**Memorandum of Understanding and Agreement (MOU/A)**

**Between**

**VA Nebraska-Western Iowa Health Care System**

**Omaha, NE**

**and**

**U.S. Department of Veterans Affairs**

**Enterprise Cloud Solutions Office**



**January 28, 2019**

*Version 1.0*

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Revision** | **Description** | **Author** |
| January 24, 2019 | 1.0 | MOU/A Between VA Nebraska-Western Iowa Health Care System and  VA ECSO | VAECSO Tom Spinelli |
| January 30, 2019 | 1.1 | Major revision to include Solution Delivery missing elements | COMS Robert Guajardo |

**Table of Contents**

[1 Purpose 1](#_Toc535570277)

[1.1 Supporting Policy Memos 1](#_Toc535570278)

[2 Scope 2](#_Toc535570279)

[3 Services and Products to Be Provided 2](#_Toc535570280)

[4 Incident Reporting 3](#_Toc535570281)

[5 Terms of Agreement 3](#_Toc535570282)

[6 Changes 3](#_Toc535570283)

[7 Points of Contact 3](#_Toc535570284)

[7.1 VistA System Owner 4](#_Toc535570285)

[7.2 VA ECSO 4](#_Toc535570286)

[7.3 Nebraska-Western Iowa Health Care System 4](#_Toc535570287)

[8 Execution 4](#_Toc535570288)

[9 Signatory Authority 4](#_Toc535570289)

[10 Appendix - Acronyms 5](#_Toc535570290)

## Purpose

In anticipation of the closure of St Louis, Missouri (SMO) Defense Enterprise Computing Center (DECC) in early 2020, which currently hosts seventy (70) Veteran Information System Technology Architecture (VistA) systems, the VA Office of Information and Technology (OI&T) Enterprise Cloud Solutions Office (ECSO), as the technology agent for the Veterans Health Administration (VHA), is providing migration and continuity of services for VistA systems in the VA Enterprise Cloud (VAEC).

VAEC is provisioned in a physically distinct and private U.S.-government data center in the continental United States (CONUS) operated by Amazon Web Services (AWS). The AWS GovCloud regions are accredited to the highest Federal Risk and Authorization Management Program (FedRAMP) security controls available to the U.S. government in accordance with the Federal Information Security Management Act (FISMA) and Federal Information Processing Standards (FIPS). The migration of VistA to AWS GovCloud will thus provide the highest level of security, reliability, scalability, and continuity of Veteran care services for all VHA end-users of VistA currently possible.

In support of this endeavor, VA ECSO is requesting a current copy of the Omaha Pre-Production VistA databases currently hosted in the DISA data center for purposes of auditing, adaptive maintenance, testing, scaling, and preparation for production deployment in the VAEC. Transition to the VAEC will enable comprehensive cloud-based security and continuity of services for VHA VistA users.

The purpose of this Memorandum of Understanding/Agreement (MOU/A) is to document the agreement between VA Nebraska-Western Iowa VistA system owner and the VA Enterprise Cloud Solutions Office (VAECSO).

This MOU/A outlines the processes employed to ensure adequate privacy and security safeguards by VA ECSO prior to production deployment to the field using the Pre-Production (Test) database from Omaha, and to ensure proper care, access, handling and disposal of the data is accomplished when it has been determined that any data is no longer required for pre-production testing and production deployment purposes.

### Supporting Policy Memos

1.1.1 On January 16, 2018, Executive Director, Strategic Sourcing, Executive Director Demand Management Division, jointly issued a policy memo on the “Use of the VA Enterprise Cloud (VAEC) to Host Applications.”

1.1.2 On April 10, 2018, Deputy Assistant Secretary (DAS), EPMO issued a policy memo on “Use of Software-as-a-Service (SaaS), Managed Services, and Cloud-Based Native Technologies and Approaches”

* + - 1. In this memo, DAS EPMO directs the ECSO to require the use of cloud native technologies and approaches with the VAEC-AWS and VAEC-Azure environments whenever optimal for the implementation of VA Cloud Strategy
      2. This memo also establishes ECSO as the governing authority for the approaches used to implement cloud native technology and processes.

