# U.S. Department of Veterans Affairs

# VAEC Application Onboarding Form
## for
## [Application Name Here]

Version v.1.0

## Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 12/11/2017 | 0.1 | Initial Draft | Daniel Beaver/<br>Wilbert Francis<br>CSRA/MPG |
| 12/11/2017 | 0.2 | Reviewed Draft | Peter Davies<br>CSRA/MPG |
| 10/12/2018 | 0.3 | Revised Draft | VAEC COMS Team/Cognosante |
| 11/19/2018 | 1.0 | Updated and finalize for signature | VAEC COMS Team/Cognosante |

We, the undersigned, approve the content of this Application Onboarding Form for the VA Enterprise Cloud (VAEC) Microsoft Azure Government High and Amazon Web Services (AWS) GovCloud High.

David Catanoso 337416

Digitally signed by David Catanoso 337416
Date: 2018.11.21 13:52:38 -05'00'

David Catanoso

Director

Enterprise Cloud Solutions Office (ECSO)

Joseph A Fourcade 269563

Digitally signed by Joseph A Fourcade 269563
Date: 2018.11.21 14:50:57 -05'00'

Joseph Fourcade
Program Manager
Enterprise Cloud Solutions Office (ECSO)

# Table of Contents


1 INTRODUCTION ..... 3

1.1 PURPOSE ..... 3
1.2 PROJECT DESCRIPTION ..... 3
1.3 ESTIMATED TIMELINE ..... 3
1.4 OVERVIEW ..... 3
1.5 AUTHORITY TO OPERATE (ATO) ..... 5
1.6 ARCHITECTURE DIAGRAM ..... 5

2 CATEGORIZATION, OPERATIONS AND HANDLING ..... 5

2.1 AVAILABILITY AND SERVICE LEVELS ..... 5
2.2 SECURITY CATEGORIZATION ..... 7
2.3 CONTINGENCY PLAN ..... 8
2.4 BACKUP AND RETENTION POLICY ..... 8

3 SERVICE DESK AND SUPPORT TRIAGE ..... 9

3.1 INCIDENT MANAGEMENT AND SERVICE DISRUPTION ..... 9
3.2 VA APPLICATION SUPPORT STRUCTURE ..... 9

4 SPECIAL SECURITY INFORMATION ..... 10

4.1 GENERAL INFORMATION ..... 11
4.2 SECURITY HISTORY ..... 11
4.3 KNOWN ISSUES ..... 12

5 CUSTOMER RESPONSIBILITY MATRIX ..... 13

5.1 CLOUD RESPONSIBILITY MATRIX WORKSHEET ..... 13

# 1 INTRODUCTION

## 1.1 Purpose

The purpose of this document is to provide application-specific information to VA personnel in support of any application brought into the VA Enterprise Cloud (VAEC). Please fill in the blanks appropriately and provide all the details possible concerning the nature of your application.

Many elements requiring your input will be surrounded in square brackets or in italics; however, do not limit yourself to just the provided template. This document is intended to facilitate the best possible support for your application in the VAEC environment. Allow this to be a useful exercise as you provide us valuable information about your application.

## 1.2 Project Description

*Provide a general description of what the project does. Describe elements of the project that leverages cloud technology. Include a description of what components will operate in the cloud and what components will operate on premise (if applicable).*

## 1.3 Estimated Timeline

*Provide a very high level estimated timeline related to this project's implementation in the cloud.*

## 1.4 Overview

[Application name] will be utilizing the following cloud model(s):

| Cloud Model | | |
|---|---|---|
| # | **Type of Cloud Service** | *(click checkbox)* |
| 1 | Platform as a Service (PaaS) | ☐ |
| 2 | Software as a Service (SaaS) | ☐ |

| | | |
|---|---|---|
| 3 | Infrastructure as a Service (IaaS) | ◯ |

**Table 1 – Cloud Model**

**Software as a Service (SaaS)** - Customer uses provider's applications over a network

**Platform as a Service (PaaS)** - Customer deploys their own applications to a cloud

**Infrastructure as a Service (IaaS)** - Customer rents processing, storage, network capacity, and other basic computing resource

[Application name] is the application used by [organization name] for [function] within the VAEC. This application is used by [user base[1]]. It consists of the following components:

| # | Software Product | Current Licenses | Future Licenses |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |

**Table 2 – Software Product(s)**

The application utilizes the following technologies and dependencies:

| # | Technology / Dependency | Description |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |

**Table 3 – Technologies/Dependencies**

[1] For example: General Public, Veterans, Administrators, Health Professionals, etc.

***Note:*** *The above list should include but not be limited to: hostnames, web servers, certificates, frameworks, content delivery packages, languages, libraries, modules, vendor products, host services, ports, protocols, and internal/external dependencies. If this application has dependencies to other projects/applications/systems operating in the VAEC environment, identify each and briefly describe the dependency.*

### 1.5 Authority to Operate (ATO)

Application/System RiskVision Name: [Application Name]

Date ATO granted: [Date issued]

Date ATO Expires: [Date Expires]

For applications **without an ATO**, refer to "ATO Cloud Security Process_Nov_19_2018_v2.0.docx" to complete the ATO process prior to proceeding with VAEC Onboarding.

