Project Change Request 1

To Addendum 5

for to Addendum 5 Access Sonoma Migration to the Cloud

This Project Change Request 1 (this "PCR") dated May 17, 2021 and executed as an amendment to the Addendum 5 dated May 14 2020 between International Business Machines Corporation ("Contractor") and County of Sonoma ("CoS" or "County" or "Client"). In the event of a conflict between the terms of the Addendum 5 and the terms of this PCR1, the terms of this PCR1 shall govern.

1. Project Background

The County together with Contractor has completed Phase 1, 2, 3, 4 and 5 of a multiphase initiative to support ACCESS Sonoma County ("ACCESS" or "ACCESS Sonoma") to address the needs of the most vulnerable residents who are often high or multi-need utilizers of County Safety Net services. The Sonoma County Safety Net Departments have received approval to execute this Project Change Request 1 to the Addendum 5 with IBM for the ACCESS Sonoma Migration to the Cloud.

This PCR1 the services for provisioning, installation, data migration, integration activities, testing, and final deployment activities for Migration to the Cloud.

This PCR1 also includes the reselling and management of Microsoft-Azure™ Government cloud resources and empowers IBM to act on behalf of Microsoft™ regarding provisioning and managing direct contact with the Microsoft Corporation. Under this agreement, IBM will register the Sonoma County Tenancy in the Microsoft-Azure™ Government cloud to enable subscription access to Microsoft-Azure™ cloud resources including Infrastructure as a Service (IaaS), Platform Services (PaaS), and Software as a Service (SaaS) licensing (collectively "MSFT-Azure").

Under this agreement, supported by the IBM and the Microsoft Cloud Solution Provider ("CSP") partnership and the attached Appendix A - Microsoft™ Cloud Agreement ("MCA"), IBM will deliver access to MSFT-Azure through a Sonoma County Tenancy. IBM will provide consumption reporting through Azure Portal™, provisioning, billing, and direct Microsoft Support for MSFT-Azure.

The attached MCA is binding through and made part of this contract. IBM will attest to the inclusion of it in the CSP and Microsoft™ will manage directly with Sonoma County and IBM any periodic changes via Microsoft's electronic MCA acceptance process. Changes there are made part of this agreement.

A Microsoft™ electronic agreement must be accepted and on file with Microsoft™ in order to start using the MSFT-Azure resources.

2. Project Scope

The PCR includes a 3 year fixed price Microsoft Azure equipment subscription, 3 year fixed price managed service, and services to migrate ACCESS to the could that will be performed by the Contractor on a time and materials (T&M) basis. The County and Contractor will implement and deliver technology to enable the use of the ACCESS SONOMA system in accordance with the capabilities outlined within this contract addendum.

2.1. Services to Migrate ACCESS to the Cloud

The County and Contractor will implement and deliver technology to enable the use of the ACCESS SONOMA system in accordance with the capabilities listed below. Contractor shall perform activities, within the schedule and hours allotted, such as assist in:

1. Kickoff Cloud Migration Activities with both IBM and Sonoma County
2. Provision Cloud infrastructure, components, and subscriptions/licenses as agreed to in section 6.1 The Azure Cloud Services
3. Move the following ACCESS Sonoma Connect360 components to cloud:
    a. API server application
    b. User workspace application
    c. ACE (App Connect Enterprise)
    d. MDM
    e. DB2
    f. Cognos
    g. DataStage
4. Deploy Connect360 components identified for cloud migration into the virtual machines on cloud.
5. Integrate the County on-premise data source systems with Connect360 infrastructure over a secured site-to-site VPN tunnel.
6. Change All IP Addresses and hostnames when servers and services are migrated to the Cloud platform.
7. Migrate Existing DB2 data in current on-premises infrastructure to the cloud.
8. Migrate WCM-Connect360 interface to AppID based WCM authentication.
9. Complete Regression and System Integration Testing on UAT and Production cloud environments for the following Components
    a. API server application
    b. User workspace application
    c. ACE (App Connect Enterprise)
    d. MDM
    e. DB2
    f. Cognos
    g. DataStage
10. Provide Testing Results to county and Conduct Go/No Go Decision

2.1.1. Assumptions:

1. IBM will set up a new Tenancy for Sonoma only if one does not exist, otherwise, IBM will add a Subscription to the current Sonoma tenant.
2. Connect360 API server application will be securely exposed over public internet.
3. Connect360 applications would continue to authenticate off the Sonoma Active Directory. Application user credentials should be available on the Sonoma AD.
4. The Sonoma County ISD team will continue to operate and maintain any on-premises infrastructure as they do today. Backup and Restore procedures for all on-premises artifacts

(LDAPS Active Directory server, BizTalk server, DataStage server) will need to leverage standard backup methods and tools, as per Sonoma County's Standard Operating Procedures.

5. MS Azure provides Azure Resource Manager (ARM) templates that can help in automating deployments and use the practice of infrastructure as code. The required target infrastructure will be defined in code to ensure parity is maintained between the PROD and TEST environments.
6. ARM templates will be created for the target environment's infrastructure, as depicted in the diagrams in above sections. These templates allow creating and deploying an entire Azure infrastructure declaratively with repeatable results. ARM Templates are idempotent, which means that the same template can be deployed many times and still get the same resource types in the same state.
7. Connect360 API server application will be securely exposed over public internet.
8. Connect360 applications would continue to authenticate off the Sonoma Active Directory. Application user credentials should be available on the Sonoma AD.
9. The Sonoma County ISD team will continue to operate and maintain any on-premises infrastructure as they do today. Backup and Restore procedures for all on-premises artifacts (LDAPS Active Directory server, BizTalk server, DataStage server) will need to leverage standard backup methods and tools, as per Sonoma County's Standard Operating Procedures.
10. MS Azure provides Azure Resource Manager (ARM) templates that can help in automating deployments and use the practice of infrastructure as code. The required target infrastructure will be defined in code to ensure parity is maintained between the PROD and TEST environments.
11. ARM templates will be created for the target environment's infrastructure, as depicted in the diagrams in above sections. These templates allow creating and deploying an entire Azure infrastructure declaratively with repeatable results. ARM Templates are idempotent, which means that the same template can be deployed many times and still get the same resource types in the same state.
12. Service disruption during actual cutover (Go Live) will be unavoidable. The service disruption will be at a maximum of 48 hours of possible downtime.
13. User Acceptance Testing will not be conducted, IBM's testing results will be provided during go/ no go meeting.
14. Sonoma County currently has a tenant with Microsoft Azure Cloud for Government and has already accepted Microsoft's Customer Service Agreement. Therefore, the MSA attached in Appendix A is for information purposes only.

2.1.2. Cloud platform

IBM shall be using the Microsoft Azure Cloud within US Government region as the target environment, to host the ACCESS Sonoma infrastructure. MS Azure US Government cloud ensures that any resources deployed in this specific region shall always stay within United States. The same constraint will also apply on the data contained within the Azure resources. This is outlined further in section 6.1. The Azure Cloud Services

2.1.3. Data Migration

Connect360 solution within ACCESS Sonoma enterprise maintains all its data within the DB2 database servers in PROD and TEST environments. This database contains following schemas where appropriate data is parked:

- CONNECT360_APP: Application data
- CONNECT360_MDM: MDM data
- CONNECT360_INT: Integration ODS data

During the cutover period, these database instances will be backed up on the on-premises DB2 servers and readied to be migrated into the target environment.

It is important to clearly differentiate between the migration of an application (and its associated data) and the actual cutover to the new instance of the application on the target Cloud platform. Applications will be "migrated" to the target Cloud platform in the relatively early stages to enable testing at all levels including Cloud Infrastructure Acceptance Test (CIAT), application Functional Testing and Non-Functional Testing.

