



STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 2

CONTRACT #: AR2485

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and Insight Pubic Sector, Inc. (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

The following is hereby amended into Attachment E:

-- Insight Public Sector Purchasing Entity Program Agreement, attached herein; and
-- those additional Service Provider Terms and Conditions, End User License Agreements, etc. provided on the Insight designated webpage of the NASPO ValuePoint website here-
<https://www.naspovaluepoint.org/portfolios/portfolio-contractor/insight-cloud-solutions/>, under document Insight – Attachment E Additional Service Provider Terms and Conditions, as may be updated from time to time.

Effective Date of Amendment: 9/28/2018

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

STATE OF UTAH

10/1/2018
Date

Christopher Hughes
Christopher Hughes (Oct 2, 2018)

Oct 2, 2018
Date

Contractor's Signature

Director, State of Utah Division of Purchasing

Date

Lisanne Steinheiser

Contractor's Name (Print)

Assistant Secretary

Title (Print)

For Division of Purchasing Internal Use

Purchasing Agent	Phone #	E-mail Address	Contract #
Solomon Kingston	801-538-3228	skingston@utah.gov	AR2485

[Purchasing Entity] Program Agreement

This [Purchasing Entity] ("Purchasing Entity") Program Agreement ("Agreement") is entered into between Purchasing Entity and Insight Public Sector. Under this Agreement, Insight Public Sector may order, on behalf of the Purchasing Entity, In-Scope Services, solely in connection with a Government Contract. These In-Scope Services are solely for the use by the Purchasing Entity, and not for use or access by Government Partner or any other third party.

Effective date. The effective date of this Agreement is the earliest effective date of any Enrollment entered into under this Agreement or the date Government Partner accepts this Agreement, whichever is earlier. Any reference in this Agreement or an Enrollment to a "day" means a calendar day, except references that specify "business day."

This Agreement consists of (1) these terms and conditions, including the Additional Use Rights and Restrictions and (2) any Enrollment entered into under this Agreement.

Please note: Documents referenced in this Agreement but not attached may be found at <http://www.microsoft.com/licensing/contracts> and are incorporated in this Agreement by reference, including the Product Terms and the Online Services Terms. These documents may contain additional terms and conditions for Products licensed under this Agreement and may be changed by Microsoft from time to time.

Additional Use Rights and Restrictions

These Additional Use Rights and Restrictions shall apply to each Enterprise's use of Products.

1. General.

Right to use. Purchasing Entity may access and use In-Scope Services, and install and use a Client (if any) included with its Subscription, only as described in this agreement. All other rights are reserved.

Acceptable use. Purchasing Entity will use In-Scope Services only per the AUP. Purchasing Entity will not use In-Scope Services in any way that infringes a third party's patent, copyright, or trademark or misappropriates its trade secret. Purchasing Entity may not reverse engineer, decompile, work around technical limits in, or disassemble In-Scope Services, except if applicable law permits despite this limit. Purchasing Entity may not rent, lease, lend, resell, transfer, or host In-Scope Services to or for third parties.

Compliance.

Purchasing Entity will comply with all laws and regulations applicable to its use of In-Scope Services.

In providing In-Scope Services, Contractor and Microsoft will comply with all laws and regulations (including applicable security breach notification law) that generally apply to IT service providers. Microsoft will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry or government function that are not generally applicable to information technology service providers. Microsoft does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Purchasing Entity will obtain any consents required: (1) to allow it to access, monitor, use, and disclose user data; and (2) for Contractor and Microsoft to provide the In-Scope Services. If Purchasing Entity is an educational institution, it will obtain any parental consent for end users' use of In-Scope Services as required by applicable law.

Customer Data. Customer Data is used only to provide Purchasing Entity In-Scope Services. This use may include troubleshooting to prevent, find and fix problems with those In-Scope Services' operation. It may also include improving features for finding and protecting against threats to users. Neither Contractor nor Microsoft will derive information from Customer Data for any advertising or other commercial purposes. As between the parties, the Purchasing Entity retains all right, title and interest in and to Customer Data. Neither Contractor nor Microsoft acquires rights in Customer Data, other than the rights Purchasing Entity grants to Microsoft through Contractor to provide the Online Services to Purchasing Entity. This paragraph does not affect Microsoft's rights in software or Online Services Contractor and Microsoft license to Purchasing Entity.

