SCO ID:

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
20-14311	CDT-7502

1. This Agreement is entered into between the Contracting Agency and the Contractor named below:

CONTRACTING AGENCY NAME
California Department of Technology

CONTRACTOR NAME
Dell Marketing LP

2. The term of this Agreement is:

START DATE
June 1, 2022

THROUGH END DATE
May 31, 2024

3. The maximum amount of this Agreement is:
$18,000,000.00 - Eighteen Million and Zero Cents

4. The parties agree to comply with the terms and conditions of the following exhibits, which are by this reference made a part of the Agreement.

Exhibits		Title	Pages
	Exhibit A	Statement of Work	7
	Exhibit A-1	Service Level Agreements (SLAs)	1
	Exhibit B	Payment and Invoicing	2
+ -	Exhibit C	Cost Proposal Worksheet	1
+ -	Exhibit D	Security and Data Protection	1
+ -	Appendix A	Microsoft Customer Terms and Conditions for Government Contract	1
+ -	Exhibit 1	Negotiated General Provisions	14
+ -	Exhibit 2	Negotiated Special Provisions	6
+ -	Exhibit 3	Other Solicitation Flow Down Terms	11
+ -	Exhibit 4	Additional Microsoft-CDT Terms	14
+ -	AMD 1	Amendment 1 to Exhibit 4: Microsoft CJIS Amendment	6
+ -	AMD 1 - Appendix A	To CJIS Amendment	3
+ -	AMD 2	Amendment 2 to Exhibit 4: Microsoft IRS 1075 Amendment	4
+ -	AMD 2 - Appendix A	To IRS 1075 Amendment	10
+ -	Exhibit 5	Initial MS OST	28
+ -	Exhibit 6	Initial MS SLA	48

SCO ID:

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
20-14311	CDT-7502

Exhibits	Title	Pages
+ - 	Contractor's final proposal and the entire invitation to Negotiate, Event ID 0000019460, are hereby incorporated as part of this contract.	

Items shown with an asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.
These documents can be viewed at https://www.dgs.ca.gov/OLS/Resources

IN WITNESS WHEREOF, THIS AGREEMENT HAS BEEN EXECUTED BY THE PARTIES HERETO.

CONTRACTOR

CONTRACTOR NAME (if other than an individual, state whether a corporation, partnership, etc.)
Dell Marketing LP

CONTRACTOR BUSINESS ADDRESS	CITY	STATE	ZIP
PO Box 910916	Pasadena	CA	91110

PRINTED NAME OF PERSON SIGNING	TITLE
Charyne Greenup	Contract Administrator
CONTRACTOR AUTHORIZED SIGNATURE	DATE SIGNED
Charyne Greenup	May 23, 2022

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME
California Department of Technology

CONTRACTING AGENCY ADDRESS	CITY	STATE	ZIP
10860 Gold Center Drive	Rancho Cordova	CA	95670

PRINTED NAME OF PERSON SIGNING	TITLE
Russ Nichols	Acting Director
CONTRACTING AGENCY AUTHORIZED SIGNATURE	DATE SIGNED
Russ Nichols (May 26, 2022 14:56 PDT)	May 26, 2022
CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL	EXEMPTION (If Applicable)
	Exempt per CDT Purchasing Authority Delegation No. CDT-7502

EXHIBIT A
STATEMENT OF WORK

1. Contract Description

   Dell Marketing LP (hereinafter referred to as the “Contractor”) agrees to provide the State of California and local government agencies, via the California Department of Technology (CDT) (hereinafter referred to as the “State” and/or “CDT”), the entire portfolio of products as identified in the contract and will be the primary point of contact for data collection, reporting, and provisions of Infrastructure as a Service (IaaS) and/or Platform as a Service (PaaS) Cloud Services for the High level to the State. This Statement of Work (SOW) covers terms and conditions for the entire portfolio of products as identified in the contract for IaaS and/or PaaS.

   Contractor is not allowed to offer any telecommunications or other services to CDT via a client-facing portal that are offered in their Cloud Service Provider’s Marketplace or portal where those, or like products or services conflict with other State mandatory contracts. Contractor shall work cooperatively with CDT to ensure prohibited Cloud Service Provider Marketplace products are not resold through this contract.

   This includes cloud based voice services, traditional analog, digital, IP, and wireless telecommunications services. Cloud based voice services include but are not limited to Cloud Telephony, Cloud Calling, Cloud PBX , Contact Center, Unified Communications, Video Conferencing, or any other cloud based software or service that facilitates the transmission, management or operation of voice or other communications.

2. Term/Period of Performance

   a. The term of this Agreement shall commence on June 1, 2022, or the date the Agreement is approved by the California Department of Technology, whichever is later (referred to herein as the “Effective Date”) and continue through May 31, 2024.
   b. The State reserves the option to extend the term of this Agreement at its sole discretion for up-to two (2) optional, two (2) year extensions.
   c. The Contractor shall not be authorized to deliver or commence services as described in this SOW until written approval has been obtained from the State. Any delivery or performance of service that is commenced prior to the signing of the Agreement shall be considered voluntary on the part of the Contractor and not eligible for payment nor compensation.

3. Contractor’s Proposal Response

   The Contractor’s response and Request for Proposal (RFP) Number 33526 are incorporated by reference into this Agreement as if attached hereto.

4. Installed On

   The cloud IaaS and/or PaaS is wholly Contractor-owned, managed and installed at the Cloud Service Provider (CSP) or the Contractor’s site.

5. Data/Information Categorization:

   Per SAM 5305.5, the State’s data housed on the Contractor’s server(s) must be at the FedRAMP High level.

6. Notices

All notices required by, or relating to, this Agreement shall be in writing and shall be sent to the parties of this Agreement at their address as contained within unless changed from time to time, in which event each party shall notify the other in writing, and all such notices shall be deemed duly given if deposited, postage prepaid, in the United States mail or e-mailed and directed to the customer service contacts referenced in the User Instructions.

The technical representative during the term of this Agreement will be:

State Agency		**Manufacturer**	
CDT, Office Technology Services		Microsoft	
Attn:	Scott MacDonald	Attn:	Rick Joyer
Phone:	(916) 228-6460	Phone:	(714) 469-6578
E-mail:	Scott.Macdonald@state.ca.gov	Web:	rijoyer@microsoft.com

Contract inquiries should be addressed to:

State Agency		**Contractor**	
CDT, Acquisitions & IT Program Management Branch		Dell Marketing LP	
Attn:	Jamie Wong	Attn:	Ashley Salinas
Address:	PO Box 1810 Rancho Cordova, CA 95741	Address:	One Dell Way Round Rock, Texas 78682
Phone:	(916) 431- 4105	Phone:	(512) 542-1237
E-mail:	Jamie.Wong@state.ca.gov	E-mail:	a.salinas@dell.com

7. Technical Requirements

a. The CSP must be FedRAMP Authorized at the High level (commensurate with the Program level being proposed by the proposal due date as identified in Section I.E., Key Action Dates).
b. The Contractor must provide a portal and training for CDT for self-provisioning. The training shall be included in the bid price.
c. The CSP must ensure, if using Network Edge Services, that the NIST ISO/IEC 27018:2019 certification has been achieved for the specific services being added to the portfolio. These services augment the CSP's IaaS and/or PaaS portfolio and may be included as part of the portfolio services without obtaining a FedRAMP Authorization to Operate (ATO) for that service. The Network Edge Services must have achieved NIST ISO/IEC 27018:2019 certification, which provides guidance aimed at ensuring that CSP's offer suitable information security controls to protect the privacy of their customers' clients by securing Personally Identifiable Information (PII) entrusted to them, for the specific service being added to the portfolio. Services that have the potential of containing confidential and/or sensitive data must have the ability to contain that service within the continental United States.
d. The CSP shall enable the State to encrypt Personal Data and Non-Public Data at rest, in use, and in transit with controlled access. The SOW and/or Service Level Agreement (SLA) will specify which party is responsible for encryption and access control of the State Data for the service model under the Agreement. If the SOW and/or SLA and the Agreement are silent, then the State is responsible for encryption and access control.
e. The CSP must provide the state with the root access to the master payer account.

Application Programming Interface Requirements (M)

The Contractor's IaaS and/or PaaS must provide open Application Programming Interfaces (API) that provide the capability to:

a. Migrate workloads between the public cloud and the State's private on-premise cloud where CDT acts as the broker of those services and has the ability to logically separate individual customers;
b. Define networks, resources and templates within a multi-tenant environment with the use of available APIs;
c. Provision and de-provision virtual machines and storage within a multi-tenant environment;
d. Add, remove and modify computing resources for virtual machines within a multi-tenant environment;
e. Add, remove and modify object and block storage within a multi-tenant environment;
f. Retrieve financial and billing information that provides detailed information for each CDT customer (i.e. Eligible Public Entity) subscriber;
g. Retrieve performance indicators for all workloads in the multi-tenant environment;
h. Retain all workloads and support within the U.S.
i. Retrieve log data from all workloads; and
j. Provide the ability to model potential workloads to determine cost of services.

Environment Requirements (M)

The Contractor's cloud environment must have the ability to:

a. Provide a multi-tenant environment that supports a parent/child administrative relationship that enables the CDT (parent) to programmatically apply compliance and regulatory requirements and standards down to the Eligible Public Entities.
b. Provide all tested and compliant modules under the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search **and/or** with FIPS 140-3 compliant cryptographic modules https://csrc.nist.gov/publications/detail/fips/140/3/final;
c. Support cost tracking by resource tags or other solutions to tracking costs for Eligible Public Entities;
d. Run and manage web applications, including .NET environments;
e. Provide managed database services with support for multiple database platforms;
f. Support Security Access Markup Language (SAML) federation;
g. Provide integration with a customer's on premise Active Directory;
h. Provide a managed service to create and control encryption keys used to encrypt data;
i. Provide a dedicated Hardware Security Module (HSM) appliance for encryption key management;
j. Provide services to migrate workloads to and from the State's VMware and HyperV environments; and
k. Provide dashboard reporting that provides performance monitoring, usage and billing information.

8. Reserved Instances (NM)

Reserved Instances may be available for use on this Agreement.

9. Contractor Responsibilities

a. The Contractor will assign a contact person for contract management purposes. The Contractor Contract Manager must be authorized to make decisions on behalf of the Contractor.
b. The Contractor shall allow the CDT or its designated third party to audit conformance including but not limited to contract terms, pricing, costing, ordering, invoicing, and reporting. Such reviews shall be conducted with at least thirty (30) calendar days advance written notice and shall not unreasonably interfere with the Contractor's business. The CSP shall allow the CDT or its designated third party to audit conformance to Attachment 14.B.4, Application Programming Interface, and Attachment 14.B.5, Environment.
c. The Contractor shall promptly notify the Eligible Public Entity in writing of any unresolved issues or problems that have been outstanding for more than three (3) business days. The Eligible Public Entity shall notify the Contractor of the same.
d. The Contractor will ensure all promotional materials or press releases referencing the contract shall be submitted to the CDT Contract Administrator for review and approval prior to release.
e. The Contractor shall only accept orders from CDT. The Contractor shall not accept purchase documents for this contract that: are incomplete; contain non-contract items; or contain non-contract terms and conditions. The Contractor must not refuse to accept orders from CDT for any other reason without written authorization from the CDT Contract Administrator.
f. The Contractor must provide CDT with an order receipt acknowledgment via e-mail within one (1) business day after receipt of an order.
g. The Contractor shall ensure invoices be submitted to the CDT on behalf of the Eligible Public Entity on a quarterly or monthly basis in arrears.