For different Connect360 applications, the cutover will involve a synchronisation of replicated data and a network "move" to the VLAN production and re-routing of interfaces to the application in the new Production environment in the cloud.

One of the aims of this plan is to minimise the amount of work required during the cutovers to reduce risk and enable the transfer of services to be completed within the limited time available.

As part of migrating into the Target Environment, a "copy" of above database schemas will be established in the target Cloud platform, to the point where it is ready for application remediation in the target environment.

2.2. Microsoft Azure

Access to the MSFT-Azure resources described in this SOW will be available for Sonoma County to begin usage within 8 weeks from the agreed estimated start date (as stated within the signature acceptance section under agreed upon start date) for MSFT-Azure detailed in Exhibit B – Microsoft Client Agreement and based on when Sonoma County electronically agrees to the electronic MCA.

Under this project, IBM will provide:

Azure Subscriptions under a Tenancy as outlined in and solely subject to the Microsoft Cloud Agreement in Appendix A

IBM will additionally be providing a Managed Services for MSFT-Azure Government only under this PCR1 as described in Section 6.3. Cloud Managed Services

3. MSFT-Azure Governance

IBM and Sonoma County will meet as agreed on a regular scheduled basis to review MSFT-Azure performance, and to share planning information as part of managed services. IBM will schedule and conduct required review meetings and inform Sonoma County of required attendees.

The following review meetings will be held:

3.1. Monthly Touch Point and Review

In the event Helpdesk Tickets are opened with Microsoft by IBM or Sonoma County, IBM and Sonoma County will review and address immediately:

a) actions that were a carry-over from a prior meeting or ticket submission
b) Change Log review
c) outstanding Helpdesk Tickets; and
d) upcoming scheduled milestones and/or events

3.2. Quarterly Financial Review

IBM and Sonoma County will review and address:

a) prior period performance, any outstanding issues, backlog, risks, or items needing special attention / escalation for resolution
b) invoices from the previous quarter
c) actual consumption against plan
d) requested changes to monthly billing
e) key changes scheduled for the following quarter that will impact project financials; and
f) forecast discussions (i.e., planned/un-planned increases or decreases in MSFT-Azure consumption).

4. Definitions

4.1. The Azure Cloud Services

The following table specifies the equipment and configurations that will be provisioned in the MSFT-Azure cloud by IBM.

Table 1 Azure BOM Assumptions

Service type	Custom name	Region	Description
Virtual Machines	Cognos on WebSphere	US Gov Virginia	2 B8MS (8 vCPUs, 32 GB RAM); Linux – Red Hat Enterprise Linux; 3 year reserved; 0 managed disks – E1, 1,000 transaction units; Inter Region transfer type, 5 GB outbound data transfer from US Gov Virginia to US Gov Texas
Virtual Machines	InfoSphere IIS/DataStage	US Gov Virginia	2 B8MS (8 vCPUs, 32 GB RAM); Linux – Red Hat Enterprise Linux; 3 year reserved; 0 managed disks – S4, 10,000 transaction units; Inter Region transfer type, 5 GB outbound data transfer from US Gov Virginia to US Gov Texas
Virtual Machines	Database	US Gov Virginia	4 DS14 v2 (16 vCPUs, 112 GB RAM); Linux – Red Hat Enterprise Linux; 3 year reserved; 0 managed disks – S4, 100,000 transaction units; Inter Region transfer type, 5 GB outbound data transfer from US Gov Virginia to US Gov Texas
Virtual Machines	AD Domain Controllers	US Gov Virginia	1 B8MS (8 vCPUs, 32 GB RAM); Windows – (OS Only); 3 year reserved; 0 managed disks – S4, 1,000 transaction units; Inter Region transfer type, 5 GB outbound data transfer from US Gov Virginia to US Gov Texas

VPN Gateway	VNET Mgmt	US Gov Virginia	VPN Gateways, VpnGw2 tier, 756 gateway hour(s), 10 S2S tunnels, 128 P2S tunnels, 0 GB, Inter-VNET VPN gateway type
Load Balancer	Load Balancer - PROD	US Gov Virginia	Standard Tier: 5 Rules, 5,000 GB Data Processed
Load Balancer	Load Balancer - UAT	US Gov Virginia	Standard Tier: 5 Rules, 5,000 GB Data Processed
Azure Active Directory		US Gov Virginia	10 users Premium P1, 5 users Premium P2, Enterprise tier, 730 directory objects, User forest hours {5, Resource forest hours {7}.
Storage Accounts	VMs	US Gov Virginia	Managed Disks, Premium SSD, P10 Disk Type 5 Disks, Pay as you go
Storage Accounts	Database	US Gov Virginia	Managed Disks, Premium SSD, P30 Disk Type 4 Disks, 1 year reserved
Azure Backup	VMs	US Gov Virginia	Azure VMs, 5 Instance(s) x 128 GB, GRS Redundancy, Low Average Daily Churn, 1,024 GB Average monthly backup data, 13 GB Average monthly snapshot usage data
Azure Backup	Databases	US Gov Virginia	Azure VMs, 4 Instance(s) x 1 TB, GRS Redundancy, Low Average Daily Churn, 6 TB Average monthly backup data, 1 TB Average monthly snapshot usage data
Azure Backup	ARO Master Nodes	US Gov Virginia	Azure VMs, 3 Instance(s) x 1,028 GB, GRS Redundancy, Low Average Daily Churn, 4,934 GB Average monthly backup data, 62 GB Average monthly snapshot usage data
Azure Backup	ARO Worker Nodes	US Gov Virginia	Azure VMs, 4 Instance(s) x 128 GB, GRS Redundancy, Low Average Daily Churn, 819 GB Average monthly backup data, 10 GB Average monthly snapshot usage data
Azure Red Hat OpenShift	ARO - PROD	US Gov Virginia	Red Hat OpenShift 4, 4 x D16s v3 Worker nodes, 4 disks, 3 x D8s v3 Master nodes, 3 disks
Bandwidth	Total Bandwidth consumption	US Gov Virginia	Internet egress, 2 TB outbound data transfer from US Gov Virginia routed via Microsoft Global Network
Azure Site Recovery	Disaster Recovery (DR)	US Gov Virginia	0 Customer instances, 16 Azure instances
Storage Accounts	DR - VMs	US Gov Virginia	Managed Disks, Premium SSD, LRS Redundancy, P10 Disk Type 5 Disks; Pay as you go
Storage Accounts	DR - Databases	US Gov Virginia	Managed Disks, Premium SSD, LRS Redundancy, P30 Disk Type 4 Disks; Pay as you go
Storage Accounts	DR - ARO master	US Gov Virginia	Managed Disks, Premium SSD, LRS Redundancy, P30 Disk Type 3 Disks; Pay as you go

Storage Accounts	DR - ARO worker	US Gov Virginia	Managed Disks, Premium SSD, LRS Redundancy, P10 Disk Type 4 Disks; Pay as you go

Note, the County will provide 4 Red Hat Enterprise License Operation Systems - 8 vCPU VM and 4 Red Hat Enterprise License Operation Systems - 16 vCPU VM

4.2. Azure Availability SLAs

a) This link (https://azure.microsoft.com/en-us/support/legal/sla/) shows the current Microsoft-Azure Service Level Agreements ("MSFT-Azure SLA's") that are incorporated herein by reference.

4.3. Cloud Managed Services

IBM will provide managed services for the MSFT-Azure cloud as shown in the table below.