Contractor and Microsoft will enable Purchasing Entity to keep Customer Data in DPT Services separate from Microsoft's consumer services.

Customer Data will not be disclosed unless required by law or allowed by this Agreement. Purchasing Entity's contact information may be provided so that a requestor can contact it. If law requires disclosure, Contractor and Microsoft will use commercially reasonable efforts to notify Purchasing Entity, if permitted.

Customer Data may be transferred to, and stored and processed in, any country Contractor or Microsoft maintain facilities, except when a tenant for DPT Services is provisioned in the United States, in which case Customer Content shall be processed and stored at rest in the Continental United States.

Security Incident Notification for DPT Services. Solely for DPT Services, the following terms and conditions apply:

If Microsoft becomes aware of any Security Incident (as defined herein), Microsoft will promptly (1) notify Purchasing Entity of the Security Incident; (2) investigate the Security Incident and provide Purchasing Entity with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Purchasing Entity's administrators by any means Microsoft selects, including via email. It is Purchasing Entity's sole responsibility to ensure Purchasing Entity's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Purchasing Entity must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any Security Incident related to an Online Service.

5-day Security Incident notification for Government Community Cloud Services. As an exception to the foregoing, notification of Security Incident solely pertaining to Government Community Cloud Services will be delivered within 5 days after Microsoft determines that a Security Incident has occurred, provided that Purchasing Entity must comply with the following requirements:

For each Online Service Tenant or Azure subscription, as applicable, as a condition of receiving notifications within 5 days, as set forth in the preceding paragraph, Purchasing Entity must register the following information by sending email to ols-notifications@microsoft.com, and must keep such information current at all times:

- 1) Purchasing Entity's Microsoft Online Direct Routing Domain (MODRD);
- 2) For one or more individual(s) to be contacted, each of whom must be registered as an administrator on the applicable Online Services, each of the following:
 - a. Name;
 - b. Title;
 - c. Email address registered as an administrator on the Online Services;
 - d. Email address not registered as a user on the Online Services;
- 3) Name of Purchasing Entity;
- 4) Enrollment number (provided by Contractor and assigned by Microsoft) to represent Purchasing Entity's Tenant or Azure Subscription, on Contractor's subcontract with Microsoft.

Microsoft expects to change the above process by which the Purchasing Entity for each tenant or subscription will be able to register their MODRD and other information for five-day Security Incident notification pursuant to these terms and conditions. In the event that a Purchasing Entity is notified by Microsoft, in the administrative console or otherwise, of revised instructions necessary to ensure five-day Security Incident notification, the Purchasing Entity must comply with such revised instructions.

Reimbursement of Security Incident Remediation Costs. To the extent that a Security Incident for a DPT Service results from Microsoft's failure to comply with its obligations under the Master Agreement (and, where applicable, Participating Addenda), and subject to the Limitation of Liability section in this Agreement, Microsoft will reimburse Purchasing Entities for reasonable out-of-pocket remediation costs incurred by such Purchasing Entities in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" are costs that (a) are customary, reasonable and expected to be paid by entities similar to Purchasing Entity, based on the nature and scope of the Security Incident, and (b) do not arise from or relate to Purchasing Entity's violation of (i) laws applicable to Purchasing Entity or (ii) Purchasing Entity's obligations to third parties, and (c) in no event include costs arising related to compliance with laws

applicable to Purchasing Entity or its industry or government function that are not generally applicable to information technology services providers. Purchasing Entity must document all such expenditures and, upon Microsoft's request, those expenditures must be validated by an independent, internationally-recognized third party industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Microsoft under this paragraph will be characterized as direct damages subject to the limitation on liability set forth in this Section, and not as special damages excluded under the "EXCLUSION OF CERTAIN DAMAGES" in the Limitation of Liability section.