   Invoices must include:
   - Eligible Public Entity Name
   - Dollar amounts
   - Usage
   - Discount
   - Date of provided services
   - Purchase Order number
   - Item Description
   - Booking Confirmation #
   - Product name
   - Code/description/customer department/subscription account number (if applicable)
   - Term date

h. The Contractor will ensure payments are to be made in accordance with Sections 23 of the Negotiated General Provisions - Exhibit 1.
i. The Contractor must provide the State with a catalog of authorized services and architecture patterns.
j. The Contractor must maintain an online catalog of available SLAs meeting the minimum requirements of Section VI, Business/Technical Requirements.

   1) The catalog website shall contain:
      i. Detailed descriptions of available IaaS and/or PaaS Cloud Services SLAs; and
      ii. Public pricing (MSRP/MSLP) on which the State discount is based.

2) The Contractor shall notify the State of any updates to the Catalog website.

10. State's Responsibilities

a. CDT will be the only authorized user of the contract and will submit orders on behalf of Eligible Public Entities using a Purchasing Authority Purchase Order (Std. 65) or using the FI$Cal Purchase Order process. Blanket orders are acceptable.

b. The State reserves the right to receive credits in the event the Contractor fails to meet an applicable SLA (see Exhibit A-1).

11. Information and Data Ownership

All information and data stored by the State of California (this includes all public agencies in the State of California that may use this Agreement) using the service provider's system(s) remains the property of the State. As such, the service provider agrees to not scan, capture or view such information or data unless expressly authorized by the appropriate representatives of the State of California. Prior to the release of any information or data belonging to the State of California to any law enforcement agency, the service provider must notify and gain the express approval of the CDT and the California Department of Justice. The service provider may respond to subpoenas or other judicial mandates that forbid notice to CDT, without breach of contract. Upon the conclusion of service as notified by the State, the service provider must provide to the State a copy of all State data stored in the service providers system within five (5) business days in the Exit Data Format specified in the technical requirements. The State and the Contractor may mutually agree on a longer time period, as required by the amount of data or the format requested. Upon acceptance of this data by the State of California, the service provider shall purge the data from any and all of its systems and provide the State confirmation that such steps have occurred within ten (10) business days. Failure to comply with any of these terms may be grounds for termination for default.

12. Problem Escalation

a. The parties acknowledge/agree that certain technical and project-related problems or issues may arise and that each party shall bring such matters to the immediate attention of the other party when identified. Known problems or issues shall be reported in regular weekly status reports or meetings. However, there may be instances where the severity of the problem justifies escalated reporting. To this extent, the State will determine the next level of severity, and notify the appropriate State and CSP personnel. The personnel notified, and the time-period taken to report the problem or issue, shall be at a level commensurate with the severity of the problem or issue.

b. The State personnel include, but are not limited to the following:

First Level: Service Desk – (916) 464-4311, ServiceDesk@state.ca.gov
Second Level: Christine Nguyen – (916) 228-6414, christine.nguyen@state.ca.gov or Taron Walton – (916) 228-6317, taron.walton@state.ca.gov
Third Level: Cary Yee, (916) 228-6493, cary.yee@state.ca.gov
Fourth Level: Scott MacDonald – (916) 228-6460, scott.macdonald@state.ca.gov

c. The Contractor personnel include, but are not limited to the following:

First Level: Trevor Azavedo, (503) 830-3427. Trevor_Azavedo@dell.com Gerard Ear, (512) 720-3258. Gerard_Ear@dell.com
Second Level: Tyler White, (512) 961-1107. Joseph.T.White@Dell.com
Third Level: Kim Wood, (737) 227-1539. Kim.Wood@Dell.com

13. Amendments

Consistent with the terms and conditions of the original solicitation, and upon mutual consent, CDT and the Contractor may execute amendments to this Agreement. No amendment or variation of the terms of this Agreement shall be valid unless made in writing, and agreed upon by both parties and approved by the State, as required. No verbal understanding or agreement not incorporated into the Agreement is binding on any of the parties. Changes to the contract regarding the administrator, list pricing and technical changes to SKUs and descriptions, will be handled by supplement only and must be approved by the contract administrator.

14. Cancellation Provisions

CDT may exercise its option to terminate the resulting Agreement at any time with thirty (30) calendar days' prior written notice.

15. Federal Tax Administration Requirements

Subject to the Internal Revenue Service (IRS), federal tax information (FTI) requirements, if an unfavorable response is received by the IRS, this contract will be terminated immediately, per Negotiated General Provisions – Exhibit 1, Section 17, Termination for Default.

16. Security and Data Protection Requirements

The State must ensure Agreements with State and non-state entities include provisions which protect and minimize risk to the State when engaging in the development, use, or maintenance of information systems, products, solutions, or services. In order to comply with the State Administrative Manual (SAM) Section 5305.8, Contractor must comply with Exhibit E, Security and Data Protection.

17. DVBE Reporting

Military and Veteran Code (MVC) 999.5(d), Government Code (GC) 14841, and California Code of Regulations (CCR) 1896.78(e) require that if the Prime Contractor had a Disabled Veteran Business Enterprise (DVBE) firm perform any element of work in the performance of the Agreement, to report the DVBE information.

Prime Contractors are required to maintain records supporting the information that all payments to DVBE subcontractor(s) were made. The Prime DVBE Subcontracting form can be found at the following link: https://www.dgs.ca.gov/PD/Services/Page-Content/Procurement-Division-Services-List-Folder/File-a-DVBE-Subcontractor and the instructions can be found at the following link: http://www.documents.dgs.ca.gov/pd/smallbus/Prime%20DVBE%20Sub%20Report%20Instruction.doc. Completed forms are to be e-mailed to: primeDVBE@state.ca.gov.

18. Reserved Instances

Reserved Instances (RIs) are available for use on this contract.

EXHIBIT A-1
SERVICE LEVEL AGREEMENTS (SLAs)

Upon award, the Contractor's SLA will be incorporated into the Agreement.

a) Service Credits

1) The state reserves the right to obtain credit in the event the Contractor fails to meet an applicable SLA.

2) Service Credits will be applied against State's next invoice. A Service Credit will be applicable and issued only if the credit amount is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other Contractor's service or account. The State's remedy for any non-excluded down time is the receipt of a service credit (if eligible) in accordance with the terms of this Exhibit A-1. Upon expiration or non-renewal of this Agreement, all service credits will be forfeited (for example, if the non-excluded downtime occurs in the last month of the Agreement term and State does not renew, then the service credit is forfeited).

b) Performance Discounts

1) In addition to any Service Credits described herein, in the event the Contractor fails to meet the Service Commitment for a period of three (3) consecutive months or an aggregate of five (5) months over an eighteen (18) month period, the State shall be entitled to an additional 15% discount off the next invoice following month in which the Contractor failed to meet the Service Commitment.

Notwithstanding the Service Credits and Performance Discounts provided herein, the State reserves the right to terminate the contract pursuant to Section 17 of the Negotiated General Provisions – Exhibit 1, for Contractor's failure to meet the Service Commitment.

EXHIBIT B
PAYMENT AND INVOICING

1. **Payment/Invoicing:**

   a. Payment for IaaS and/or PaaS will be made quarterly or monthly in arrears upon receipt of a correct invoice, except Reserved Instances (RIs) as described below. The invoice shall include booking confirmation of the CDT order; including but not limited to, the product name, code/description/customer department/subscription account number (if applicable), and term date, date of provided services; and shall reference the Agency Order Number.

      1) Reserved Instances (RI) Payment/Invoicing

         - Payment will be made according to the terms in this section, upon receipt of a correct invoice for RI(s) and must be included separately as its own line item and identified as an RI.

   b. Fiscal Management Report

      1) The Contractor agrees to provide quarterly Fiscal Management Reports electronically in Excel format, as shown in Item 3) Sample Template below, identifying services in accordance with the Agreement at no additional cost. The report must contain, but not limited to, the product name, code/description/customer department/subscription account number, term date, services being utilized, and the monthly amount being charged.

      2) Adhoc reports must be provided when/if requested.

      3) Sample Template

Account Name	**Account Number**	**Month 1 Charges**	**Month 2 Charges**	**Month 3 Charges**	**TOTAL**
Department Name	000000000	100.00	100.00	100.00	300.00

   c. Submit your invoice using only **one** of the following options:

      1) Send via U.S. mail in **TRIPLICATE** to:

         California Department of Technology
         Administration Division – Accounting Office
         P. O. Box 1810
         Rancho Cordova, CA 95741

         OR

      2) Submit electronically at: APInvoices@state.ca.gov.

2. Prompt Payment Clause:

Payment will be made in accordance with, and within the time specified, in Government Code Chapter 4.5, commencing with Section 927. Payment to small/micro businesses shall be made in accordance with and within the time specified in Chapter 4.5, Government Code 927 et seq.

3. Budget Contingency Clause:

a. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Contract does not appropriate sufficient funds for the program, this Contract shall be of no further force and effect. In this event, the State shall have no liability to pay any funds whatsoever to the Contractor or to furnish any other considerations under this Contract and Contractor shall not be obligated to perform any provisions of this Contract.

b. If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Contract with no liability occurring to the State, or offer a contract amendment to the Contractor to reflect the reduced amount.

EXHIBIT C
COST PROPOSAL WORKSHEET

Published list price or greater for IaaS offerings for FedRAMP High.

Contract Line Item # (CLIN)	Item Description	Contract Discount
2	Infrastructure as a Service for FedRAMP High	14.65%

Item Description	Reserved Instance Discount % off MSIP/MSRP
Infrastructure as a Service	***7.65%***

Published list price or greater for PaaS offerings for FedRAMP High.

Item Description	Published List Price	Discount Level	Contract Discount %	Contract $
Platform as a Service	$250,000	Base	14.65%	$213,375.00
	$250,000	A	14.65%	$213,375.00
	$250,000	B	14.65%	$213,375.00
	$250,000	C	14.65%	$213,375.00
	$1,000,000		**Evaluated Total:**	$ 853,500.00

Item Description	Reserved Instance Discount % off MSIP/MSRP
Platform as a Service	***7.65%***

(link to catalog)	All prices are in US Dollars (S). This is a summary estimate, not a quote. For up to date pricing information, please visit: https://azure.microsoft/pricing/calculator

EXHIBIT D
SECURITY AND DATA PROTECTION

Contractor shall certify to The National Institute of Standards and Technology (NIST) 800-171 standard and the DGS Cloud Computing Services Special Provisions publication requirements. At a minimum, provision shall cover the following:

1. The Contractor assumes responsibility of the confidentiality, integrity and availability of the data under its control. The Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards at all times during the term of the Agreement to secure such data from data breach or loss, protect the data and information assets from breaches, introduction of viruses, disabling of devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its data or affects the integrity of that data.