Table 2 Azure Cloud Managed by IBM, Platform-as-a-Service

Service	Description
Remote Access Management	Provides management of remote access accounts to the Clients' hosted and managed environments.
SIOC-SIEM	Security Information and Event Management (SIEM) for systems, monitored by the SIOC 24x7x365
SIOC-AV/HIPS	Antivirus and Host Intrusion Prevention Systems (HIPS) for systems, monitored by the SIOC 24x7x365
SIOC-System Scan	System vulnerability scans conducted by the SIOC with weekly scan reports send to the Client.
SIOC-Baseline Scan	Compliance scanning for Client hosts against security configuration baselines (i.e., CIS Benchmarks, or DISA STIGs)
Systems Administration - Linux	Client Operating System maintenance, including patching, vulnerability remediation, tuning, troubleshooting and issue resolution - Linux
Data Backup Management	Backup and restoration of client data using the CSP native tools and systems, which includes scheduling backup jobs, resolving failed backup job issues and conducting restoration activities to retrieve and restore data when requested.
Enterprise System Management (ESM)	Monitor the core functions of availability, performance, and event management. including 24x7x365 monitoring networks, systems and critical business services with real-time alerting, ticketing, notification and reporting capabilities.
Enterprise Operation Center - EOC	Respond to incident alarms and events of Client system that are monitored by FIMS, 24x7x365. This service is only available for systems monitored by the ESM service.
Service Desk - Medium (11-25)	Record and track incidents, problems, requests and change activity in the FIMS ticketing system (11-25)
Network and Firewall Management	Administration of firewalls, networks and VLANs within the tenant boundary. This includes management of the security zones, routes and ports that reside on physical and/or virtual infrastructure, which is separate from the management of the physical device itself.

Service	Description
Load Balancer Administration	Administration of Client load balancing needs, both physical and virtual
DS&P Oversight	DS&P Oversight and management allows for IBM's DS&P consultant to monitor the projects client and technical environments, identifying contractual, regulatory requirements and security risks while translating all of this into needed DS&P controls. These controls will be in place for the lifespan of the project. See appendix C for additional responsibilities
Project Oversight	Project oversight includes both Database Administrator and Project Manager The Database Administrator oversite to manage vulnerabilities, updates, patches, penetration testing and Access Sonoma Deployments The Project Manager will provider oversight of the overall Manages Services project for the lifespan of the project. Their responsibilities will include, but are not limited to, working with the onboarded IBM team to identify any risks to the program, conduct Monthly and Quarterly Managed Service Reviews with the county, review and monitor and any security risks, respond to questions or concerns, record and track escalations, billing, and communicating patches/deployments

5. IBM Responsibilities

5.1. Project Management

An IBM Project Manager will establish a framework for project planning, communications, reporting, procedural and contractual activity, and other activities associated with the Services, and will:

a) Create a Project Workplan for services to deliver

b) Review the SOW and the contractual responsibilities of both parties with the Sonoma County Project Manager

c) Maintain project communications through the Sonoma County Project Manager

d) Review, with respect to only the MSFT-Azure, the IBM standard invoice format and billing procedure to be used on the project, with the Sonoma County Project Manager

e) Coordination of Help Activities to facilitate the MSFT-Azure Subscriptions:

   a. Respond to L2 & L3 requests from Sonoma County for MSFT-Azure issues
   b. If there is a requirement, facilitate and resolve L3 Help requests with Microsoft

f) Coordination of the CSP service desk are provided by IBM, as part of the SOW review, IBM and Sonoma County will mutually agree to the process to contact the CSP Service desk.

g) Review the Monthly Consumption Reporting and Billing

h) Conduct Quarterly True Up Meetings

5.2. Project Kickoff

IBM will facilitate, for the MSFT-Azure scope of this agreement, a project kickoff meeting for up to two (2) hours with Sonoma County selected participants day 1 of the project or on a mutually agreed date and time.

IBM will:

a) discuss project team roles and responsibilities;

b) review this statement of work;

Completion Criteria:

IBM has conducted the kickoff meeting.

5.3. Assist Sonoma with Microsoft Support

IBM will coordinate support directly with Microsoft. Sonoma County is responsible for basic Helpdesk support within Sonoma County and will direct only MSFT-Azure specific help requests to IBM CSP Support as defined in the project kickoff.

IBM will assist Sonoma County as follows:

A. Manage Support directly with Microsoft during the contract coverage hours;

B. IBM will use IBM's Microsoft Premier Support agreements to manage any L3 help requests outside of stated contract coverage

Sonoma County agrees to: Route MSFT-Azure support request to IBM CSP Support as defined in the kickoff

Completion Criteria: this is an ongoing task for the duration of the contract

5.4. Resources and Hours of Coverage

C. Work under this SOW will be performed at IBM facility or remotely.

D. IBM may use personnel and resources in locations worldwide and third-party suppliers to support the delivery of products and services.

E. IBM will provide the Services under this SOW during normal business hours, 8:00 AM to 6:00 PM Eastern Time, except national holidays

6. Sonoma County Responsibilities

IBM's performance is dependent upon Sonoma County fulfillment of its responsibilities at no charge to IBM. Any delay or idle time in performance of Sonoma County's responsibilities may result in additional charges and/or delay of the completion of the Services and will be handled in accordance with the Project Change Control Procedure.

While Sonoma County is engaged in a services agreement in which IBM is providing enhanced services, Sonoma County will list IBM as the "Partner of Record" for that specific engagement. The Partner of Record is the partner or organization who helped or is helping with design, build, deploy and/or manage MSFT-Azure resources for a specific engagement, but not necessarily the partner who sold the subscriptions. By assigning the partner of record, Sonoma County will secure IBM's support for Azure deployments and provide visibility to usage and account activities for the solution IBM delivers.

6.1. Sonoma County Project Manager

Prior to the start of this project, Sonoma county will designate an ACCESS Sonoma Project Manager to whom all communications relative to this project will be addressed and who will have the authority to act on behalf of Sonoma County in all matters regarding this SOW. The ACCESS Sonoma Project Manager's responsibilities include the following:

a) Manage Sonoma County personnel and responsibilities for this project.

b) Serve as the interface between IBM and all Sonoma County departments participating in the project.

c) Administer the Project Change Control Procedure with the IBM Project Manager.

d) Participate in project meetings.

e) Obtain and provide information, data, and decisions within 3 working days of IBM's request unless Sonoma County and IBM agree in writing to a different response time.

f) Review and accept deliverables submitted by IBM in accordance with the Deliverable Acceptance Procedure.

g) Help resolve project issues and Sonoma County's deviations from the estimated schedule, and escalate issues within Sonoma County organizations, as necessary; and

h) Review with the IBM Project Manager any Sonoma County invoice/billing requirements. Such requirements that deviate from IBM's standard invoice format or billing procedures may affect price and will be managed through the Project Change Control Procedure.

6.2. Other Sonoma County Responsibilities

Sonoma County will:

a) ensure IBM delivers value to ACCESS Sonoma with Microsoft's support. Sonoma County will assign IBM as "Partner of Record" for the County's MSFT-Azure implementation project. The Partner of Record is the partner or organization who helped or is helping with design, build, deploy and/or manage the MSFT-Azure solution. By assigning the partner of record, Sonoma County will secure IBM's support for Azure deployment services and provide visibility to usage and account activities for the solution IBM delivers.

b) provide safe access, suitable office space, supplies, high speed connectivity to the Internet, and other facilities needed by IBM personnel while working at Sonoma County's location. The IBM project team will be located in an area adjacent to Sonoma County's project personnel, and all necessary security badges and clearance will be provided for access to this area.

c) ensure that Sonoma County staff is available to provide such assistance as IBM reasonably requires and that IBM is given reasonable access to Sonoma County senior management, as well as any members of its staff to enable IBM to provide the Services. Sonoma County will ensure that its staff has the appropriate skills and experience. If any Sonoma County staff fails to perform as required, Sonoma County will make suitable additional or alternative staff available.