Changes. In-Scope Services may be changed periodically. As such, Purchasing Entity's use of them will be subject to a revised OST, then-current as of the date it renews its subscription. For In-Scope Services that include client software, Purchasing Entity may be required to run a client software upgrade on its devices after a change to maintain full functionality, in accordance with the terms and conditions of the OST.

Use rights. Use rights specific to each In-Scope Service are posted online at the link to the OST, which is hereby incorporated by reference into this agreement.

2. Confidentiality and Security.

For DPT Services, Contractor and Microsoft will (a) implement and maintain all appropriate administrative, physical, technical, procedural safeguards and organizational measures, internal controls, and data security routines intended to protect Customer Data against accidental loss or change, unauthorized disclosure or access, unlawful destruction, hacks, introduction of viruses, disabling devices, malware, and other forms of malicious or inadvertent acts that can disrupt Purchasing Entity's access to its Customer Data; and (b) not disclose Customer Data, except as required by law or expressly allowed. Neither party will make any public statement about this agreement's terms without the other's prior written consent.

3. Term, Termination, and Suspension.

Reserved.

4. Limited warranty; disclaimer.

Contractor warrants that In-Scope Services will meet the SLA terms during the Subscription; Purchasing Entity's only remedy for breach of warranty is stated in the SLA. *Contractor provides no (and disclaims to the extent permitted by law any) other warranties, express, implied, or statutory, including warranties of merchantability or fitness for a particular purpose.*

5. Indemnification.

Reserved.

6. Limitation of Liability.

Reserved.

7. Agreement mechanics

Purchasing Entity must send notice by regular mail, return receipt requested, to the address on the Portal (effective when delivered). Contractor or Microsoft may email notice to your account administrators (effective when sent). Purchasing Entity may not assign this agreement, or any right or duty under it. If part of this agreement is held unenforceable, the rest remains in force. Failure to enforce this agreement is not a waiver. The parties are independent contractors. This agreement does not create an agency, partnership, or joint venture. This agreement is governed by the laws applicable to Purchasing Entity, without regard to conflict of laws. This agreement (including the SLA and OST) and Contractor's price sheet are the parties' entire agreement on this subject and supersedes any concurrent or prior communications. Agreement terms that require performance, or apply to events that may occur, after termination or expiration will survive, including §5. In-Scope Service and any Client associated therewith are subject to U.S. export jurisdiction. Purchasing Entity must comply with the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end-use, and destination restrictions. For more information, see <http://www.microsoft.com/exporting/>. Microsoft delivers In-Scope Services, and the rights granted to us also apply to them.

8. Miscellaneous Microsoft Terms and Conditions

- A. **Accessibility.** Microsoft supports the government's obligation to provide accessible technologies to its citizens with disabilities as required by Section 508 of the Rehabilitation Act of 1973, and its state law counterparts (including applicable California provisions). Microsoft encourages its customers (including Purchasing Entities under the Master Agreement and Participating Addenda) to judiciously compare product accessibility performance. The Voluntary Product Accessibility Templates ("VPATs") for the Microsoft technologies used in providing the online services can be found at Microsoft's VPAT page. Further information regarding Microsoft's commitment to accessibility can be found at www.microsoft.com/enable.
- B. **DPT Services Information Security Policy.** For each DPT Service, Microsoft follows a written data security policy ("Information Security Policy") that complies with the control standards and frameworks shown in the table below.

DPT Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Office 365 Services	Yes	Yes	Yes	Yes*	Yes*
Microsoft Dynamics CRM Online Services	Yes	Yes	Yes	Yes	Yes
Microsoft Azure Core Services	Yes	Yes	Yes	Varies**	Varies**
Microsoft Intune Online Services	Yes	Yes	Yes	Yes	Yes

*Does not include Yammer Enterprise.

**Current scope is detailed in the audit report and summarized in the Microsoft Azure Trust Center.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate a standard or framework in the table above, unless it is no longer used in the industry and it is replaced with a successor (if any). Azure Government Services meet a separate set of control standards and frameworks, as detailed on the Microsoft Azure Trust Center.

