measures.

* + 1. ACS will use the appropriate technical and organizational measures stated in Appendix 1.
		2. Appendix 1 applies to the production system of the Cloud Service. Customer should not store any Personal Data in non-production environments.
		3. 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.

# Security Breach Notification.

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

# 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.

# CERTIFICATIONS AND AUDITS

* 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:

* + 1. 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;
		2. A Security Breach has occurred;
		3. Customer or another Data Controller has reasonable grounds to suspect that ACS is not in compliance with its obligations under this DPA;
		4. An audit is formally requested by Customer’s or another Data Controller’s data

protection authority; or

* + 1. Mandatory Data Protection Law provides Customer with a direct audit right.

# Audit Restrictions.

The Customer’s 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 Customer and the GSA MAS Contractor. 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. If an audit determines that ACS has breached its obligations under the Agreement, ACS will promptly remedy the breach at its own cost.

# DEFINITIONS

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

**“ACS”** means AeroCloud Systems Incorporated or 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.

# Physical Access Control.

ACS’s Cloud Infrastructure is hosted on Amazons AWS and is access controlled by their own policies and procedures which can be found in Exhibit A.

# 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.

# 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.

# 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 Purchase Order. 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).

# 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.

# 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.

# 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.

# Data Integrity Control.

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

ACS has implemented a multi-layered defense 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

Exhibit A