d) provide all information and materials reasonably required to enable IBM to provide the Services. IBM will not be responsible for any loss, damage, delay, or deficiencies in the Services arising from inaccurate, incomplete, or otherwise deficient information or materials supplied by or on behalf of Sonoma County.

e) consent and will obtain any necessary consents for IBM and its subcontractors to process the business contact information of Sonoma County, its employees and contractors worldwide for our business relationship. IBM will comply with requests to access, update, or delete such contact information.

f) obtain all necessary permissions for IBM to use, provide, store and process data to which Sonoma County gives IBM access to perform the Services. Sonoma County will not give IBM access to data subject to governmental regulation or requiring security measures beyond those specified in this SOW unless IBM has first agreed in writing to implement additional required security measures.

g) if making available to IBM any facilities, software, hardware or other resources in connection with IBM's performance of Services, obtain at no cost to IBM, obtain any licenses or approvals related to these resources that may be necessary for IBM to perform the Services. IBM will be relieved of its obligations that are adversely affected by Sonoma County's failure to promptly obtain such licenses or approvals. Sonoma County agrees to reimburse IBM for any reasonable expenses that IBM may incur from Sonoma County's failure to obtain these licenses or approvals.

h) be responsible for determining that any non-IBM products and their integration are following national building and installation codes and other laws and regulations, including product safety regulations.

i) perform Sonoma County roles and responsibilities as indicated in the Information Security Table of Roles and Responsibilities Appendix C.

j) provide 4 Red Hat Enterprise License Operation Systems - 8 vCPU VM and 4 Red Hat Enterprise License Operation Systems - 16 vCPU VM

k) Establish an IPSec VPN tunnel between Azure subscription and on-premises ISD LAN

l) Open network ports and firewall rules in the ISD LAN, for communication between following on-premises servers and Azure VM (over the VPN tunnel):

   - BizTalk server: to push client data flat files to the AppConnect instance in Azure.
   - DataStage server: to gather report data in the Cognos instance in Azure.
   - Active Directory server: to provide LDAPS based authentication security to Connect360 applications hosted in Azure.

m) Add IBM user accounts to the County Active Directory server to facilitate testing of authentication procedures.

n) Update the DNS entry in the on-premises DNS servers to point Connect360 endpoints to the new IP address(es) in Azure.

o) Assist with the installation and setup of the wildcard-domain based SSL certificate across Connect360 applications in Azure.

p) Add few IBM user accounts to the County Active Directory server to facilitate testing of authentication procedures.

q) Perform final database backups during the cutover period to facilitate migrating Connect360 data out from on-premises DB2 instance to Azure DB2 VM.

r) Assist with the final shutdown of on-premises VMs upon successful completion of migration activities.

s) Assist with the final dismantling of current VPN tunnel to IBM Cloud based WCM application once the migrated environment is verified to be up and running.

t) Provide communication of Migration to Cloud completion to Access Sonoma users

7. Applicable Standards

IBM will maintain a Cloud Solution Provider status with Microsoft™.

8. Access Sonoma Cloud Platform

IBM shall be using the Microsoft Azure Cloud within US Government region as the target environment, to host the ACCESS Sonoma infrastructure. MS Azure US Government cloud ensures that any resources deployed in this specific region shall always stay within the United States. The same constraint will also apply to data contained within the Azure resources.

Microsoft Azure Government provides industry standard security, protection, and compliance services as part of its Government offering. Azure Government services handle data that is subject to certain government regulations and requirements.

Additional information on the overall proposed solution can be found in the Cloud Migration Plan

8.1. Compliance

The environments will leverage Azure Government Community Cloud (GCC) High which provides FedRAMP High, ITAR, DFARS, DOD SRG L4 Controls, IRS 1075, and CJIS data handling compliance assurances. MS Azure IaaS, PaaS and SaaS offerings on the Government Community Cloud have been FedRAMP Authorized Since 04/29/2020. All Azure services are available immediately for supporting secure US government workloads, including CJIS, IRS 1075 FTI, HIPAA, DoD, and federal agency data.Security Architecture

8.1.1. Systems and Communication Protection

The proposed environment is comprised of Virtual Machines (VMs) and the OpenShift container platform, organized in 3 separate tiers of network zones. The TEST and PROD environments will be hosted in separate Azure Vnets, with separate subnets carved out for application and database tiers. In addition to the application and database tier, a front DMZ will be implemented using the Azure Load Balancer service, to protect entire Azure Vnet (for PROD and TEST) from the external access. Ports shall be accessible only for identified, necessary services within these subnets, with the help of Network Security Groups (NSGs). Containerized applications within the OpenShift clusters will have complete network isolation and access will be managed with the help of OpenShift Routes. Such a setup will ensure that access to VMs and containerized applications is thoroughly secured and managed in a central location.

Encryption controls applicable shall be as below -

- Data in motion: Communications between user and system will be encrypted and occur in the SSL layer. Inter-server communications within the Azure Vnets and with on-premises ISD DMZ zones will also be encrypted.
  - Data at rest wiill encrypted with Server-side encryption (SSE) on Azure managed disks (OS as well as data disks). Backups shall be encrypted and managed by the IBM FIMS team.

8.1.2. Disaster Recovery (DR)

Backups and DR will be managed by IBM. The Connect360 system will be deployed in Azure USGOV VA and will be backed up in Azure USGOV TX using Azure Site Recovery. In case of a failure in VA, the system will be restored in TX within 24 hours with a data loss of no more than 24 hours. (RTO/RPO = 24/24)

9. Estimated Schedule

The ability to provision software/Infrastructure described in this SOW will be available for Sonoma County to begin usage within 8 weeks from the agreed estimated start date (as stated within the signature acceptance section under agreed upon start date), and based on the time that Sonoma County has responded to the Microsoft™ electronic registration process of the Sonoma County - Tenancy:

- MSFT-Azure Tenancy Duration: 37.5 months

The Services will be performed consistent with the estimated to complete 4-6 weeks after the start. Both parties agree to make reasonable efforts to carry out their respective responsibilities in order to achieve the following schedule.

If the Work Order signature date is beyond the Estimated Start Date, the Estimated Start Date will automatically be extended to the date of the last signature on this Work Order. The Estimated End Date will automatically be extended by the same number of days.

10. Completion Criteria

IBM will have fulfilled its obligations under this SOW when any one of the following first occurs:

A. The specified work to provision the MSFT-Azure cloud have been completed and the MSFT-Azure Tenancy Duration has been fulfilled;

B. the MSFT-Azure Services are terminated in accordance with the provisions of this SOW and the Agreement.

11. Additional Terms and Conditions

11.1. Termination

Either party may terminate this Statement of Work by giving the other party not less than 30 days written notice provided that Sonoma County has no right to terminate this SOW at any time when the IBM Managed Services SOW is active. Upon termination, Sonoma County will pay the following amounts to IBM the charges for Services IBM provides and Products IBM delivers through termination, and all costs and expenses IBM incurs in terminating the Services. The Services charge will also be subject to any adjustment charges specified in Charges.

11.2. Sonoma County Directed Suppliers

If Sonoma County explicitly requests that IBM use a specific subcontractor or supplier of products or services for any portion of the Services described in this SOW, IBM will use such subcontractor or supplier contingent upon successful negotiations and execution of an acceptable procurement agreement, including pricing, with such subcontractor or supplier. Additionally, the use of such subcontractor or supplier will be subject to the Project Change Control Procedure, if such use could impact the project scope, schedule, cost, resources, or other terms of this SOW. IBM will have no obligation to perform an independent assessment, nor makes any representation as to the qualifications or charging practices of such subcontractor or supplier

11.3. IBM Intellectual Capital

IBM will be using preexisting IBM proprietary tools, (“IBM Tool(s)”) during the Services to perform the IBM responsibilities. These IBM Tools and associated documentation: 1) are not provided to Sonoma County under the terms of this SOW, 2) are not needed for Sonoma County to receive the benefit of the Services described in this SOW, and 3) remain the property of IBM.