Subject to non-disclosure obligations, Microsoft will make each Information Security Policy available to Purchasing Entity, along with other information reasonably requested by Purchasing Entity regarding Microsoft security practices and policies.

Purchasing Entity is solely responsible for reviewing each Information Security Policy and making an independent determination as to whether it meets Purchasing Entity's requirements.

- C. **Microsoft Audits of DPT Services.** For each DPT Service, Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each DPT Service.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which will be Microsoft's Confidential Information. The Microsoft Audit Report will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If Purchasing Entity requests, Microsoft will provide Purchasing Entity with each Microsoft Audit Report so that Purchasing Entity can verify Microsoft's compliance with the security obligations under the DPT. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

- D. **HIPAA/HITECH Business Associate.** If Purchasing Entity is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data, as those terms are defined in 45 CFR § 160.103, this agreement includes execution of the HIPAA Business Associate Agreement ("BAA"), the full text of which identifies the DPT Services to which it applies and is available at <http://aka.ms/BAA>. Purchasing Entity may opt out of the BAA by instructing Contractor to send the following information to Microsoft in a written notice (under the terms of the Contractor's subcontract with Microsoft):

- the full legal name of Purchasing Entity and any Affiliate that is opting out;
 - the volume licensing agreement number to which the opt out applies.
- E. **FedRAMP.** During the term of a Purchasing Entity's subscription for Government Community Cloud Services, those services will be operated in accordance with a written data security policy and control framework that is consistent with the requirements of NIST 800-53 Revision 4, or successor standards and guidelines (if any), established to support Federal Risk and Authorization Management Program (FedRAMP) accreditation at a Moderate Impact level. Microsoft intends for Government Community Cloud Services to support FedRAMP Authority to Operate ("ATO"), and Microsoft will use commercially reasonable efforts to obtain an ATO from a Federal agency, and to maintain such ATO through continuous monitoring processes and by conducting regular FedRAMP audits.
- F. **Background Checks.** Microsoft performs the following background checks on all US personnel who have potential to access Customer Data. Adherence to this policy is one of the control procedures addressed by the Microsoft Audit Report per the section of the Microsoft Online Services Terms titled "Microsoft Audits of Online Services." Such Background Checks will be performed in accordance with the Fair Credit Reporting Act and will consist of Social Security Number trace, seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for job related crimes, Office of Foreign Assets Control List (OFAC) check, Bureau of Industry and Security List (BIS) check and Office of Defense Trade Controls Debarred Persons List (DDTC) check.
- Additionally, for States with which Microsoft has entered into a Microsoft CJIS Information Agreement and provided an FBI CJIS Addendum Certification to the applicable CJIS Systems Agency (CSA, e.g. the California Department of Justice), for its CJIS Covered Services (which are most of the Microsoft Government Community Cloud Services), Microsoft submits its personnel that have access to unencrypted Criminal Justice Information and other Customer Content (including both employees and subcontractors, where applicable) for FBI NCIC fingerprint background checks and adjudication by each such CSA.
- G. **Click-Through Terms.** For the Microsoft In-Scope Services sold and licensed to Purchasing Entities hereunder, no click-through licensing terms presented to end users or administrators, as they pertain to the delivery, operation or use of such services, shall be binding. For clarity, to the extent that certain services may present terms of use for a web portal used to administer and configure the In-Scope Services, or to download software in conjunction with the In-Scope Services, such terms of use shall be binding, to the extent that there are no equivalent terms and conditions in the Master Agreement which pertain to the use of such web portals.

9. Definitions.

"AUP" means the section of the OST titled "Acceptable Use Policy".

"Azure Consumption-Based Services" means any Microsoft Online Service made available for Purchasing Entity's use and consumption under the Microsoft Azure Administrative Portal, following Purchasing Entity's initial subscription order for such services, subject to consumption fees billed to Purchasing Entity (or debited against its prepaid Azure monetary commitment balance, if applicable) as described in the applicable Product Terms.