1.1.3 On January 7, 2019, Principal DAS (PDAS), OIT issued a policy memo mandating the use of the VAEC for New Development.

## Scope

The VA ECSO is responsible for data management, complying with all conditions of use, establishment, and maintenance of all applicable security policies, processes and procedures as specified in this Agreement to prevent unauthorized access to the data. As such, it is understood that the VA ECSO will meet the following responsibilities in its use of the VistA database:

* + Access to any personally identifiable patient or employee information (PII/PHI) provided by the facility will be limited to authorized personnel working under VA ECSO-approved Project teams. It should be noted that the VA ECSO staff includes contractors who will need access to this database for set up and testing purposes. Access will not be granted until all security and privacy requirements for background checks, training, and business associate agreements are completed.
  + Use of the data covered under this agreement other than for those uses specified herein, must be justified by the requestor and approved by the VAEC Chief Information Systems or Area Manager, and Information Security Officer at the VAEC prior to use.
  + VA ECSO will treat the entire database as containing sensitive data, and as such, any printouts from the database will be handled and disposed of in accordance with VA and Veterans Health Administration (VHA) information security and privacy policies and procedures.
  + If/when it has been documented that the database is no longer required for any purpose, project, or program, the VA ECSO PM shall confirm in writing with the relevant VA ECSO Team the decision to remove the database. VA ECSO is responsible for removing and destroying the data from the system in accordance with VA and VHA media sanitization policies to prevent unauthorized access.
  + All VA ECSO-approved project personnel will access the data in the VAEC in accordance with the minimum necessary standards outlined in VHA Handbook 1605.2.
  + All VA ECSO-approved project personnel with access to the data must have completed all required VA Privacy and Information Security Training.
  + Existing, approved production applications that connect to VISTA and which are also hosted ​*within* ​VAEC may be connected directly to the VA EC-based VISTA with no additional approvals or gateways required. Connection of applications/environments to VISTA that are hosted ​*outside* ​VAEC will use VA trusted gateways as required, such as the Trusted Internet Connection (TIC).
  + When an employee leaves a Project, the individual’s access to the database will be terminated.

## 3 Services and Products to Be Provided

Services and products to be provided entails the transfer of a copy of the facility’s pre-production VistA from the DISA/DECC to the VAEC Test/Dev network in complete production-testable form. The preferred method utilizes Secure File Transfer Protocol (SFTP).

The steps to securely transfer a copy of the Omaha VistA datasets are as follows:

1. The VAEC Point of Contact (POC) will make contact with the Omaha POC.
2. The Omaha POC will create a new Test account and place a copy of the pre-production VistA database files in this account. .
3. Upon a mutually agreed upon date, the VAEC POC will SFTP the Test account datasets to an encrypted EBS storage location in VAEC.
4. The VAEC COMS POC will migrate the Test account data to an encrypted S3 bucket for rapid secure access and installation into a primary and secondary VAEC Cache instance.

After the Test account database is loaded into the encrypted VAEC S3 bucket, the VA POC is responsible for performing the following actions after the VA ECSO teams approved VistA back-end and front-end VistA servers have been created and make available to the VAEC POC:

1. The VAEC POC will install Cache 2017 onto the Cache servers.
2. The VAEC POC will access the secure S3 bucket to install the copied datasets into the VAEC Cache primary and secondary instances with the assistance of the VA COMS POC.
3. The VAEC POC will christen the domain to establish its new identity.

If transfer by SFTP is unavailable, alternative VA approved data transfer methods can be discussed with the VAEC POC and the Omaha POC. Any alternate data transfer method must be approved for use by the VA OIT ECSO team and program.