2. Confidential, sensitive or personal information shall be encrypted in accordance with SAM 5350.1 and SIMM 5305-A.

3. The Contractor shall comply with statewide policies and laws regarding the use and protection of information assets and data. Unauthorized use of data by Contractor or third parties is prohibited.

4. Signed Security and Confidentiality Statement for all personnel assigned during the term of the Agreement.

5. Apply security patches and upgrades, and keep virus protection software up-to-date on all information asset on which data may be stored, processed, or transmitted.

6. The Contractor shall notify the State data owner immediately if a security incident involving the information asset occurs.

7. The State data owner shall have the right to participate in the investigation of a security incident involving its data or conduct its own independent investigation. The Contractor shall allow the State reasonable access to security logs, latency statistics, and other related security data that affects this Agreement and the State's data, at no cost to the State.

8. The Contractor shall be responsible for all costs incurred by the State due to security incident resulting from the Contractor's failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, destruction; loss, theft or misuse of an information asset. If the contractor experiences a loss or breach of data, the contractor shall immediately report the loss or breach to the State. If the State data owner determines that notice to the individuals whose data has been lost or breached is appropriate, the contractor will bear any and all costs associated with the notice or any mitigation selected by the data owner. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data.

9. The Contractor shall immediately notify and work cooperatively with the State data owner to respond timely and correctly to public records act requests.

10. The Contractor will dispose of records of State data as instructed by the State during the term of this agreement. No data shall be copied, modified, destroyed or deleted by the Contractor other than for normal operation or maintenance during the Agreement period without prior written notice to and written approval by the State.

11. Remote access to data from outside the territorial United States, including remote access to data by authorized support staff in identified support centers, is prohibited unless approved in advance by the State.

12. The physical location of Contractor's data center where the Data is stored shall be within the territorial United States.

1/17/18

Appendix A
Microsoft Customer Terms and Conditions for Government Contract

Section 1: Requirement to incorporate Microsoft Customer Terms and Conditions. Collectively, Microsoft calls each of the Exhibits (and the Amendments thereto), listed below in this Section 1, the "Microsoft Customer Terms and Conditions" (as also defined in Section 1 of the Agreement). Government Partner agrees to include (and make binding upon CDT), in the Government Contract, each of these Exhibits and Amendments, the text of which appears in in Section 2 of this Appendix A, below:

(1) **The Negotiated General Provisions** (Exhibit 1).

(2) **The Negotiated Special Provisions** (Exhibit 2).

(3) **Other Solicitation Flow Down Terms** (Exhibit 3).

(4) **The Additional Microsoft - CDT Terms** (Exhibit 4), including the following amendments thereto:

a. **CJIS Amendment** (Amendment 1), solely applicable to Criminal Justice Information.

b. **IRS 1075 Amendment** (Amendment 2), solely applicable to Federal Tax Information.

(5) **The Locked OST** (Exhibit 5).

(6) **The Locked SLA** (Exhibit 6).

Section 2: Exhibits and Amendments of the Microsoft Customer Terms and Conditions. The parties acknowledge that

a. Microsoft and CDT engaged in the Cloud Service Provider negotiation as mentioned in the section of the Solicitation titled "Key Action Dates."

b. The result of such negotiation was mutual agreement between CDT and Microsoft, with respect to incorporation of the terms and conditions of the Exhibits and Amendments shown below in this Section.

Accordingly, Government Partner shall include the following Exhibits and Amendments of Appendix A in its Government Contract with CDT, subject to the other terms and conditions of this Agreement between Microsoft and Government Partner.

Remainder of Page Intentionally Left Blank

Exhibit 1
Negotiated General Provisions

These Negotiated General Provisions shall apply to CDT' (and its User Agencies') use of Permitted Services, and are hereby added to the Government Contract (as defined in Exhibit 4, below). The Negotiated General Provisions shall supersede the original document titled **"Reseller Enabled General Provisions – Cloud Computing,"** referenced in the Solicitation. Except for those provisions in this Exhibit 1 which are marked to be applicable only to the Reseller (which is the Contractor hereunder), Microsoft has accepted flow-down of these Negotiated General Provisions in its separate contract with Contractor.

---

1. DEFINITIONS: Unless otherwise specified in the Statement of Work, the following terms shall be given the meaning shown, unless context requires otherwise.

a) **"Application Program"** means a computer program which is intended to be executed for the purpose of performing useful work for the user of the information being processed. Application programs are developed or otherwise acquired by the user of the Hardware/Software system, but they may be supplied by the Contractor.

b) **"Business entity"** means any individual, business, partnership, joint venture, corporation, S-corporation, limited liability company, sole proprietorship, joint stock company, consortium, or other private legal entity recognized by statute.

c) **"Buyer"** means the State's authorized contracting official.

d) **"Contract"** means this Contract or agreement (including any purchase order), by whatever name known or in whatever format used.

e) **"Contractor"** means the Business Entity with whom the State enters into this Contract. Contractor shall be synonymous with "supplier", "vendor", "Reseller", or other similar term.

f) **"Deliverables"** means the Services and other items (e.g. reports) to be delivered pursuant to this Contract, including any such items furnished incident to the provision of services.

g) **"Documentation"** means manuals and other published materials necessary or useful to the State in its use or maintenance of the Services provided hereunder and includes online materials, virtual help, and help desk where available. Manuals and other published materials customized for the State hereunder constitute Work Product if such materials are required by the Statement of Work.

h) **"Eligible State Entity"** means each of the California State entities authorized to purchase the Deliverables and services offered hereunder which will be documented at the time of contract execution, and which the parties agree may be amended as needed from time to time in order to accommodate reorganization of the State government.

i) **"Goods"** means all types of tangible personal property, including but not limited to materials, supplies, and equipment (including computer and telecommunications equipment).

j) **"Hardware"** usually refers to computer equipment and is contrasted with Software. See also equipment.

k) **"Infrastructure as a Service"** means commercial services offered for sale to the State and are defined by the National Institute of Standards and Technology (NIST) Special Publication 800-145 or its successors.

l) **"Platform as a Service"** means commercial services offered for sale to the State and are defined by the National Institute of Standards and Technology (NIST) Special Publication 800-145 or its successors.

m) **"Maintenance"** means that maintenance performed by the Contractor which results from a Services failure, and which is performed as required, i.e., on an unscheduled basis.

n) **"Reseller"** means the agent(s) of Microsoft authorized to perform aspects of this agreement as specified herein including, but not limited to sales, fulfillment, invoicing, returns, and customer service.

o) **"Services"** means the cloud computing services, including Infrastructure as a Service and Platform as a Service but not Software as a Service, offered to the State by the Contractor herein.

p) **"Software"** means an all-inclusive term which refers to any computer programs, routines, or subroutines supplied by the Contractor, including operating Software and Application Programs

q) **"State"** means the government of the State of California, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the State of California.

r) **"State Data"** means all data submitted to, processed by, or stored in the Contractor's Services under this contract and includes but is not limited to all data that originated with the State, all data provided by the State or its Users, and data generated, manipulated, produced, reported, or otherwise emanating from or by applications run by the State on the Services. For clarity, State Data is synonymous with "Customer Data", as that term is used in various provisions of the Microsoft Customer Terms and Conditions incorporated into the Contract.

s) **"Statement of Work"("SOW")** means the requirements contained in the contract including but not limited to (a) the Microsoft Customer Terms and Conditions and (b) the mutually accepted technical requirements, for cloud computing services, including Infrastructure as a Service and Platform as a Service but not Software as a Service, offered to the State by the Contractor herein.

t) **"User"** means any individual, organization, or system that accesses the Contractor's Services under this contract including but not limited to State employees, contractors, customers, and constituents.

u) **"U.S. Intellectual Property Rights"** means intellectual property rights enforceable in the United States of America, including without limitation rights in trade secrets, copyrights, and U.S. patents.

2. CONTRACT FORMATION:

a) If this Contract results from a sealed bid offered in response to a solicitation conducted pursuant to Chapters 2 (commencing with Section 10290), 3 (commencing with Section 12100), and 3.6 (commencing with Section 12125) of Part 2 of Division 2 of the Public Contract Code (PCC), then Contractor's bid is a firm offer to the State which is accepted by the issuance of this Contract and no further action is required by either party.

b) If this Contract results from a solicitation other than described in paragraph a), above, the Contractor's quotation or proposal is deemed a firm offer and this Contract document is the State's acceptance of that offer.

c) If this Contract resulted from a joint bid, it shall be deemed one indivisible Contract. Each such joint Contractor will be jointly and severally liable for the performance of the entire Contract. The State assumes no responsibility or obligation for the division of orders or purchases among joint Contractors.

3. COMPLETE INTEGRATION: This Contract, including any documents incorporated herein by express reference, is intended to be a complete integration and there are no prior or contemporaneous different or additional agreements pertaining to the subject matter of the Contract.

4. SEVERABILITY: The Contractor and the State agree that if any provision of this Contract is found to be illegal or unenforceable, such term or provision shall be deemed stricken and the remainder of the Contract shall remain in full force and effect. Either party having knowledge of such term or provision shall promptly inform the other of the presumed non-applicability of such provision.

5. INDEPENDENT CONTRACTOR: Contractor and the agents and employees of the Contractor, in the performance of this Contract, shall act in an independent capacity and not as officers or employees or agents of the State.

6. APPLICABLE LAW: This Contract shall be governed by and shall be interpreted in accordance with the laws of the State of California; venue of any action brought with regard to this Contract shall be in Sacramento County, Sacramento, California. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Contract.

7. COMPLIANCE WITH STATUTES AND REGULATIONS:

a) The State and the Contractor warrants and certifies that in the performance of this Contract, it will comply with all statutes and regulations of the United States and the State of California applicable to protection of data or Personally Identifiable information as defined in the National Institute of Standards and Technology Special Publication 800-122 or any successor Publication, and all statutes applicable to it as a corporation. The Contractor agrees to, defend the State against any loss, cost, damage or liability by reason of the Contractor’s violation of this provision;

b) The State will notify the Contractor of any such claim in writing and tender the defense thereof within reasonable time; and

c) The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) when substantial principles of government or public law are involved, when litigation might create precedent affecting future State operations or liability, or when involvement of the State is otherwise mandated by law, the State may participate in such action at its own expense with respect to attorneys’ fees and costs (but not liability); (ii) where a settlement would impose liability on the State, affect principles of California government or public law, or impact the authority of the State, the California Department of Technology will have the right to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations.

d) If this Contract is in excess of $554,000, it is subject to the requirements of the World Trade Organization (WTO) Government Procurement Agreement (GPA). This provision applies only to the Reseller.

e) To the extent that this Contract falls within the scope of Government Code Section 11135, the Reseller will be responsible to respond to and resolve any complaint brought to its attention, regarding accessibility of its products or services. The State shall designate an authorized representative who will be responsible for submission to Reseller of complaints received by the State regarding the accessibility of Contractor’s products. Reseller shall be responsible to review and respond to all complaints regarding accessibility brought to the attention of the State. The State and Reseller shall work together to determine a reasonable response and resolution of all complaints. The State acknowledges that Reseller can satisfy its duty to respond to and resolve complaints under this provision by taking action it deems appropriate under the circumstances, which may in some instances include no further action beyond responding to the complaint.