"Client" means device software, if any, that Contractor or Microsoft provides to Purchasing Entity with In-Scope Services.

"Contractor" means Insight Public Sector.

"Customer Content" means the subset of Customer Data created by users, which includes the following:

- For Office 365 Services, Customer Content shall at least include Exchange Online mailbox content (email body, calendar entries, and the content of email attachments), SharePoint Online site content and the files stored within that site, and Skype for Business Online archived conversations.
- For Microsoft Dynamics CRM Online Services, Customer Content means the entities of Customer Data managed by the Microsoft Dynamics CRM Online Services.
- For Microsoft Azure Core Services, Customer Content includes all Customer Data except as may be noted in the Microsoft Azure Trust Center (which Microsoft may update from time to time, but will not add exceptions for existing Microsoft Azure Core Services in general release).
- For Microsoft Intune Online Services, Customer Content includes all Customer Data except as may be noted in the "Data Location" section of the Microsoft Intune Trust Center.

“Customer Data” means all data, including all text, sound, or image files that are provided to Microsoft by, or on behalf of, Purchasing Entity through its use of In-Scope Services.

“DPT” means the section of the OST titled “Data Processing Terms.”

“DPT Services” means the Microsoft Online Services to which the DPT applies. As of the date this Agreement was executed by the parties, DPT Services include “Microsoft Dynamics CRM Online Services,” “Office 365 Services,” “Microsoft Intune Online Services,” and “Microsoft Azure Core Services,” which consist of the following component Microsoft Online Services:

DPT Services	
Microsoft Dynamics CRM Online Services	Microsoft Dynamics CRM Online services made available through volume licensing or the Microsoft online services portal, excluding (1) Microsoft Dynamics CRM for supported devices, which includes but is not limited to Microsoft Dynamics CRM Online services for tablets and/or smartphones and (2) any separately-branded service made available with or connected to Microsoft Dynamics CRM Online, such as Microsoft Social Engagement, Parature, from Microsoft, and Microsoft Dynamics Marketing.
Office 365 Services	The following services, each as a standalone service or as included in an Office 365-branded plan or suite: Exchange Online, Exchange Online Archiving, Exchange Online Protection, Advanced Threat Protection, SharePoint Online, OneDrive for Business, Project Online, Skype for Business Online, Sway, Office Online, Delve Analytics, Customer Lockbox, and Yammer Enterprise. Office 365 Services do not include Office 365 ProPlus, any portion of PSTN Services that operate outside of Microsoft’s control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded “for Office 365.”
Microsoft Azure Core Services	Cloud Services (web and worker roles), Virtual Machines (including with SQL Server), Storage (Blobs, Tables, Queues), Virtual Network, Traffic Manager, Batch, Web Sites, BizTalk Services, Media Services, Mobile Services, Service Bus, Notification Hub, Workflow Manager, Express Route, Scheduler, Multi-Factor Authentication, Active Directory, Rights Management Service, SQL Database, and HDInsight.
Microsoft Intune Online Services	The cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune such as Mobile Device Management for Office 365.

“Government Community Cloud Services” means the Microsoft Online Services identified as such (a subset of DPT Services) in the DPT and Product Terms.

“In-Scope Services” means the Microsoft Online Services for which subscription licenses are sold to Purchasing Entity by Contractor. In-Scope Services include, but are not limited to DPT Services. Except for Azure Consumption-Based Services (which are billed based upon the quantities of such services consumed by Purchasing Entity), Purchasing Entity will order individual licenses from Contractor for all In-Scope Services Licenses.

“Master Agreement” means the agreement (described therein as “NASPO ValuePoint Master Agreement for Cloud Services”) between Contractor and the Lead State, subject to the terms and conditions of the Participating Addendum between Contractor and Purchasing Entity’s State (if different from Utah), and which resulted from award of contract under Utah Solicitation Number CH16012.

“Microsoft” means Microsoft Corporation, which is subcontractor to Contractor and delivers the In-Scope Services.

“Online Services” means the Microsoft-hosted services for which Purchasing Entity acquires Licenses from Contractor hereunder.