### 1.6 Architecture Diagram

The following diagram provides an overview of the infrastructure and architecture inherent to this application.

[Insert current application diagram]

## 2 CATEGORIZATION, OPERATIONS AND HANDLING

### 2.1 Availability and Service Levels

Some applications/systems require being available for certain periods of time, for example, either 24x7, 9-5, or weekends. Please provide the expected hours of availability for your application:

**Expected hours of availability:** [Availability time period]

Some applications/systems have periods during the year where user activity peaks higher than usual. For example, high volume healthcare enrollment period, major streaming of Department special events, etc.

**Special peak periods:** [list times and details]

The application has the following Interconnection Agreements:

| # | Type[2] | System/Application | Expiration Date |
|---|---|---|---|
| 1 | | | |

[2] For example: Service Level Agreement(s) (SLA), Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA).

| | | | |
|---|---|---|---|
| 2 | | | |
| 3 | | | |

**Table 4 – Interconnection Agreement(s)**

### 2.2 Security Categorization

This application [does/does not] store, process, and/or transmit Protected Health Information (PHI) or Personally Identifiable Information (PII). The Personally Identifiable Information (PII) and/or Protected Health Information (PHI) stored, processed, or transmitted by this application includes:

| # | Type[3] | Description |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |

**Table 5 – Security Categorization**

**For systems with an existing ATO, the below information can be found in RiskVision and the application/system SSP, section 1.2.**

| Security Objective | **Ranking** (Low/Moderate/High) |
|---|---|
| Confidentiality | |
| Integrity | |
| Availability | |

**Table 6 – Security Objective Ranking**

It has been determined that the baseline security categorization for the system is as follows:

| Security Categorization | |
|---|---|

**Table 7 – Baseline Security Categorization**

[3] For example: Social Security Number, Health Records, Date of Birth, etc.

### 2.3 Contingency Plan

The following Business Impact Assessment is currently in place for this application/system:

| # | Application Services/Components | RTO[4] | RPO[5] |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

**Table 8 – Application/System RTO / RPO**

### 2.4 Backup and Retention Policy

The following backup and retention policies should be implemented in the VA environment:

[List any relevant requirements]

[4] Recovery time objective (RTO) is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels. The RTO defines the point in time after a failure or disaster at which the consequences of the interruption become unacceptable.

[5] A recovery point objective (RPO) is the maximum acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs

# 3 SERVICE DESK AND SUPPORT TRIAGE

Service Management processes are enabled by the VA National Service Desk (NSD), 1-855-673-4357.

## 3.1 Incident Management and Service Disruption

When incidents are assigned to technical support groups that manage and respond to incidents, they will use this document to guide them in the resolution process, including reading details about starting and stopping the application, enlisting vendors for support, or corresponding with the following application support groups to troubleshoot the issue.

VA will facilitate and lead the resolution of any issue related to service disruption. This includes the coordination of contractor staff and the inclusion of key VA stakeholder teams. VA will also triage all incidents as defined by Standard Operating Procedures (SOPs) and escalate as appropriate with other contractors.

Please list application/system personnel responsible for incident response, in the order that they should be contacted.

| # | POC Name | Email | Phone |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

## 3.2 VA Application Support Structure

Application/System Owner:

| # | Name | Phone Number | Email Address |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

Information Security Officer:

| # | Name | Phone Number | Email Address |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

Operational Support Team(s):

| # | Name | Phone Number | Email Address |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

Vendor Support Team(s):

| # | Name | Phone Number | Email Address |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

**Application Manager:**

| # | Name | Phone Number | Email Address |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

**System Steward(s):**

| # | Name | Phone Number | Email Address |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

## 4 SPECIAL SECURITY INFORMATION

The following sections will enable the VAEC Security Team to provide the appropriate service regarding this specific application. Please provide answers to the questions below.

### 4.1 General Information

Does this application have any other components or services not covered elsewhere in this document?

| |
|---|
| [Identify any relevant information] |

### 4.2 Security History

Has this application been subject to security assessments or vulnerability scans in the past?

| # | Scan Type *(Host / Static Code / Dynamic Application)* | Scan Tool *(Nessus / BigFix / McAfee / Other)* | Performed By | Date | Scan Result/ Comments |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |

**Table 9 – Past Security Scans**

### 4.3 Known Issues

Is any portion of the application especially fragile or volatile?

| |
|---|
| [Identify any relevant information] |

Are there any known vulnerabilities associated with this application (include Nessus plugin # and severity of finding, if applicable)?

| |
|---|
| [Identify any relevant information] |

Should any portion of this application be exempt from vulnerability scanning for any reason? For example, past history of vulnerability scans crashing the application.

| |
|---|
| [Identify any relevant information] |

# 5 CUSTOMER RESPONSIBILITY MATRIX

The Customer Responsibility Matrix (CRM) documents the application security control baseline requirements and the requisite roles and responsibility for each team and cross-functional department. The CRM describes the actions VAEC customers must take to comply with NIST and VA security control requirements for maintaining an ATO. The document lists the requisite controls and the responsible party for the control origination/responsibility.

## 5.1 Cloud Responsibility Matrix Worksheet

Refer to “VAEC_CustomerResponsibilityMatrix_Nov_8_2018_Draft_v07.xlsx".