8. CONTRACTOR’S POWER AND AUTHORITY: The Contractor warrants that it has full power and authority to grant the rights herein granted and will reimburse the State for any loss, cost, liability, and expense (including reasonable attorney fees) arising out of any breach of this warranty. Further, the Contractor avers that it will not enter into any arrangement with any third party which might abridge any rights of the State under this Contract.

a) The State will notify the Contractor of any such claim in writing and tender the defense thereof within a reasonable time; and

b) The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) when substantial principles of government or public law are involved, when litigation might create precedent affecting future State operations or liability, or when involvement of the State is otherwise mandated by law, the State may participate in such action at its own expense with respect to attorneys' fees and costs (but not liability); (ii) where a settlement would impose liability on the State, affect principles of California government or public law, or impact the authority of the State, the California Department of Technology will have the right to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations.

9. ASSIGNMENT: This Contract shall not be assignable by the Contractor in whole or in part without the written consent of the State. The State's consent shall not be unreasonably withheld or delayed. For the purpose of this paragraph, the State will not unreasonably prohibit the Contractor from freely assigning its right to payment, provided that the Contractor remains responsible for its obligations hereunder.

10. WAIVER OF RIGHTS: Any action or inaction by the State or the failure of the State on any occasion, to enforce any right or provision of the Contract, shall not be construed to be a waiver by the State of its rights hereunder and shall not prevent the State from enforcing such provision or right on any future occasion. The rights and remedies of the State herein are cumulative and are in addition to any other rights or remedies that the State may have at law or in equity.

11. ORDER OF PRECEDENCE: In the event of any inconsistency between the articles, attachments, specifications or provisions which constitute this Contract, the following order of precedence shall apply:

a) These negotiated Reseller-Enabled General Provisions – Cloud Computing (hereafter referred to in the Microsoft Terms and Conditions as Exhibit 1, the "Negotiated General Provisions"). In the instances provided herein where the paragraph begins: "Unless otherwise specified in the Statement of Work" provisions specified in the Statement of Work replacing these paragraphs shall take precedence over the paragraph referenced in these General Provisions Cloud Computing).

b) Contract form, i.e., Purchase Order STD 65, Standard Agreement STD 213, etc., and any amendments thereto. The contract form applies solely to Reseller (as Contractor).

c) The negotiated Reseller-Enabled Special Provisions – Infrastructure as a Service and Platform as a Service (hereafter referred to in the Microsoft Terms and Conditions as Exhibit 2, the "Negotiated Special Provisions").

d) All other Exhibits (and Amendments thereto) which comprise the Microsoft Customer Terms and Conditions (each of which is a part of the Statement of Work), including any specifications incorporated by reference herein. In the case of a conflict between any of these Exhibits and Amendments that is not otherwise expressly resolved in those Exhibits and Amendments, their terms will control in the following order:

   i. The "Other Solicitation Terms" (Exhibit 3), which amends certain provisions of the Solicitation that are incorporated into the Government Contract, and establishes which of such provisions flow down to Microsoft as Cloud Service Provider.

   ii. Any Amendment to the Additional Microsoft - CDT Terms (Exhibit 4). As of the Agreement Effective Date, only the following Amendments are included:

      a. Amendment 1 (CJIS Amendment)

b. Amendment 2 (IRS 1075 Amendment)

iii. All other provisions of Exhibit 4 that do not conflict with its Amendments, except for the following items listed in #4, below.:

iv. The following documents, in order, each of which is incorporated by reference into the Government Contract pursuant to the terms and conditions of the Additional Microsoft - CDT Terms (Exhibit 4):

a. The Product Terms (to the extent applicable to Permitted Services)

b. Subject to the terms and conditions of Section 1.c of Exhibit 4:

1) The Locked OST and Locked SLA (shown in Exhibits 5 and 6 of these Microsoft Customer Terms and Conditions, respectively), solely with respect to the components of Permitted Services expressly included therein; and

2) Each dated version of MS OST and MS SLA applicable to Permitted Services components not expressly included in the Locked OST or Locked SLA.

e) Cost worksheets (applicable only to the Reseller); and

f) All other attachments incorporated in the Contract by reference (applicable only to the Reseller, except to the extent, if any, Microsoft's acceptance of flow down of such attachments is expressly stipulated in the Microsoft Customer Terms and Conditions.

12. WARRANTY:

a) Limited Warranty for Services. Contractor warrants that:

i. Services will be performed in accordance with the applicable Service Level Agreement; and

ii. All customer support for Services will be performed with professional care and skill.

b) Such Limited Warranty will be for the duration of Customer's use of the Services, subject to the notice requirements in the applicable Service Level Agreement. This Limited Warranty is subject to the following limitations:

i. any implied warranties, guarantees or conditions not able to be disclaimed as a matter of law last for one year from the start of the limited warranty;

ii. the limited warranty does not cover problems caused by accident, abuse or use in a manner inconsistent with this agreement or the Services Terms, or resulting from events beyond Contractor's reasonable control;

iii. the limited warranty does not apply to components of Software products that the Eligible State Entity may be permitted to redistribute;

iv. the limited warranty does not apply to free, trial, pre-release, or beta Services; and

v. the limited warranty does not apply to problems caused by the failure to meet minimum system requirements.

c) **Remedies for breach of limited warranty**. If Contractor fails to meet any of the above limited warranties and Customer notifies Contractor within the warranty period, then Contractor will provide the remedies identified in the Service Level Agreement for the affected Online Service. These are Customer's only remedies for breach of the limited warranty, unless other remedies are required to be provided under applicable law or as may be specifically provided in the Statement of Work or elsewhere in this Contract.

d) **DISCLAIMER OF OTHER WARRANTIES.** OTHER THAN THIS LIMITED WARRANTY, CONTRACTOR PROVIDES NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS. CONTRACTOR DISCLAIMS ANY IMPLIED REPRESENTATIONS, WARRANTIES OR CONDITIONS, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR TITLE. THESE DISCLAIMERS WILL APPLY UNLESS APPLICABLE LAW DOES NOT PERMIT THEM.

e) Contractor shall apply anti-malware controls to the Services to help avoid malicious software gaining unauthorized access to State Data, including malicious software originating from public networks. Such controls shall at all times equal or exceed the controls consistent with the industry standards for such data, but in no event less than the controls that Contractor applies to its own internal corporate electronic data of like character.

f) Unless otherwise specified in the Statement of Work:

i. The Contractor does not warrant that any Software provided hereunder is error-free or that it will run without immaterial interruption.

ii. The Contractor does not warrant and will have no responsibility for a claim to the extent that it arises directly from (A) a modification made by the State, unless such modification is approved or directed by the Contractor, (B) use of Software in combination with or on products other than as specified by the Contractor, or (C) misuse by the State.

g) All warranties, including special warranties specified elsewhere herein, shall inure to the State, its successors, assigns, customer agencies, and governmental users of the Deliverables or services.

14. SAFETY AND ACCIDENT PREVENTION (Applies to Reseller Only): In performing work under this Contract on State premises, the Contractor shall conform to any specific safety requirements contained in the Contract or as required by law or regulation. The Contractor shall take any additional precautions as the State may reasonably require for safety and accident prevention purposes. Any violation of such rules and requirements, unless promptly corrected, shall be grounds for termination of this Contract in accordance with the default provisions hereof.

15. TERMINATION FOR NON-APPROPRIATION OF FUNDS:

a) If the term of this Contract extends into fiscal years subsequent to that in which it is approved, such continuation of the Contract is contingent on the appropriation of funds for such purpose by the Legislature. If funds to effect such continued payment are not appropriated, the Contractor agrees to terminate any services supplied to the State under this Contract, and relieve the State of any further obligation therefor.

b) The State agrees that if it appears likely that subsection a) above will be invoked, the State and Contractor shall agree to take all reasonable steps to prioritize work and Deliverables and minimize the incurrence of costs prior to the expiration of funding for this Contract.

16. TERMINATION FOR THE CONVENIENCE OF THE STATE:

a) The State may terminate performance of work under this Contract for its convenience in whole or, from time to time, in part, if the California Department of Technology determines that a termination is in the State's interest. The California Department of Technology shall terminate by delivering to the Contractor a Notice of Termination specifying the extent of termination and the effective date thereof.

b) After receipt of a Notice of Termination, and except as directed by the State, the Contractor shall immediately stop work as specified in the Notice of Termination, regardless of any delay in determining or adjusting any amounts due under this clause.

c) After termination, the Contractor shall submit a final termination settlement proposal to the State in the form and with the information prescribed by the State except that in no instance shall the Contractor seek nor will the State pay for costs not specified on an order for services regardless of Contractors' liability or costs for materials, equipment, software, facilities, or sub-contracts. The Contractor shall submit the proposal promptly, but no later than 90 days after the effective date of termination, unless a different time is provided in the Statement of Work or in the Notice of Termination.

d) The Contractor and the State may agree upon the whole or any part of the amount to be paid as requested under subsection (c) above.

e) Unless otherwise set forth in the Statement of Work, if the Contractor and the State fail to agree on the amount to be paid because of the termination for convenience, the State will pay the Contractor the following amounts; provided that in no event will total payments exceed the amount payable to the Contractor if the Contract had been fully performed:

i. The Contract price for Deliverables or services accepted or retained by the State and not previously paid for;

f) The Contractor will use generally accepted accounting principles, or accounting principles otherwise agreed to in writing by the parties, and sound business practices in determining all costs claimed, agreed to, or determined under this clause.

17. TERMINATION FOR DEFAULT:

a) The State may, subject to the clause titled "Force Majeure", by written notice of default to the Contractor, terminate this Contract in whole or in part if the Contractor fails to

i. Perform the Services within the time specified in the Contract or any amendment thereto;

ii. Make progress, so that the lack of progress endangers performance of this Contract; or

iii. Perform any of the other provisions of this Contract.

b) The State's right to terminate this Contract under subsection a) above, may be exercised only if the failure constitutes a material breach of this Contract and if the Contractor does not cure such failure within the time frame stated in the State's cure notice, which in no event will be less than thirty(30) days, unless the Statement of Work calls for a different period.

c) **Intentionally left blank.**

d) Both parties, State and Contractor, upon any termination for default, have a duty to mitigate the damages suffered by it. The State shall pay Contract price for completed and accepted Deliverables.

e) The rights and remedies of the State in this clause are in addition to any other rights and remedies provided by law or under this Contract, and are subject to the clause titled "Limitation of Liability."

18. FORCE MAJEURE: Except for defaults of subcontractors at any tier, the Contractor shall not be liable for any excess costs if the failure to perform the Contract arises from causes beyond the control and without the fault or negligence of the Contractor. Examples of such causes include, but are not limited to:

a) Acts of God or of the public enemy, and

b) Acts of the federal or State government in either its sovereign or contractual capacity.

If the failure to perform is caused by the default of a subcontractor at any tier, and if the cause of the default is beyond the control of both the Contractor and subcontractor, and without the fault or negligence of either, the Contractor shall not be liable for any excess costs for failure to perform.