11.4. Information Security and Data Protection

Sonoma County and IBM each agree to perform their information security responsibilities as listed in the Appendix C entitled “Information Security Roles and Responsibilities Table”.

Sonoma County agrees that no Sonoma County personal data that is subject to European General Data Protection Regulations (GDPR) requirements will be provided to IBM under this transaction.

A. In the event of a change, Sonoma County will notify IBM in writing and IBM’s Data Processing Addendum (DPA) at http://ibm.com/dpa will apply and supplements the Agreement. Additionally, IBM and Sonoma County will agree on a DPA Exhibit (as described in the DPA). The DPA Exhibit and, if applicable, a custom services DPA amendment will be added as an Appendix D to this transaction.

11.5. IBM Professional Errors & Omissions insurance coverage

Professional Errors & Omissions insurance coverage for actual or alleged breach of duty, neglect, error, misstatement, misleading statements or omission, solely for acts or omissions committed by IBM in providing professional services for Sonoma with a minimum per claim and aggregate limit of USD 5,000,000. Coverage includes network security, unauthorized access, unauthorized use, receipt or transmission of a malicious code, denial of service attack, unauthorized disclosure or misappropriation of private information, privacy liability, notification costs, credit card monitoring, and fine & penalties incurred by the customer.

11.6. COVID-19 Changes

The parties acknowledge and agree that COVID-19 is an event beyond the parties' reasonable control and it is not possible to foresee (or advisable to try and foresee) its duration, impact or extent (including measures and recommendations that may be put in place by regulators). As such, where a party's non-monetary obligations are not performed, affected, and/or delayed and that is attributable to COVID-19 or its related impacts, notwithstanding any other provision in the agreement, the affected party will not be responsible for such non-performance, affected performance or delay. The parties will act reasonably to discuss the affected obligations, potential workarounds and related issues in good faith and will document any agreed changes to the agreement.

12. Pricing

Pricing for this SOW is comprised of the following components

1. Subscription pricing for production and QA/UAT Cloud managed services and equipment, and
2. Labor Services to migrate ACCESS to the cloud.

The total estimated charges for this SOW are **$790,522.76**

Table 3, Pricing Table

Component	Reference Section	Term	Pricing
3 Yr Fixed Price Cloud Managed Services and Equipment subscription	Section 4.1 The Azure Cloud Services and 4.3 Cloud Managed Services	May 17th 2021 to June 30th 2024	**$691,082.76**
Total T&M Labor Services for Migration to cloud	12.2. Labor Services	May 17, 2021 to June 30th 2021	**$99,440**
	Total Services and Products		**$790,522.76**

12.1. Azure IAAS Subscriptions and Managed Services

The Azure Consumption Subscriptions are being provided on a consumption basis with estimated fees for MSFT-Azure Infrastructure As A Service (IAAS) components. These IAAS components include Virtual Machines, Reserved Instances reservations, and Pay-as-You-Go (PAYGO) consumption for MSFT-Azure resources including non-virtual machines products, or, other platform services as consumed. Sonoma County will be charged for Azure resources when those resources are provisioned and are being consumed per the Appendix A: Microsoft Customer Agreement.

The total Charges for an estimated 3-year period are $691,082.76 , after qualified rebates and are exclusive of any travel and living expenses, other reasonable expenses incurred in connection with the Services, and any applicable taxes. Any estimate given by IBM of any charge whether for planning or any other purpose is only an estimate. As these are estimated amounts, actual fees may differ.

Should Sonoma County be required under any law or regulation of any governmental entity or authority, domestic or foreign, to withhold or deduct any portion of the payments due to IBM, then the sum payable to IBM shall be increased by the amount necessary to yield to IBM an amount equal to the sum it would have received had no withholdings or deductions been made.

Any early termination of a three year reserve as described in the BOM (Section 5.1) will result early termination penalty from Sonoma County. This penalty will Sonoma County's responsibility

12.1.1.Payment Schedule

IBM will invoice the county Annually over 37 months at the end of each term with the expected start date being within 5 days of the actual signing, as outlined in the table below:

Table 4, Yearly Payment Schedule

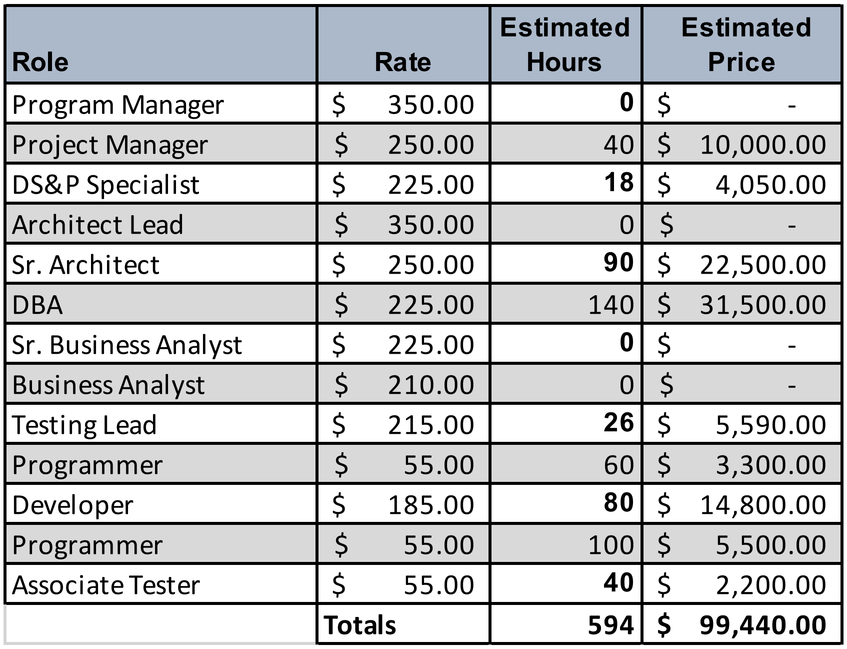
Term	Year	Length	Description	Amount
1	FY 20-21	**1 Month**	Year 1 Fixed Price Cloud Managed Services and Equipment Subscription	**$25,382.76**
2	FY 21-22	**12 Months**	Year 2 Fixed Price Cloud Managed Services and Equipment Subscription	**$221,900.00**

3	FY 22-23	**12 Months**	Year 3 Fixed Price Cloud Managed Services and Equipment Subscription	**$221,900.00**
4	FY 23-24	**12 Months**	Year 4 Fixed Price Cloud Managed Services and Equipment Subscription	**$221,900.00**
			Total	**$691,082.76**

12.2. Labor Services

Labor services will be performed and invoiced on a time and materials basis, inclusive of all costs unless otherwise agreed in writing, at the end of each month for hours worked that month and documented in the monthly status report. The monthly status report will also contain a cumulative total of hours consumed against the total hours estimated in the table below. Contractor is only authorized to work up to the estimated total price regardless of Scope, Completion Criteria, or Exit Criteria; the change control process will be utilized should additional funding be required. Hours will be invoiced using Labor Rates based upon the Estimated Hours in the following table

Hours will be invoiced monthly using Labor Rates based upon the Estimated Hours in the following table:



Role	Rate	Estimated Hours	Estimated Price
Program Manager	$ 350.00	**0**	$ -
Project Manager	$ 250.00	40	$ 10,000.00
DS&P Specialist	$ 225.00	**18**	$ 4,050.00
Architect Lead	$ 350.00	0	$ -
Sr. Architect	$ 250.00	**90**	$ 22,500.00
DBA	$ 225.00	140	$ 31,500.00
Sr. Business Analyst	$ 225.00	**0**	$ -
Business Analyst	$ 210.00	0	$ -
Testing Lead	$ 215.00	**26**	$ 5,590.00
Programmer	$ 55.00	60	$ 3,300.00
Developer	$ 185.00	**80**	$ 14,800.00
Programmer	$ 55.00	100	$ 5,500.00
Associate Tester	$ 55.00	**40**	$ 2,200.00
	Totals	**594**	**$ 99,440.00**

Figure 2: T&M Labor Rate Table

The total estimated T&M Services for PCR activities is $99,440 and is inclusive of normal travel and living expenses for IBM personnel.