“OST” means the Microsoft “Online Services Terms,” which are additional terms that apply to Purchasing Entity’s use of Online Services published on the Volume Licensing Site and updated from time to time, and is subject to terms and conditions in the OST which govern which version of OST is applicable to a particular subscription order.

“Portal” means the Online Services Portal for each In-Scope Service.

“Product Terms” means the document that provides information about Microsoft Products and Professional Services available through volume licensing. The Product Terms document is available on the Volume Licensing Site and is updated from time to time.

“Security Incident” means any unlawful access, use, theft or destruction to any Customer Data stored on Microsoft’s equipment or in Microsoft’s facilities, or unauthorized access to such equipment or facilities resulting in use, theft, loss,

disclosure, alteration or destruction of Customer Data. All references to “Data Breach” in the Master Agreement shall be deemed to mean Security Incident.

“Service Level Agreement” (“SLA”) means the document which specifies the standards to which Microsoft agrees to adhere and by which it measures the level of service for an In-Scope Service. Microsoft’s current and archived prior version SLAs are available at the Volume Licensing Site. With respect to any In-Scope Service ordered under the this Agreement, the most current SLA available at the onset of a subscription License term shall apply to that In-Scope Service for the duration of that subscription License Term, after which (for any subsequent renewal subscription License term) it will be superseded by the version current at the time of renewal.

“Subscription” means an order for a quantity of an In-Scope Service, including but not limited to (a) orders for User Subscription Licenses for one or more In-Scope Services; and (b) an order for the purpose of establishing a subscription for Azure Consumption-Based Services.

“Volume Licensing Site” means <http://www.microsoft.com/licensing/contracts> or a successor site.

Enterprise Enrollment

This Microsoft Enterprise Enrollment is entered into between the Purchasing Entity and Insight Public Sector. Under this Enrollment, Government Partner may order In-Scope Services for the benefit of the Purchasing Entity and not for use or access by Government Partner or any other third party.

This Enrollment consists of: (1) these terms and conditions, (2) the terms of the Enterprise Agreement, (3) any supplemental contact information form or Previous Agreement/Enrollment form and other forms that may be required and (4) any order submitted under this Enrollment. This Enrollment may only be entered into under the Agreement titled "Microsoft NASPO ValuePoint Enterprise Agreement for Government Partners".

All terms used but not defined are located at <http://www.microsoft.com/licensing/contracts>.

Effective date. The initial effective date will be the date this Enrollment is accepted by Microsoft, unless this Enrollment renews Subscription Licenses from another agreement or enrollment, in which case the initial effective date will be the day following the expired agreement's or enrollment's expiration date. The effective date of any subsequent renewal term shall be the day following the expiration of the previous term. Any reference to "anniversary date" refers to the anniversary of the effective date applicable during each term.

Term. The initial term of this Enrollment will expire on the last day of the month, 36 full calendar months from the effective date of the initial term. If the Enrollment is renewed, the renewal term will expire 36 full calendar months after the effective date of the renewal term. Notwithstanding the foregoing, the term will expire or terminate upon the expiration or early termination of the Master Agreement, unless otherwise agreed in writing between the parties, as set forth in the Agreement. Any reference in this Enrollment to "day" will be a calendar day.

Prior Enrollment(s). If renewing Subscription Licenses from another enrollment or agreement, the previous enrollment or agreement number must be identified.

Enrollment Details

1. Purchasing Entity's Enterprise.

- a. Identify which Affiliates are included in the Enterprise. (Required) Affiliates must be entire entities, not partial entities.

Check **only one** box in this section. If no boxes are checked, Microsoft will deem the Enterprise to include the Purchasing Entity only, with no other Affiliates included. If more than one box is checked, Microsoft will deem the Enterprise to include the largest number of Affiliates.