19. RIGHTS AND REMEDIES OF STATE FOR DEFAULT (Applies to Reseller Only):

a) In the event of the termination of the Contract, either in whole or in part, by reason of default or breach by the Contractor, any loss or damage sustained by the State in procuring any items which the Contractor agreed to supply shall be borne and paid for by the Contractor (but subject to the clause entitled “Limitation of Liability”).

b) The State reserves the right to offset the reasonable cost of all damages caused to the State against any outstanding invoices or amounts owed to the Contractor or to make a claim against the Contractor therefore.

20. LIMITATION OF LIABILITY:

a) Contractor’s liability for damages to the State for any cause whatsoever, and regardless of the form of action, whether in Contract or in tort, shall be limited to the Collective Aggregate Purchase Value which is defined as the then current sum of the amounts paid in aggregate by all State entities for all Services purchased.

b) The foregoing limitation of liability shall not apply (i) to any liability under provisions herein entitled “Compliance with Statutes and Regulations” (ii) to liability under provisions herein entitled “Patent, Copyright, and Trade Secret Indemnity” or to any other liability (including without limitation indemnification obligations) for infringement of third party intellectual property rights; (iii) to claims arising under provisions herein calling for indemnification for third party claims against the State for death, bodily injury to persons or damage to real or tangible personal property caused by the Contractor’s negligence or willful misconduct; or (iv) to costs or attorney’s fees that the State becomes entitled to recover as a prevailing party in any action.

c) The State’s liability for damages for any cause whatsoever, and regardless of the form of action, whether in Contract or in tort, shall be limited to the Collective Aggregate Purchase Value, as that term is defined in subsection a) above. Nothing herein shall be construed to waive or limit the State’s sovereign immunity or any other immunity from suit provided by law.

d) IN NO EVENT WILL EITHER THE CONTRACTOR OR THE STATE BE LIABLE FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES, EVEN IF NOTIFICATION HAS BEEN GIVEN AS TO THE POSSIBILITY OF SUCH DAMAGES, EXCEPT (I) TO THE EXTENT THAT THE CONTRACTOR’S LIABILITY FOR SUCH DAMAGES IS SPECIFICALLY SET FORTH IN THE STATEMENT OF WORK OR (II) TO THE EXTENT THAT THE CONTRACTOR’S LIABILITY FOR SUCH DAMAGES ARISES OUT OF SUB SECTION B)(I), B)(II), OR B)(IV) ABOVE.

21. INDEMNIFICATION (Applies to Reseller Only): The Contractor agrees to indemnify, defend and save harmless the State, its officers, agents and employees from any and all third party claims, costs (including without limitation reasonable attorneys’ fees), and losses due to the injury or death of any individual, or the loss or damage to any real or tangible personal property, resulting from the willful misconduct or negligent acts or omissions of the Contractor or any of its affiliates, agents, subcontractors, employees, suppliers, or laborers furnishing or supplying work, services, materials, or supplies in connection with the performance of this Contract. Such defense and payment will be conditional upon the following:

a) The State will notify the Contractor of any such claim in writing and tender the defense thereof within a reasonable time; and

b) The Contractor will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) when substantial principles of government or public law are involved, when litigation might create precedent affecting future State operations or liability, or when involvement of the State is otherwise mandated by law, the State may participate in such action at its own expense with respect to attorneys' fees and costs (but not liability); (ii) where a settlement would impose liability on the State, affect principles of California government or public law, or impact the authority of the State, the California Department of Technology will have the right to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (iii) the State will reasonably cooperate in the defense and in any related settlement negotiations.

22. INVOICES (Applies to Reseller Only): Unless otherwise specified, invoices shall be sent to the address set forth herein. Invoices shall be submitted in triplicate and shall include the Contract number; release order number (if applicable); item number; unit price, extended item price and invoice total amount. State sales tax and/or use tax shall be itemized separately and added to each invoice as applicable.

23. REQUIRED PAYMENT DATE (Applies to Reseller Only): Payment will be made in accordance with the provisions of the California Prompt Payment Act, Government Code Section 927 et. seq. Unless expressly exempted by statute, the Act requires State agencies to pay properly submitted, undisputed invoices not more than 45 days after:

a) the date of acceptance of Deliverables or performance of services; or

b) receipt of an undisputed invoice, whichever is later.

24. TAXES (APPLIES TO RESELLER ONLY): Unless otherwise required by law, the State of California is exempt from Federal excise taxes. The State will only pay for any State or local sales or use taxes on the services rendered or Goods supplied to the State pursuant to this Contract.

25. CONTRACT MODIFICATION: No amendment or variation of the terms of this Contract shall be valid unless made in writing, signed by the parties and approved as required. No oral understanding or agreement not incorporated in the Contract is binding on any of the parties.

26. CONFIDENTIALITY OF DATA: All State Data, as defined herein, made available to the Contractor in order to carry out this Contract, or which become available to the Contractor in carrying out this Contract, shall be protected by the Contractor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State. The identification of all such confidential data and information as well as the State's procedural requirements for protection of such data and information from unauthorized use and disclosure shall be provided by the State in writing to the Contractor. If the methods and procedures employed by the Contractor for the protection of the Contractor's data and information are deemed by the State to be adequate for the protection of the State's confidential information, such methods and procedures may be used, with the written consent of the State, to carry out the intent of this paragraph. The Contractor shall not be required under the provisions of this paragraph to keep confidential any data or information which is or becomes publicly available, is already rightfully in the Contractor's possession without obligation of confidentiality, is independently developed by the Contractor outside the scope of this Contract, or is rightfully obtained from third parties.

27. NEWS RELEASES: Unless otherwise exempted, news releases, endorsements, advertising, and social media content pertaining to this Contract shall not be made without prior written approval of the California Department of Technology.

28. PROTECTION OF PROPRIETARY SOFTWARE AND OTHER PROPRIETARY DATA:

a) The State agrees that all material appropriately marked or identified in writing as proprietary and furnished hereunder by the Contractor are provided for the State's exclusive use for the purposes of this Contract only. All such proprietary data shall remain the property of the Contractor. The State agrees to take all reasonable steps to ensure that such proprietary data are not disclosed to others, without prior written consent of the Contractor, subject to the California Public Records Act.

b) The State will insure, prior to disposing of any media, that any licensed materials contained thereon have been erased or otherwise destroyed.

c) The State agrees that it will take appropriate action by instruction, agreement or otherwise with its employees or other persons permitted access to proprietary data to satisfy its obligations in this Contract with respect to use, copying, modification, protection and security of proprietary materials and data, subject to the California Public Records Act.

29. PATENT, COPYRIGHT AND TRADE SECRET INDEMNITY: This section left intentionally blank.

30. DISPUTES:

For disputes involving purchases made under this Agreement, to the extent permitted by applicable law, the California Department of Technology ("CDT") shall act on behalf of the State party or entity involved with the dispute. CDT in cooperation with the State party or entity involved with the dispute shall seek to resolve the dispute with Contractor on behalf of the State party or entity. The Contractor and CDT shall deal in good faith and attempt to resolve potential disputes informally through face-to-face negotiations with persons fully authorized to resolve the dispute or through non-binding mediation utilizing a mediator agreed to by the parties, rather than through litigation. No formal proceedings for the judicial resolution of such dispute, except for the seeking of equitable relief may begin until either such persons conclude, after a good faith effort to resolve the dispute, that resolution through continued discussion is unlikely.

Notwithstanding the existence of a dispute under, related to or involving this Contract, the parties shall continue without delay to carry out all of their responsibilities, including providing of Services in accordance with the State's instructions regarding this Contract. Contractor's failure to diligently proceed in accordance with the State's instructions regarding this Contract that are not affected by the dispute shall be considered a material breach of this Contract.

31. EXAMINATION AND AUDIT (Applies to Reseller Only): The Contractor agrees that the State or its designated representative shall have the right to review and copy any records and supporting documentation directly pertaining to performance of this Contract. The Contractor agrees to maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated. The Contractor agrees to allow the auditor(s) access to such records during normal business hours and in such a manner so as to not interfere unreasonably with normal business activities and to allow interviews of any employees or others who might reasonably have information related to such records. Further, the Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Contract. The State shall provide reasonable advance written notice of such audit(s) to the Contractor.

32. PRIORITY HIRING CONSIDERATIONS (Applies to Reseller Only): If this Contract includes services in excess of $200,000, the Contractor shall give priority consideration in filling vacancies in positions funded by the Contract to qualified recipients of aid under Welfare and Institutions Code Section 11200 in accordance with PCC Section 10353.

33. COVENANT AGAINST GRATUITIES: The Contractor warrants that no gratuities (in the form of entertainment, gifts, or otherwise) were offered or given by the Contractor, or any agent or representative of the Contractor, to any officer or employee of the State with a view toward securing the Contract or securing favorable treatment with respect to any determinations concerning the performance of the Contract. For breach or violation of this warranty, the State shall have the right to terminate the Contract, either in whole or in part.

34. NONDISCRIMINATION CLAUSE:

a) During the performance of this Contract, the Contractor and its subcontractors shall not unlawfully discriminate, harass or allow harassment, against any employee or applicant for employment because of sex, sexual orientation, race, color, ancestry, religious creed, national origin, disability (including HIV and AIDS), medical condition (cancer), age, marital status, and denial of family care leave. The Contractor and subcontractors shall insure that the evaluation and treatment of their employees and applicants for employment are free from such discrimination and harassment. The Contractor and subcontractors shall comply with the provisions of the Fair Employment and Housing Act (Government Code, Section 12990 et seq.) and the applicable regulations promulgated thereunder (California Code of Regulations, Title 2, Section 7285.0 et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code Section 12990 (a-f), set forth in Chapter 5 of Division 4 of Title 2 of the California Code of Regulations are incorporated into this Contract by reference and made a part hereof as if set forth in full. The Contractor and its subcontractors shall give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other agreement.

b) The Contractor shall include the nondiscrimination and compliance provisions of this clause in all subcontracts to perform work under the Contract.

35. NATIONAL LABOR RELATIONS BOARD CERTIFICATION: The Contractor swears under penalty of perjury that no more than one final, unappealable finding of contempt of court by a federal court has been issued against the Contractor within the immediately preceding two-year period because of the Contractor's failure to comply with an order of the National Labor Relations Board. This provision is required by, and shall be construed in accordance with, PCC Section 10296.

36. ASSIGNMENT OF ANTITRUST ACTIONS: Pursuant to Government Code Sections 4552, 4553, and 4554, the following provisions are incorporated herein:

a) In submitting a bid to the State, the supplier offers and agrees that if the bid is accepted, it will assign to the State all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. 15) or under the Cartwright Act (Chapter 2, commencing with Section 16700, of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of Goods, material or other items, or services by the supplier for sale to the State pursuant to the solicitation. Such assignment shall be made and become effective at the time the State tenders final payment to the supplier.

b) If the State receives, either through judgment or settlement, a monetary recovery for a cause of action assigned under this chapter, the assignor shall be entitled to receive reimbursement for actual legal costs incurred and may, upon demand, recover from the State any portion of the recovery, including treble damages, attributable to overcharges that were paid by the assignor but were not paid by the State as part of the bid price, less the expenses incurred in obtaining that portion of the recovery.

c) Upon demand in writing by the assignor, the assignee shall, within one year from such demand, reassign the cause of action assigned under this part if the assignor has been or may have been injured by the violation of law for which the cause of action arose and

i. the assignee has not been injured thereby, or

ii. the assignee declines to file a court action for the cause of action.