## 4 Incident Reporting

The VA OIT official discovering a security incident involving data provided under this agreement will report it internally in accordance with the established incident reporting procedures, and to the corresponding POC in the facility as listed in this MOU/A so that the incident can be appropriately managed and reported within both organizations. Contact information for both the facility and VA OIT staff will be included in the MOU/A.

## 5 Terms of Agreement

This Agreement is effective upon the date of the signature of the last party signing this Agreement and will remain in effect for eighteen months after the last date of signatures in the signature block below. If the parties wish to extend this agreement, they may do so by reviewing, updating, and reauthorizing this agreement. The newly-signed agreement should explicitly supersede this agreement, which should be referenced by title and date. If one or both parties wish to terminate this agreement prematurely, they may do so upon thirty (30) days advance notice or in the event of a security incident that necessitates an immediate response. Upon termination, all data and media associated with this agreement will be removed from VAEC systems and destroyed in accordance with VA and VHA media sanitization policies.

## 6 Changes

This Agreement may be modified by the mutual agreement of both parties upon thirty (30) calendar days of notification, or sooner if the parties so desire. Any notification will be made in writing and signed by both parties. This Agreement, or any of its specific provisions, may be modified only by the signature approval of the parties’ signatory to the Agreement or designees or by their respective official successors.

## 7 Points of Contact

The following individuals are key POCs for purposes of coordinating changes to this Agreement or other technical and administrative issues that may arise.

### 7.1 VistA System Owner

**Vanessa Davis, VistA System Owner**

Email: [Vanessa.Davis@va.gov](mailto:Vanessa.Davis@va.gov)

Phone: (240) 432-4869

### 7.2 VA ECSO

**David Catanoso, Director VAECSO**

Email: [David.Catanoso@va.gov](mailto:David.Catanoso@va.gov)

Phone: 732-440-9583

### 7.3 VA Nebraska-Western Iowa Health Care System

**Gail Graham, Director, VHA Central Iowa Medical Center**

Email: [gail.graham@va.gov](mailto:gail.graham@va.gov)

Phone: 515.699.5850

## 8 **Execution**

This successor Memorandum of Understanding and Agreement is executed this \_\_29th day of January 2019 .

## 9 **Signatory Authority**

We, the undersigned, mutually agree to the terms of this agreement.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

David Catanoso Date

Director, VA Enterprise Cloud Services Office

Email: [David.Catanoso@va.gov](mailto:David.Catanoso@va.gov)

Phone: 732-440-9583

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Gail Graham Date

Director, VHA Central Iowa Medical Center

Email: [gail.graham@va.gov](mailto:gail.graham@va.gov)

Phone: 515.699.5850

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Charles Solomon-Jackson Date

DCSD Cloud ISSO, IT Operations and Services

Email: [Charles.Solomon-Jackson@va.gov](mailto:Charles.Solomon-Jackson@va.gov)

Phone: (909) 583-6307

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Vanessa Davis Date

VistA System Owner

Email: [Vanessa.Davis@va.gov](mailto:Vanessa.Davis@va.gov)

Phone: 240-432-4869

## 10 **Appendix - Acronyms**

**Table 1: Acronyms**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| AWS | Amazon Web Services |
| DECC | Defense Enterprise Computing Center |
| DISA | Defense Information Systems Agency |
| ECSO | Enterprise Cloud Solutions Office |
| CONUS | Continental United States |
| FedRAMP | Federal Risk and Authorization Management Program |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| MOU/A | Memorandum of Understanding/Agreement |
| OIT | Office of Information and Technology |
| PHI | Protected Health Information |
| PII | Personal Identifiable Information |
| POC | Point of Contact |
| VA | U.S. Department of Veterans Affairs |
| VAEC | VA Enterprise Cloud |
| VAECSO | VA Enterprise Cloud Services Office |
| VHA | Veterans Health Administration |
| VISTA | Veterans Health Information Systems and Technology Architecture |