- ☐ Purchasing Entity only
- ☐ Purchasing Entity and all its Affiliates
- ☐ Purchasing Entity and the following Affiliate(s) (Only identify specific affiliates to be included if fewer than all Affiliates are to be included in the Enterprise):

- ☐ Purchasing Entity and all Affiliates, with the following Affiliate(s) excluded

- b. Please indicate whether Purchasing Entity's Enterprise will include all new Affiliates acquired after the start of this Enrollment: ☐ Yes, ☐ No.

2. Contact information.

Each party will notify the other in writing if any of the information in the following contact information page(s) changes. The asterisks (*) indicate required fields. By providing contact information, Purchasing Entity consents to its use for purposes of administering this Enrollment by Government Partner, its Affiliates, and other parties that help administer this Enrollment. The personal information provided in connection with this Enrollment will be used and protected in accordance with the privacy statement available at <https://www.microsoft.com/licensing/servicecenter>.

- a. **Purchasing Entity primary contact.** This contact is the primary contact for the Enrollment from within Purchasing Entity. This contact is also an Online Administrator for the Volume Licensing Service Center and may grant online access to others. The primary contact will be the default contact for all purposes unless separate contacts are identified for specific purposes.

Name of entity (must be legal entity name)*

Contact name: First* Last*

Contact email address*

Street address*

City*

Province*

Postal code*

Country*

Phone

Tax ID

** indicates required field*

- b. Notices contact and Online Administrator.** This contact (1) receives the contractual notices, (2) is the Online Administrator for the Volume Licensing Service Center and may grant online access to others, and (3) is authorized to reserve Licenses for eligible Online Services, including adding or reassigning Licenses, and stepping-up prior to an annual order.

☐ Same as Purchasing Entity primary contact (default if no information is provided below, even if box is not checked)

Contact name: First*

Last*

Contact email address*

Street address*

City*

Province*

Postal code*

Country*

Phone

Language preference. Choose the language for notices. English

☐ This contact is a third party (not Purchasing Entity). Warning: This contact receives personally identifiable information about Purchasing Entity.

** indicates required field*

- c. Online Services Manager.** This contact is authorized to (1) manage the Online Services ordered under the Enrollment and (2) reserve Licenses for eligible Online Services, including adding or reassigning Licenses and stepping-up prior to an annual order.

IMPORTANT NOTE: If the email address used for Online Services Manager is the same email address that has been used either (a) a tenant administrator (for an existing Microsoft Online Services tenant), or (b) as Online Services Manager pursuant to another enrollment that is associated with a tenant for Microsoft Online Services, then the subscription order(s) associated with this Enrollment will automatically be associated with that tenant.

The only way to ensure that a new tenant is created will be to ensure that a unique email address, not used for either of the foregoing purposes, is used. When a unique email address is used, the Online Services Manager will receive an activation email at that address, and will be presented with a choice to “Sign Up” (for a new tenant) or “Sign In” (to associate this Enrollment with an existing tenant).

☐ Same as notices contact and Online Administrator (default if no information is provided below, even if box is not checked)

Contact name: First*

Last*

Contact email address*

Phone

☐ This contact is from a third party organization (not Purchasing Entity). Warning: This contact receives personally identifiable information of Purchasing Entity.

** indicates required field*

3. Price level.

The price level indicated in this section will be the price level for the initial Enrollment term for all Products ordered on the Product Selection Form and for any Additional Products in the same pool(s).

Qualified Devices: Government Partner represents that the total number of Qualified Devices in Purchasing Entity's Enterprise is, or will be increased to, this number during the initial term of this Enrollment (This number must be equal to at least 250 Qualified Devices).	
Qualified Users: Government Partner represents that the total number of Qualified Users in Purchasing Entity's Enterprise is, or will be increased to, this number during the initial term of this Enrollment (This number must be equal to at least 250 Qualified Users).	

Number of desktops/users	Price level	Price level (for pools in which Government Partner orders an Enterprise Product or Enterprise Online Service):	Qualified Desktop	Qualified User
15,000* and above	D		D	D
Price level (for pools in which Government Partner does not order an Enterprise Product):			Price level "D"	

By signing below, Purchasing Entity confirms that all information provided in this Agreement is correct.

Signature*

Printed name*

Printed title*

Date*