12.3. SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties hereto have caused this SOW to be duly executed by their respective authorized representatives, as of the Effective Date.

By: ______________________________	By: ___________________________________
Name: ______________________________	Name:___________________________________
Title: _______________________________	Title: ___________________________________
Date: _______________________________	Date:___________________________________

Appendix A – Microsoft Customer Agreement

2020 Microsoft
Customer Agreement.

Appendix C - Information Security Roles and Responsibilities Table

Personal Information (“PI”) is any information that identifies or can reasonably be used to identify, contact, or locate the individual to whom such information pertains. Personal Information includes information that relates to individuals in their personal capacity (e.g., an individual's home address) as well as information that relates to individuals in their professional or business capacity (e.g., an individual's business address.)

Sensitive Personal Information (“SPI”) refers to information that is considered "sensitive" due to the risks that such information could be misused to significantly harm an individual in a financial, employment or social way. Examples of SPI include: an individual’s name in conjunction with that individual’s social security number, driver’s license number, state identification number, medical information, date of birth, electronic signature, or mother’s maiden name.

Business Sensitive Information (“BSI”) refers to information that may warrant special handling such as supply chain vendor list or pricing data, strategic plans, network diagrams, etc. Any such protective measures will be documented in this SOW and are in addition to the Agreement for Exchange of Confidential Information (“AECI”) or other applicable written non-disclosure or confidentiality provisions.

The following IBM and Client responsibilities shown below in the Information Security Roles and Responsibilities table, which will be discussed and updated.

Control Area	INFORMATION SECURITY ROLES AND RESPONSIBILITIES	IBM	Client
1	**Security Policy**		
a	Determine appropriate information security policy requirements based on business objectives, assessment of risk, and interpretation of legal, regulatory and contractual obligations ● Validate that the workstation and application security controls meet Client requirements driven by security policy and risk acceptance ● Identify security requirements for new applications ● Request exceptions to the base Roles and Responsibilities as defined in this table, as needed		R
b	Notify IBM if Client information security requirements change through Project Change Control Procedure, as defined by the Statement of Work so that parties may assess if and how to implement, including impact to cost, scope or schedule		R
c	Review the Roles and Responsibilities as defined by this table periodically but at least every ***18*** months		R
d	Review the Roles and Responsibilities as defined by this table with Client, periodically but at least every ***18*** months for projects longer than 18 mos.	R	
e	Provide Client with this table which communicates Client and IBM responsibilities for Client’s application development and maintenance services and the handling of Client’s data.	R	
f	Respond to exception or Project Change Requests from Client and determine if such requests result in additional or modified services or changes to information security Roles and Responsibilities, all of which will be managed through the Project Change Control Procedure as defined by the Statement of Work	R	
2	**Organization of Information Security**		
a	Designate a knowledgeable Client focal point for information security related activities		R
b	Provide contact information for the primary contact and for an authorized secondary contact		R
c	Coordinate all information security activities with third parties other than those contracted by IBM		R
d	Designate a knowledgeable IBM focal point for information security related activities including: ● Interfacing with the Client focal point on security requirements ● Implementation of security requirements for which IBM is responsible in accordance with the negotiated and agreed to Roles and Responsibilities (as defined by this table)	R	
e	Provide contact information for the primary contact and for an authorized secondary contact	R	
f	Coordinate security activities with third parties contracted by IBM (as defined by this table)	R	
3	**Asset Management**		

a	Be responsible for its information assets, including software, physical assets, and services		R
b	Communicate to IBM any Client European Economic Area (EEA) origin personal data and provide IBM with data processing and data security instructions for such data		R
c	Identify and communicate to IBM any Client data designated as confidential, business sensitive information (BSI), personal information (PI), and sensitive personal information (SPI) that IBM will have access to. Provide data for testing that does not contain PI/SPI/BSI		R
d	Be responsible for identifying, providing and funding the appropriate information security controls and communicating relevant requirements to IBM for: ● Data transmitted via public telecommunications facilities or services. ● Transport of confidential information, personal information, sensitive personal information and business sensitive information (e.g., encryption, transport over secure lines); and ● Storing of confidential information, personal information, sensitive personal information and business sensitive information (e.g., encryption of data on portable media or other special handling or treatment) ● Printing of Client information ● Data discard or destruction requirements		R
e	Follow approved Project Change Control Procedure (defined in the GBS Statement of Work) for security related changes	R	
f	Handle information identified by the Client as confidential, business sensitive, personal and sensitive personal in accordance with the following controls: ● On applications, protect Client data by access controls as specified under IBM Responsibilities, in Area 6, 'Access Control' ● Store portable storage media containing Client data as defined in this table or some other specifically named document. ● When information is printed at IBM locations, keep printed information identified by Client as confidential, business sensitive, personal and sensitive personal in a locked container or physically controlled area	R	
4	**Human Resources Security**		
a	Address information security in the hiring, termination and personnel management processes for Client personnel		R
b	Provide security awareness training to Client personnel and other network or system users authorized by Client		R
c	Identify and provide to IBM any Client-specific personnel requirements such as background checks or others applicable by law		R
d	Identify and provide to IBM any Client-specific security training required for IBM personnel		R
e	Take appropriate management action if there is a misuse of authority by any Client personnel		R
f	Address Client security requirements in joining and leaving the project, and in personnel management processes for IBM personnel	R	
g	Provide the current IBM security education package to IBM personnel joining the project	R	
h	Address agreed-to personnel requirements as described in this SOW	R	
i	Take appropriate management action if there is a misuse of an IBM employee's granted authorizations.	R	
5	**Physical and Environmental Security**		
a	Secure work areas and restrict access from general public at Client sites where IBM personnel will work		R
b	Identify and provide to IBM any Client-specific information security requirements for printing, storing and transmitting Client information		R
c	Define where IBM personnel will work: ● IBM locations or Client sites ● Define remote or work at home options		R
d	Supply and manage secure workstation image(s) including anti-virus software, firewall protection, and whole-disk encryption for workstations provided by Client to IBM personnel		R
e	Respond to virus attacks and initiate corrective action on workstations provided by Client to IBM personnel		R
f	Define requirements for return of assets and removal of access rights to Client physical assets upon IBM personnel termination or change of employment		R
g	Provide and manage physical security of IBM owned workstations	R	
h	Perform workplace security inspections of IBM personnel at IBM sites and Client sites (related to execution of this SOW) where IBM personnel will work from	R	
i	Provide security for work areas and restrict access from general public at IBM sites	R	