37. DRUG-FREE WORKPLACE CERTIFICATION: The Contractor certifies under penalty of perjury under the laws of the State of California that the Contractor will comply with the requirements of the Drug-Free Workplace Act of 1990 (Government Code Section 8350 et seq.) and will provide a drug-free workplace by taking the following actions:

a) Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited and specifying actions to be taken against employees for violations, as required by Government Code Section 8355(a).

b) Establish a Drug-Free Awareness Program as required by Government Code Section 8355(b) to inform employees about all of the following:

i. the dangers of drug abuse in the workplace;

ii. the person's or organization's policy of maintaining a drug-free workplace;

iii. any available counseling, rehabilitation and employee assistance programs; and,

iv. penalties that may be imposed upon employees for drug abuse violations.

c) Provide, as required by Government Code Section 8355(c), that every employee who works on the proposed or resulting Contract:

i. will receive a copy of the company's drug-free policy statement; and,

ii. will agree to abide by the terms of the company's statement as a condition of employment on the Contract.

38. FOUR-DIGIT DATE COMPLIANCE: Contractor warrants that it will provide only Four-Digit Date Compliant (as defined below) Deliverables and/or services to the State. “Four Digit Date Compliant” Deliverables and services can accurately process, calculate, compare, and sequence date data, including without limitation date data arising out of or relating to leap years and changes in centuries. This warranty and representation is subject to the warranty terms and conditions of this Contract and does not limit the generality of warranty obligations set forth elsewhere herein.

39. SWEATFREE CODE OF CONDUCT:

a) Contractor declares under penalty of perjury that no equipment, materials, or supplies furnished to the State pursuant to the Contract have been produced in whole or in part by sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor, or with the benefit of sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor. The Contractor further declares under penalty of perjury that they adhere to the Sweatfree Code of Conduct as set forth on the California Department of Industrial Relations website located at www.dir.ca.gov, and Public Contract Code Section 6108.

b) The Contractor agrees to cooperate fully in providing reasonable access to its records, documents, agents or employees, or premises if reasonably required by authorized officials of the State, the Department of Industrial Relations, or the Department of Justice to determine the Contractor’s compliance with the requirements under paragraph (a)

40. RECYCLED CONTENT REQUIRMENTS: The Contractor shall certify in writing under penalty of perjury, the minimum, if not exact, percentage of post-consumer material (as defined in the Public Contract Code (PCC) Section 12200-12209), in products, materials, goods, or supplies offered or sold to the State that fall under any of the statutory categories regardless of whether the product meets the requirements of Section 12209. The certification shall be provided by the contractor, even if the product or good contains no postconsumer recycled material, and even if the postconsumer content is unknown. With respect to printer or duplication cartridges that comply with the requirements of Section

12156(e), the certification required by this subdivision shall specify that the cartridges so comply (PCC 12205 (b)(2)). A state agency contracting officer may waive the certification requirements if the percentage of postconsumer material in the products, materials, goods, or supplies can be verified in a written advertisement, including, but not limited to, a product label, a catalog, or a manufacturer or vendor Internet web site. Contractors are to use, to the maximum extent economically feasible in the performance of the contract work, recycled content products (PCC 12203(d)).

41. CHILD SUPPORT COMPLIANCE ACT: For any Contract in excess of $100,000, the Contractor acknowledges in accordance with PCC Section 7110, that:

a) The Contractor recognizes the importance of child and family support obligations and shall fully comply with all applicable State and federal laws relating to child and family support enforcement, including, but not limited to, disclosure of information and compliance with earnings assignment orders, as provided in Chapter 8 (commencing with Section 5200) of Part 5 of Division 9 of the Family Code; and

b) The Contractor, to the best of its knowledge is fully complying with the earnings assignment orders of all employees and is providing the names of all new employees to the New Hire Registry maintained by the California Employment Development Department.

42. AMERICANS WITH DISABILITIES ACT: The Contractor assures the State that the Contractor complies with the Americans with Disabilities Act of 1990 (42 U.S.C. 12101 et seq.).

43. ELECTRONIC WASTE RECYCLING ACT OF 2003: The Contractor certifies that it complies with the applicable requirements of the Electronic Waste Recycling Act of 2003, Chapter 8.5, Part 3 of Division 30, commencing with Section 42460 of the Public Resources Code. The Contractor shall maintain documentation and provide reasonable access to its records and documents that evidence compliance.

44. USE TAX COLLECTION: In accordance with PCC Section 10295.1, the Contractor certifies that it complies with the requirements of Section 7101 of the Revenue and Taxation Code. Contractor further certifies that it will immediately advise the State of any change in its retailer's seller's permit or certification of registration or applicable affiliate's seller's permit or certificate of registration as described in subdivision (a) of PCC Section 10295.1.

45. EXPATRIATE CORPORATIONS: Contractor hereby declares that it is not an expatriate corporation or subsidiary of an expatriate corporation within the meaning of PCC Sections 10286 and 10286.1, and is eligible to contract with the State.

46. DOMESTIC PARTNERS: For contracts over $100,000 executed or amended after January 1, 2007, the Contractor certifies that the Contractor is in compliance with Public Contract Code Section 10295.3.

47. SMALL BUSINESS PARTICIPATION AND DVBE PARTICIPATION REPORTING REQUIREMENTS:

a) If for this Contract the Contractor made a commitment to achieve small business participation, then the Contractor must within 60 days of receiving final payment under this Contract (or within such other time period as may be specified elsewhere in this Contract) report to the awarding department the actual percentage of small business participation that was achieved. (Govt. Code § 14841.)

b) If for this Contract the Contractor made a commitment to achieve disabled veteran business enterprise (DVBE) participation, then Contractor must within 60 days of receiving final payment under this Contract (or within such other time period as may be specified elsewhere in this Contract) certify in a report to the awarding department: (1) the total amount the prime Contractor received under the Contract; (2) the name and address of the DVBE(s) that participated in the performance of the Contract; (3) the amount each DVBE received from the prime Contractor; (4) that all payments under the Contract have been made to the DVBE; and (5) the actual percentage of DVBE participation that was achieved. A person or entity that knowingly provides false information shall be subject to a civil penalty for each violation. (Mil. & Vets. Code § 999.5(d); Govt. Code § 14841.)

48. LOSS LEADER: It is unlawful for any person engaged in business within this state to sell or use any article or product as a “loss leader” as defined in Section 17030 of the Business and Professions Code. (PCC 12104.5(b).).

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Exhibit 2
Negotiated Special Provisions

These Negotiated Special Provisions shall apply to CDT' (and its User Agencies') use of Permitted Services, and are hereby added to the Government Contract (as defined in Exhibit 4, below). The Negotiated Special Provisions shall supersede the original document titled **"Reseller Enabled Cloud Computing Special Provisions – Infrastructure as a Service and Platform as a Service,"** referenced in the Solicitation.

Except for those provisions in this Exhibit 2 which are marked to be applicable only to the Reseller (which is the Contractor hereunder), Microsoft has accepted flow-down of these Negotiated Special Provisions in its separate contract with Contractor.

I. THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR INFRASTRUCTURE AS A SERVICE (IAAS) AND PLATFORM AS A SERVICE (PAAS), AS DEFINED BELOW. THESE SPECIAL PROVISIONS ARE TO BE ATTACHED TO THE RESELLER ENABLED GENERAL PROVISIONS -- CLOUD COMPUTING (THE "GENERAL PROVISIONS") AND ACCOMPANIED BY, AT MINIMUM, A STATEMENT OF WORK (SOW) AND SERVICE LEVEL AGREEMENT (SLA).

II. STATE AGENCIES MUST FIRST:

a) **CLASSIFY THEIR DATA PURSUANT TO THE CALIFORNIA STATE ADMINISTRATIVE MANUAL (SAM) 5305.5;**

b) **CONSIDER THE FACTORS TO BE TAKEN INTO ACCOUNT WHEN SELECTING A PARTICULAR TECHNOLOGICAL APPROACH, IN ACCORDANCE WITH SAM 4981.1, 4983 AND 4983.1 AND THEN;**

c) **MODIFY THESE SPECIAL PROVISIONS THROUGH THE SOW AND/OR SLA TO MEET THE NEEDS OF EACH ACQUISITION.**

1. DEFINITIONS:

a) "Authorized Persons" means the Service Provider's employees, contractors, subcontractors or other agents who need to access the State's Data to enable the Service Provider to perform the services required.

b) "Data Breach" means any unlawful access, use, theft or destruction to any Customer Data stored on the Cloud Service Provider's equipment or facilities, or unauthorized access to such equipment or facilities that results in the use, disclosure, destruction, alteration, loss or theft of State Data.

c) "Infrastructure-as-a-Service" (IaaS) means commercial services offered for sale to the State and are defined by the National Institute of Standards and Technology (NIST) Special Publication 800-145 or its successors as, "The capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components (e.g., host firewalls)."

d) "Platform-as-a-Service" (PaaS) means commercial services offered for sale to the State and are defined by the National Institute of Standards and Technology (NIST) Special Publication

800-145 or its successors as, “The capability provided to the consumer to deploy onto the cloud infrastructure consumer- created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.”

e) “Security Incident” is synonymous with Data Breach. For clarity, Microsoft’s OST and other material refers exclusively to Security Incident, as Microsoft does not distinguish between Data Breach and Security Incident, and do not report potential events (only confirmed ones).

f) “Service Level Agreement” (SLA) means a written agreement between both the State and the Service Provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, and (4) any remedies for performance failures.

g) “Service Provider” means the Contractor, subcontractors, agents, resellers, third parties and affiliates who may provide the services agreed to under the Contract.

h) “State Data” means all data submitted to, processed by, or stored in the Service Provider’s Services under this contract and includes but is not limited to all data that originated with the State, all data provided by the State or its Users, and data generated, manipulated, produced, reported by or otherwise emanating from or by applications run by the State on the Services. For clarity, State Data is synonymous with “Customer Data”, as that term is used in various provisions of the Microsoft Customer Terms and Conditions incorporated into the Contract and includes the following:

i. “Non-Public Data” means data submitted to the Service Provider’s IaaS or PaaS Service, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that may be exempt by statute, regulation or policy from access by the general public as public information.

ii. “Personal Data” means data submitted to the Service Provider’s IaaS or PaaS Service that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver’s license, passport); financial account information, including account number, credit or debit card numbers; Education Records; Employment Records; or protected health information (PHI) relating to a person.

a. “Education Records” covered by the Family Educational Rights and Privacy Act (FERPA) as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

b. “Employment Records” held by a covered entity in its role as employer.

c. “Protected Health Information” (PHI) means Individually Identifiable Health Information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes Education Records and Employment Records.