j	Supply and install IBM anti-virus software and upgrades for IBM supplied workstations	R	
k	Respond to virus attacks and initiate corrective action on IBM supplied workstations	R	
l	Install whole-disk encryption on IBM-supplied workstations	R	
6	**Access Control**		
a	Authorize, administer and manage user IDs and passwords for Client managed applications, systems and subsystems		R
b	Provide unique login IDs and passwords to IBM personnel for Client managed applications, systems and subsystems		R
c	Define access control requirements and process and administer logical access for network infrastructure systems and devices under Client management		R
d	Define access control requirements for Client applications, databases and other Client software on systems across all environments (development, test, production)		R
e	Define what constitutes privileged access and access control requirements for users with privileged access to Client applications, databases and other Client software on systems across all environments (development, test, production)		R
f	Administer revocation of access for Client managed applications, systems and subsystems as appropriate, based on validation activities and when requested by IBM		R
g	Define revocation requirements for Client applications, databases and other Client software on systems across all environments (development, test, production)		R
h	Be responsible for revalidating the employment status and business need for access to Client applications and systems for Client personnel		R
i	Be responsible for revalidating the business need for IBM personnel access to Client managed applications, systems and subsystems, periodically but at least every ***12*** months		R
j	Be responsible for implementing access changes to Client managed applications, systems and subsystems based on input from IBM employment validation activities for IBM personnel		R
k	Revalidate the list of privileges associated with User ID's assigned to IBM personnel with access to Client managed applications, systems and subsystems, periodically but at least every ***12*** months,		R
l	Revalidate shared ID's assigned to IBM with access to Client applications, databases and other Client software on systems across all environments (development, test, production), periodically but at least every ***12*** months		R
m	Validate User ID baseline inventory and share results of updates made to User IDs used by IBM staff ● Retain evidence of completion for two revalidation cycles		R
n	Define data protection technique requirements to be used to access Client applications, databases and other Client software on systems across all environments (development, test, production), such as data masking and encryption, and supply tools to meet requirements		R
o	Define requirements for secure disposal of Client information from workstations or storage media		R
p	Define criteria for IBM personnel termination of access rights to Client's logical assets upon conclusion of assignment or change of employment		R
q	Log and monitor activities of IBM privileged users with access to Client managed applications and systems; provide the monitoring results to IBM		R
r	Provide initial (one time) acknowledgement for shared ID's that will be used by IBM personnel		R
s	Submit request to revoke access to Client systems, applications, databases and other Client software when IBM personnel no longer require access	R	
t	Respond to revalidation of employment status, business need and access privileges to Client systems, applications, databases, other Client software assigned to IBM personnel ● Retain evidence of completion for two revalidation cycles ● Submit or notify Client of access changes needed as a result of revalidation activities	R	
u	Respond to revalidation of shared ID's to Client systems, applications, databases, other Client software assigned to IBM personnel Retain evidence of completion for two revalidation cycles Submit or notify of access changes needed as a result of revalidation activities	R	
v	Where IBM has the ability to establish password configuration settings on Client applications, verify that passwords for IBM personnel working on Client applications conform to the IBM standards unless Client requirements are more stringent, at the discretion of IBM	R	
w	Perform a baseline inventory of User ID's to Client systems, applications, databases, other Client software assigned to IBM personnel and communicate User ID baseline inventory to Client for validation	R	
x	Adhere to Client data protection technique requirements using tools provided by Client	R	
y	Provide follow-up for issues identified via monitoring of IBM privileged User IDs when alerted by Client	R	

z	Dispose Client data in all forms within IBM's control based on Client's classification and direction. If Client has not provided any data disposal direction, then data will be disposed of in a manner consistent with IBM internal practices for IBM confidential information	R	
7	**Information Security Incident Management**		
a	Provide a 24/7 contact plan for reporting security incidents		R
	● Inform IBM of any application and information security incidents involving IBM personnel ● Provide a Client security incident coordinator ● Make decisions on actions to resolve security incidents involving Client network, systems, personnel or data, including, if appropriate, collection of evidence ● Interface, as needed, with external entities such as law enforcement, legal or regulatory agencies		
b	Assist Client in initial security incident evaluation for security incidents involving IBM personnel that are reported by Client as part of security incident management	R	
8	**Compliance**		
a	Identify and interpret legal, regulatory or contractual security requirements that are applicable to its business and inform IBM of any additional or changed requirements (for example data export or transfer restrictions and privacy laws)		R
b	Review periodic security reporting provided by IBM		R
c	Provide support for application assessments including Client audit activities, issue management services and closure of issues after audit (closure of issues impacting cost, schedule, quality may require that the Project Change Control Procedure be followed)	R	
d	Provide periodic, basic security reporting as defined by IBM	R	
9	**Separation of Duties**		
a	Perform application separation of duties analysis and conflict resolution		R
b	Implement change management on separation of duties analysis		R
c	Perform annual review of separation of duties analysis		R
d	Authorize code promotions, data changes and database changes to production		R
e	Inform Client of any role, responsibility, or access changes of IBM personnel	R	

Appendix D – Data Processing Addendum

Data Processing Addendum

This Data Processing Addendum (DPA) and its applicable DPA Exhibits apply to the Processing of Personal Data by IBM on behalf of Client (Client Personal Data) subject to the General Data Protection Regulation 2016/679 (GDPR) or any other data protection laws identified at www.ibm.com/dpa/dpl (together 'Data Protection Laws') in order to provide services (Services) pursuant to the Agreement between Client and IBM. DPA Exhibits for each Service will be provided in the applicable Transaction Document (TD). This DPA is incorporated into the Agreement. Capitalized terms used and not defined herein have the meanings given them in the applicable Data Protection Laws. In the event of conflict, the DPA Exhibit prevails over the DPA which prevails over the rest of the Agreement

1. Processing

1.1 Client is (a) a Controller of Client Personal Data or (b) acting as Processor on behalf of other Controllers and has been instructed by and obtained the authorization of the relevant Controller(s) to agree to the Processing of Client Personal Data by IBM as Client's subprocessor as set out in this DPA. Client appoints IBM as Processor to Process Client Personal Data. If there are other Controllers, Client will identify and inform IBM of any such other Controllers prior to providing their Personal Data, in accordance with the DPA Exhibit.

1.2 A list of categories of Data Subjects, types of Client Personal Data, Special Categories of Personal Data and the processing activities is set out in the applicable DPA Exhibit for a Service. The duration of the Processing corresponds to the duration of the Service, unless otherwise stated in the DPA Exhibit. The purpose and subject matter of the Processing is the provision of the Service as described in the Agreement.

1.3 IBM will Process Client Personal Data according to Client's documented instructions. The scope of Client's instructions for the Processing of Client Personal Data is defined by the Agreement, and, if applicable, Client's and its authorized users' use and configuration of the features of the Service. Client may provide further legally required instructions regarding the Processing of Client Personal Data (Additional Instructions) as described in Section 10.2. If IBM notifies Client that an Additional Instruction is not feasible, the parties shall work together to find an alternative. If IBM notifies the Client that neither the Additional Instruction nor an alternative is feasible, Client may terminate the affected Service, in accordance with any applicable terms of the Agreement. If IBM believes an instruction violates the Data Protection Laws, IBM will immediately inform Client, and may suspend the performance of such instruction until Client has modified or confirmed its lawfulness in documented form.

1.4 Client shall serve as a single point of contact for IBM. As other Controllers may have certain direct rights against IBM, Client undertakes to exercise all such rights on their behalf and to obtain all necessary permissions from the other Controllers. IBM shall be discharged of its obligation to inform or notify another Controller when IBM has provided such information or notice to Client. Similarly, IBM will serve as a single point of contact for Client with respect to its obligations as a Processor under this DPA.

1.5 IBM will comply with all Data Protection Laws in respect of the Services applicable to IBM as Processor. IBM is not responsible for determining the requirements of laws or regulations applicable to Client's business, or that a Service meets the requirements of any such applicable laws or regulations. As between the parties, Client is responsible for the lawfulness of the Processing of the Client Personal Data. Client will not use the Services in a manner that would violate applicable Data Protection Laws.