1) “Individually Identifiable Health Information” means Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan,

employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

i. “Public Data” means all other data not specifically mentioned above.

i) “State Identified Contact” means the person or persons designated in writing by the State to receive Security Incident or Data Breach notification. For purposes of this Contract, State Identified Contacts shall be individuals that are registered by the State as administrators in the Microsoft Azure administrative portal. For clarity, if more than one administrator is identified by the State, Microsoft may only contact one of them.

j) “Statement of Work” (SOW) means the requirements contained in the contract, including but not limited to (a) the Microsoft Customer Terms and Conditions and (b) the mutually accepted technical requirements, for cloud computing services, including Infrastructure as a Service and Platform as a Service but not Software as a Service, offered to the State by the Contractor herein.

2. DATA OWNERSHIP:

The State will own all right, title and interest in all State Data. The Service Provider shall not access State user accounts or State Data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Contract, (4) at the State’s written request or (5) as required by law.

3. DATA PROTECTION:

Duty of Integrity: Provider will ensure the integrity of all State Data at all times by preventing unauthorized destruction or corruption.

Duty of Protection: Service Provider will ensure there is no inappropriate or unauthorized access to or use of State Data at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity and availability of State Data within its control and comply with the following conditions:

a) In addition to the Compliance with Statues and Regulations provisions set forth in the General Provisions, the Service Provider shall comply as required with:

   i. The California Information Practices Act (Civil Code Sections 1798 et seq).
   ii. NIST Special Publication 800-53 Revision 4 or its successor.
   iii. Privacy provisions of the Federal Privacy Act of 1974.

b) All State Data obtained by the Service Provider within its control in the performance of this Contract shall become and remain the property of the State.

c) Unless otherwise set forth in the SOW and/or SLA, Service Provider shall enable the State to encrypt Personal Data and Non-Public Data at rest, in use, and in transit with controlled access. The SOW and/or SLA will specify which party is responsible for encryption and access control of the State Data for the service model under Contract. If the SOW and/or SLA and the Contract are silent, then the State is responsible for encryption and access control.

d) Unless otherwise set forth in the SOW and/or SLA, it is the State’s responsibility to identify data it deems as Non-Public Data to the Service Provider. The level of protection and encryption for all Non-Public Data shall be identified and made a part of this Contract.

e) At no time shall any Personal Data and Non-Public Data or processes — which either belong to or are intended for the use of State or its officers, agents or employees — be copied, disclosed or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction without the express written consent of the State except as permitted in Section 2 above or in the Microsoft Customer Terms and Conditions.

f) **(For PaaS Only)** Encryption of Data at Rest: The Service Provider shall make available storage encryption consistent with validated cryptography standards in accordance with applicable FIPS 140-2 (or its successor) standards as referenced in FedRAMP.

4. DATA LOCATION:

The Service Provider shall provide its services to the State and its end users solely from data centers in the continental United States. Storage of State Data at rest shall be located solely in data centers in the continental United States. The Service Provider shall not allow its personnel or contractors to store State Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Service Provider shall permit its personnel and contractors to access State Data remotely only as required to provide technical user support or other customer support. The Service Provider may provide technical user support or other customer support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this Contract.

5. SECURITY INCIDENT OR DATA BREACH NOTIFICATION:

Subject to the requirement to register administrator contact information, as set forth in the following paragraph, if Microsoft becomes aware of a Security Incident (which, for the purposes of this Contract, shall be synonymous with Data Breach, as defined above), Microsoft will as soon as possible and no later than five (5) business days after Microsoft determines that a Security Incident has occurred (1) notify one or more State Identified Contacts of the Security Incident; (2) investigate the Security Incident and provide the State 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. Microsoft and Contractor shall reasonably cooperate fully with the State, its agents and law enforcement in accordance with Microsoft's security policies.

Notification(s) of Security Incidents will be delivered to one or more of the State's administrators (see definition of State Identified Contact, above) by any means Microsoft selects, including via email. It is the State's sole responsibility to ensure its administrators maintain accurate contact information on the Azure Government service 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.

The State must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

Incident Response Process:

- Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.
- Microsoft tracks, or enables Eligible State Entities to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.
- Service Monitoring: Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.

6. DATA BREACH RESPONSIBILITIES: RESERVED

7. NOTIFICATION OF LEGAL REQUESTS:

Microsoft will not disclose State Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as the State directs, (2) as described in the Microsoft Customer Terms and Conditions, or (3) as required by law. Microsoft will not disclose State Data to law enforcement unless required by law. Should law enforcement contact Microsoft with a demand for State Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from the State. If compelled to disclose State Data to law enforcement, then Microsoft will promptly notify the State (or Contractor on the State's behalf) and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third party request for State Data (such as requests from the State's End Users), Microsoft will promptly notify the State (or Contractor) unless prohibited by law. If Microsoft is not required by law to disclose the State Data, Microsoft will reject the request. If the request is valid and Microsoft could be compelled to disclose the requested information, Microsoft will attempt to redirect the third party to request the State Data from the State. Except as the State directs, Microsoft will not provide any third party: (1) direct, indirect, blanket or unfettered access to State Data; (2) the platform encryption keys used to secure State Data or the ability to break such encryption; or (3) any kind of access to State Data if Microsoft is aware that such data is used for purposes other than those stated in the request.

In support of the above, Microsoft may provide the State (and/or Contractor's) basic contact information to the third party.

8. DATA PRESERVATION AND RETRIEVAL:

For ninety (90) days following the expiration date (or early termination date) of this Contract ("Retention Period"), or upon notice of termination of this Contract, Service Provider shall provide the State self-service access to Customer Data.

Upon request by the State at least 30 days prior to expiration, and in the event that the State does not choose to renew the Contract and subscription for a longer term as provided in the Contract, Service Provider will make arrangements for the State (or its Prime Contractor, if applicable) to extend its Contract and paid subscription for the PaaS and IaaS services, for a 90-day period, during which the services will retain their normal functionality.

During any Retention Period, and any period of service suspension, the Service Provider shall not take any action to intentionally erase any Customer Data, and Customer Data access shall continue to be made available to the State without alteration.

9. BACKGROUND CHECKS:

The Service Provider shall conduct criminal background checks on its Authorized Persons and not provide access to State Data to any persons who fail such background checks, in accordance with the requirements of FedRAMP (High Specification) and any US Federal Government regulation that Service Provider's IaaS and PaaS services are subject to.. Additionally, the Service Provider shall allow the California Department of Justice (CADOJ) in CADOJ's capacity as CJIS Systems Agency, to perform in-state background checks of Authorized Persons, in accordance with FBI CJIS Policy and CLETS. Service Provider will not permit access to Customer Data by individuals who fail such background checks. The Service Provider shall promote and maintain an awareness of the importance of securing State Data among the Service Provider's employees and agents.

10. ACCESS TO SECURITY LOGS AND REPORTS:

Service Provider shall allow the State reasonable self-service access to security logs, information, latency statistics, data, and other related security data that affect this Contract and Customer Data, at no cost to the State. The parties recognize that the type of self-service access and security data made available to the State may be subject to change.

11. CONTRACT AUDIT (APPLIES TO RESELLER ONLY):

The Service Provider shall allow the State to audit conformance to the Contract terms. The State may perform this audit or Contract with a third party at its discretion and at the State's expense.

12. DATA CENTER AUDIT:

As of the date of the proposal, Microsoft has achieved FedRAMP High ATO for Azure Government Services as set forth at the Microsoft Trust Center Compliance page for Microsoft

Trust Center Compliance page for FedRAMP at https://www.microsoft.com/enus/trustcenter/compliance/fedramp. Microsoft anticipates commencement of the process for annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audits of its data centers, or the applicable successor to such SSAE standard. While SSAE 16 audits are not currently performed, Microsoft will be able to demonstrate to the State a mapping of the FedRAMP control standards with their corresponding SSAE 16 standards, in order to demonstrate compliance with the intent of this requirement. All such audits will be at Microsoft's own expense. The Service Provider shall provide a redacted version of the audit report and Service Provider's plan to correct any negative findings upon request after receipt of a signed confidential nondisclosure agreement from the State. The Service Provider may remove its proprietary information from the redacted version.

13. CHANGE CONTROL AND ADVANCE NOTICE: INTENTIONALLY LEFT BLANK.

14. SECURITY PROCESSES:

The Service Provider shall disclose its non-proprietary security processes to the State such that adequate protection and flexibility can be attained between the State and the Service Provider. The State and the Service Provider shall understand each other's roles and responsibilities, which shall be set forth in the SOW and/or SLA.

15. IMPORT AND EXPORT OF DATA:

During the term of a subscription or any Retention Period, the State shall have the ability to import or export data in whole or in part at its discretion without interference from the Service Provider.

16. RESPONSIBILITIES AND UPTIME GUARANTEE:

The Service Provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment are the responsibility of the Service Provider. Unless otherwise agreed in a Statement of Work or SLA, the system shall be available 24/7/365 (except for scheduled maintenance downtime),and shall provide service to customers as defined in the SOW and/or SLA.

17. RIGHT TO REMOVE INDIVIDUALS:

The State shall have the right at any time to require the Service Provider remove from interaction with State any Service Provider representative who the State believes is detrimental to its working relationship with the Service Provider. The State shall provide the Service Provider with notice of its determination, and the reasons it requests the removal. The Service Provider shall not assign the person to any aspect of the Contract or future work orders without the State's consent.

18. RESERVED

19. RESERVED

Exhibit 3
Other Solicitation Flow Down Terms

As used in this Exhibit 3, **"Solicitation"** means the State of California's competitive procurement identified by Event ID 0000003775 (specifically, Addendum 9 thereof), titled "Platform as a Service and Infrastructure as a Service CLOUD SERVICES."

These Other Solicitation Flow Down Terms shall apply to CDT' (and its User Agencies') use of Permitted Services, and are hereby added to the Government Contract (as defined in Exhibit 4, below). Each provision shown below (a) is numbered in accordance with the boilerplate Solicitation section number to which it corresponds (and, where applicable, amends).
In accordance with Solicitation Section 2, "Contractor Responsibility," Contractor represents that it is a Reseller and is authorized by the Cloud Service Provider, Microsoft (as of the effective date of the Government Contract) to resell the Permitted Products to CDT hereunder, for use by User Agencies for which CDT is contractually responsible.

Microsoft does not accept either (a) provisions below marked as applicable only to the Reseller; or (b) terms and conditions of the Solicitation not expressly contained in the Exhibits and Amendments (including but not limited to this Exhibit 3) of the Microsoft Terms and Conditions.
CDT agrees that (except where Microsoft has expressly accepted flow down of a provision in its separate agreement with Reseller), it accepts the terms and conditions of this Exhibit 3, including but not limited to the agreement to substitute the revised final wording of each provision shown below in the column titled "Final language of each applicable provisions," in lieu of the original wording of the same-numbered section in the boilerplate Solicitation, in accordance with the applicable statements in the column titled "Statement of Amendment or Acceptance."

Contractor's representation of Microsoft's acceptance of flow down of certain provisions (with or without revisions), in Microsoft's separate agreement with Reseller (Contractor), is indicated (as applicable) below in the column titled "Statement of Amendment or Acceptance."