2. Technical and organizational measures

2.1 Client and IBM agree that IBM will implement and maintain the technical and organizational measures set forth in the applicable DPA Exhibit (TOMs) which ensure a level of security appropriate to the risk for IBM's scope of responsibility. TOMs are subject to technical progress and further development. Accordingly, IBM reserves the right to modify the TOMs provided that the functionality and security of the Services are not degraded.

3. Data Subject Rights and Requests

3.1 IBM will inform Client of requests from Data Subjects exercising their Data Subject rights (e.g., including but not limited to rectification, deletion and blocking of data) addressed directly to IBM regarding Client Personal Data. Client shall be responsible to handle such requests of Data Subjects. IBM will reasonably assist Client in handling such Data Subject requests in accordance with Section 10.2.

3.2 If a Data Subject brings a claim directly against IBM for a violation of their Data Subject rights, Client will reimburse IBM for any cost, charge, damages, expenses or loss arising from such a claim, to the extent that IBM has notified Client about the claim and given Client the opportunity to cooperate with IBM in the defense and settlement of the claim. Subject to the terms of the Agreement, Client may claim from IBM damages resulting from Data Subject claims for a violation of their Data Subject rights caused by IBM's breach of its obligations under this DPA and the respective DPA Exhibit.

4. Third Party Requests and Confidentiality

4.1 IBM will not disclose Client Personal Data to any third party, unless authorized by the Client or required by law. If a government or Supervisory Authority demands access to Client Personal Data, IBM will notify Client prior to disclosure, unless such notification is prohibited by law.

4.2 IBM requires all of its personnel authorized to Process Client Personal Data to commit themselves to confidentiality and not Process such Client Personal Data for any other purposes, except on instructions from Client or unless required by applicable law.

5. Audit

5.1 IBM shall allow for, and contribute to, audits, including inspections, conducted by the Client or another auditor mandated by the Client in accordance with the following procedures:

1. Upon Client's written request, IBM will provide Client or its mandated auditor with the most recent certifications and/or summary audit report(s), which IBM has procured to regularly test, assess and evaluate the effectiveness of the TOMs, to the extent set out in the DPA Exhibit.
2. IBM will reasonably cooperate with Client by providing available additional information concerning the TOMs, to help Client better understand such TOMs.
3. If further information is needed by Client to comply with its own or other Controllers audit obligations or a competent Supervisory Authority's request, Client will inform IBM in writing to enable IBM to provide such information or to grant access to it.
4. To the extent it is not possible to otherwise satisfy an audit right mandated by applicable law or expressly agreed by the Parties, only legally mandated entities (such as a governmental regulatory agency having oversight of Client's operations), the Client or its mandated auditor may conduct an onsite visit of the IBM facilities used to provide the Service, during normal business hours and only in a manner that causes minimal disruption to IBM's business, subject to coordinating the timing of such visit and in accordance with any audit procedures described in the DPA Exhibit in order to reduce any risk to IBM's other customers.

Any other auditor mandated by the Client shall not be a direct competitor of IBM with regard to the Services and shall be bound to an obligation of confidentiality.

5.2 Each party will bear its own costs in respect of paragraphs a. and b. of Section 5.1, otherwise Section 10.2 applies accordingly.

6. Return or Deletion of Client Personal Data

6.1 Upon termination or expiration of the Agreement IBM will either delete or return Client Personal Data in its possession as set out in the respective DPA Exhibit, unless otherwise required by applicable law.

7. Subprocessors

7.1 Client authorizes the engagement of other Processors to Process Client Personal Data (Subprocessors). A list of the current Subprocessors is set out in the respective DPA Exhibit. IBM will notify Client in advance of any addition or replacement of the

Subprocessors as set out in the respective DPA Exhibit. Within 30 days after IBM's notification of the intended change, Client can object to the addition of a Subprocessor on the basis that such addition would cause Client to violate applicable legal requirements. Client's objection shall be in writing and include Client's specific reasons for its objection and options to mitigate, if any. If Client does not object within such period, the respective Subprocessor may be commissioned to Process Client Personal Data. IBM shall impose substantially similar but no less protective data protection obligations as set out in this DPA on any approved Subprocessor prior to the Subprocessor initiating any Processing of Client Personal Data.

7.2 If Client legitimately objects to the addition of a Subprocessor and IBM cannot reasonably accommodate Client's objection, IBM will notify Client. Client may terminate the affected Services as set out in the Agreement, otherwise the parties shall cooperate to find a feasible solution in accordance with the dispute resolution process.

8. Transborder Data Processing

8.1 In the case of a transfer of Client Personal Data to a country not providing an adequate level of protection pursuant to the Data Protection Laws (Non-Adequate Country), the parties shall cooperate to ensure compliance with the applicable Data Protection Laws as set out in the following Sections. If Client believes the measures set out below are not sufficient to satisfy the legal requirements, Client shall notify IBM and the parties shall work together to find an alternative.

8.2 By entering into the Agreement, Client is entering into EU Standard Contractual Clauses as set out in the applicable DPA Exhibit (EU SCC) with (i) each Subprocessor listed in the respective DPA Exhibit that is an IBM affiliate located in a Non-Adequate Country (IBM Data Importers) and (ii) IBM, if located in a Non-Adequate Country, as follows:

1. if Client is a Controller of all or part of the Client Personal Data, Client is entering into the EU SCC in respect to such Client Personal Data, and
2. if Client is acting as Processor on behalf of other Controllers of all or part of the Client Personal Data, then Client is entering into the EU SCC:

(i) as back-to-back EU SCC in accordance with Clause 11 of the EU Standard Contractual Clauses (Back-to- Back SCC), provided that Client has entered into separate EU Standard Contractual Clauses with the Controllers, or

(ii) on behalf of the other Controller(s).

Client agrees in advance that any new IBM Data Importer engaged by IBM in accordance with Section 7 shall become an additional data importer under the EU SCC and/or Back-to-Back SCC.

8.3 If a Subprocessor located in a Non-Adequate Country is not an IBM Data Importer (Third Party Data Importer) and EU SCC are entered into in accordance with Section 8.2, then, IBM or an IBM Data Importer shall enter into Back-to-Back SCC with such a Third Party Data Importer. Otherwise, Client on its own behalf and/or, if required, on behalf of other Controllers shall enter into separate EU Standard Contractual Clauses or Back-to-Back SCC as provided by IBM.

8.4 If Client is unable to agree to the EU SCC or Back-to-Back SCC on behalf of another Controller, as set out in section 8.2 and 8.3, Client will procure the agreement of such other Controller to enter into those agreements directly. Additionally, Client agrees and, if applicable, procures the agreement of other Controllers that the EU SCC or the Back-to-Back SCC, including any claims arising from them, are subject to the terms set forth in the Agreement, including the exclusions and limitations of liability. In case of conflict, the EU SCC and Back-to-Back SCC shall prevail.

9. Personal Data Breach

9.1 IBM will notify Client without undue delay after becoming aware of a Personal Data Breach with respect to the Services. IBM will promptly investigate the Personal Data Breach if it occurred on IBM infrastructure or in another area IBM is responsible for and will assist Client as set out in Section 10.

10. Assistance

10.1 IBM will assist Client by technical and organizational measures for the fulfillment of Client's obligation to comply with the rights of Data Subjects and in ensuring compliance with Clients obligations relating to the security of Processing, the notification and communication of a Personal Data Breach and the Data Protection Impact Assessment, including prior consultation with the responsible Supervisory Authority, if required, taking into account the nature of the processing and the information available to IBM.

10.2 Client will make a written request for any assistance referred to in this DPA. IBM may charge Client no more than a reasonable charge to perform such assistance or an Additional Instruction, such charges to be set forth in a quote and agreed in writing by the parties, or as set forth in an applicable change control provision of the Agreement. If Client does not agree to the quote, the parties agree to reasonably cooperate to find a feasible solution in accordance with the dispute resolution process.