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
7	III.A.4	**III. CONFIDENTIALITY (M)(E)** **IV. THE CONTRACTOR, AND ITS CSP IF ANY, ENGAGING IN IT SERVICES TO THE STATE PERTAINING TO THIS PROJECT AND REQUIRING CONTACT WITH CONFIDENTIAL STATE INFORMATION, WILL BE REQUIRED TO EXERCISE SECURITY PRECAUTIONS FOR SUCH DATA THAT IS MADE AVAILABLE AND MUST ACCEPT FULL LEGAL RESPONSIBILITY FOR THE PROTECTION OF THIS CONFIDENTIAL INFORMATION. THIS INCLUDES FINANCIAL, STATISTICAL, PERSONAL, TECHNICAL AND ALL OTHER TYPES OF DATA AND INFORMATION**	**In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
		RELATING TO OPERATIONS OF ANY STATE OR LOCAL AGENCY, WHETHER EXPRESSLY MADE AVAILABLE TO THE CONTRACTORS OR ENCOUNTERED COINCIDENT TO PROGRAMMING WORK OR TESTING. **V. UNDER NO CIRCUMSTANCES SHALL THE CONTRACTOR OR ITS CSP, IF ANY, USE OR PUBLISH, SELL, OR OTHERWISE DISCLOSE TO ANY THIRD PARTY THE CONTENTS OF ANY RECORDS OR DATA, OR REPORTS DERIVED FROM DATA, SUBMITTED FOR PROCESSING WITHOUT THE AUTHORIZATION AND CONSENT OF THE STATE IN WRITING.**	
9	III.A.7	**VI. FEDERAL DEBARMENT (M) (E)** **VII. EXPENDITURES FROM THIS CONTRACT MAY INVOLVE FEDERAL FUNDS. THE FEDERAL DEPARTMENT OF LABOR REQUIRES ALL STATE AGENCIES WHICH ARE EXPENDING FEDERAL FUNDS HAVE IN THE CONTRACT FILE A CERTIFICATION BY THE CONTRACTOR THAT THEY HAVE NOT BEEN DEBARRED NOR SUSPENDED FROM DOING BUSINESS WITH THE FEDERAL GOVERNMENT. RESPONDENTS MUST COMPLETE AND SUBMIT THE EXHIBIT B, FEDERAL DEBARMENT CERTIFICATION FORM WITH THE RESPONSE SUBMITTAL.**	**Microsoft represents it has not been debarred nor suspended from doing business with the Federal Government.** **In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**
9	III.A.9	**VIII. <ENTIRE SECTION TITLED "CALIFORNIA CIVIL RIGHTS LAWS">**	**Microsoft represents it complies with this provision.** **In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**
9	III.A.10	**IX. SUBCONTRACTORS.** **X. A RESPONDENT RESELLING A CSP'S SERVICES IS NOT CONSIDERED A SUBCONTRACTOR. IN THIS SITUATION, THE RESELLER WOULD BE THE CONTRACTOR**	• **In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
		OF THE CSP'S SERVICES.	
12	IV.B.1	**Application Programming Interfaces** The Contractor's IaaS and PaaS must provide open Application Programming Interfaces (API) that, subject to Cloud Service Provider's published instructions and requirements, provide the capability to: a. Migrate workloads between the public cloud and the State's private on-premise cloud where CDT acts as the broker of those services and has the ability to logically separate individual customers; b. Define networks, resources and templates within a multi-tenant environment with the use of available APIs; c. Provision and de-provision virtual machines and storage within a multi-tenant environment; d. Add, remove and modify computing resources for virtual machines within a multi-tenant environment; e. Add, remove and modify object and block storage within a multi-tenant environment; f. Retrieve financial and billing information that provides detailed information for each CDT customer subscriber; g. Retrieve performance indicators for all workloads in the multi-tenant environment; h. Retain all workloads within the U.S.; i. Retrieve log data from all workloads; and j. Provide the ability to model potential workloads to determine cost of services.	- **In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**
12	IV.B.2	**Environment** Subject to Cloud Service Provider's published instructions and requirements, the Contractor's cloud environment must have the ability to: a. Provide a multi-tenant environment that supports a parent/child administrative relationship that enables the CDT (parent) to programmatically apply compliance and regulatory requirements and standards down to the child (CDT customers) entities; b. Provide FIPS 140-2 complaint cryptographic modules – http://csrc.nist.gov/groups/STM/cmvp/standards.html;	- **In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
		c. Support cost tracking by resource tags or other solutions to tracking costs for individual customers; d. Run and manage web applications, including .NET environments; e. Provide managed database services with support for multiple database platforms; f. Support Security Access Markup Language (SAML) federation; g. Provide integration with a customer's on-premises Active Directory; h. Provide a managed service to create and control encryption keys used to encrypt data; i. Provide a dedicated Hardware Security Module (HSM) appliance for encryption key management; j. Provide a managed service to provision, manage, deploy and revoke SSL/TLS certificates; k. Provide services to migrate workloads to and from the State's VMware and HyperV environments; and l. Provide dashboard reporting that provides performance monitoring, usage and billing information.	
12	IV.B.3	**XI. CATALOG** **XII. THE CONTRACTOR SHALL PROVIDE THE WITH A CATALOG OF AUTHORIZED SERVICES.**	**In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**
12	IV.B.4	**XIII. AMERICANS WITH DISABILITIES ACT** **XIV. THE CONTRACTOR SHALL SUPPORT 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. CONTRACTOR SHALL PROVIDE A URL WHERE ITS VOLUNTARY PRODUCT ACCESSIBILITY TEMPLATES ("VPATS") FOR ITS TECHNOLOGIES USED IN PROVIDING THE PAAS AND IAAS SERVICES.**	**In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
13	IV.B.5	**XV. CATALOG WEBSITE** **XVI. THE CONTRACTOR (AND/OR THE CLOUD SERVICE PROVIDER) SHALL MAINTAIN AN ONLINE CATALOG OR WEBSITE LISTING AVAILABLE IAAS AND PAAS SERVICES MEETING THE MINIMUM REQUIREMENTS OF SECTION IV B, REQUIREMENTS. SLAS WILL BE POSTED TO CONTRACTOR'S (AND/OR THE CLOUD SERVICE PROVIDER'S) WEBSITE, ALTHOUGH NOT NECESSARILY ON THE CATALOG WEBSITE.** **XVII. A. THE CATALOG WEBSITE SHALL CONTAIN:** **XVIII. (1) DETAILED DESCRIPTIONS OF AVAILABLE PAAS AND IAAS CLOUD SERVICES OFFERINGS; AND** **XIX. (2) STATE SPECIFIC CONTRACT PRICING OR PUBLIC PRICING ON WHICH THE STATE DISCOUNT IS BASED.** **XX.B. THE CONTRACTOR SHALL PROVIDE THE STATE THE ABILITY TO RECEIVE CATALOG SERVICES UPDATES THAT IMPACT CUSTOMER SERVICES:**	**In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation. Please see Exhibit 4, Section 1.c, for information about the applicable SLA.**
13	IV.B.6	**Contract termination.** a. Suspension of services: During any period of suspension or contract negotiation or disputes, the Service Provider shall not take any action to intentionally erase any State of California data. b. Termination of any services or agreement in entirety: In the event of termination of any services or agreement in entirety, the Service Provider shall not take any action to intentionally erase any State of California data for a period of 90 days after the effective date of the termination. After such 90 day period, the Service Provider shall have no	**In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
		obligation to maintain or provide any State of California data. Within this 90 day timeframe, vendor will continue to secure and back up State of California data covered under the contract. c. Deleted, section number reserved. d. Post-Termination Assistance: The State of California shall be entitled to any post-termination assistance generally made available with respect to the Services.	
14	IV.B.7	Security a. FedRAMP Services being offered shall possess FedRAMP authorization of High. The Contractor shall maintain such authorization level through the life of the contract. The Contractor shall notify the State CA of lapse in maintaining FedRAMP High Authorization to Operate (ATO). Failure to obtain FedRAMP High ATO with 30 days may result in a cancellation of the contract. b. Threat Information The Respondent shall provide vulnerability and threat information to the State containing a list of events and the sources thereof for the State's tenant servers. The event data must include information as to what services were accessed and what action was performed, as well as who accessed the service. Unauthorized login attempt information must also be available. c. Deleted – section number reserved. d. Security Reports The Contractor shall allow the State access to system security information that affect this contract, its data, and/or processes. This includes the ability for the State to request a report of the records that a specific user accessed over a specified period of time. e. Discovery Contractor will not disclose Customer Data outside of Contractor or its controlled subsidiaries and affiliates except (1) as the State directs, (2) as described in the Service Provider Terms, or (4) as required by law. Contractor will not disclose Customer Data to law enforcement unless required by law. Should law enforcement contact Contractor with a demand for Customer Data, Contractor	**In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
		will attempt to redirect the law enforcement agency to request that data directly from the State. If compelled to disclose Customer Data to law enforcement, then Contractor will promptly notify the State (or its Prime Contractor, if applicable) and provide a copy of the demand unless legally prohibited from doing so. Upon receipt of any other third party request for Customer Data (such as requests from the State's end users), Contractor will promptly notify the State (or its Prime Contractor, if applicable) unless prohibited by law. If Contractor is not required by law to disclose the Customer Data, Contractor will reject the request. If the request is valid and Contractor could be compelled to disclose the requested information, Contractor will attempt to redirect the third party to request the Customer Data from the State. Except as the State directs, Contractor will not provide any third party: (1) direct, indirect, blanket or unfettered access to Customer Data; (2) the platform encryption keys used to secure Customer Data or the ability to break such encryption; or (3) any kind of access to Customer Data if Contractor is aware that such data is used for purposes other than those stated in the request. In support of the above, Contractor may provide the State's (and/or its Prime Contractor's) basic contact information to the third party. f. Employees The Service Provider shall conduct criminal background checks on its Authorized Persons, and not provide access to State Data to any persons who fail such background checks, in accordance with the requirements of FedRAMP (High specification) and any US Federal Government regulation that Service Provider's IaaS and PaaS services are subject to. Additionally, the Service Provider shall allow the California Department of Justice (CADOJ), in CADOJ's capacity as CJIS Systems Agency, to perform in-state background checks of Authorized Persons, in	

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
		accordance with FBI CJIS Policy and CLETS. Service Provider will not permit access to Customer Data by individuals who fail such background checks. The Service Provider shall promote and maintain an awareness of the importance of securing State Data among the Service Provider's employees and agents.	
		g. Penetration Testing The Contractor shall allow the State to conduct penetration testing of the State's applications hosted in the PaaS and IaaS Contractor's environment within seven (7) business days of notification by the State. Because such testing can be indistinguishable from a real attack, the State agrees to conduct such penetration testing only after obtaining approval in advance from Contractor, which such approval will not be reasonably withheld.	
		h. Deleted – section number reserved	
		i. Data Centers The Contractor's proposed data centers must be within the continental United States.	
		j. Alternate Data Centers The Contractor's alternate data center locations must be within the continental United States.	
		k. Disaster Recovery (NR) The Contractor shall submit disaster recovery and potential mitigation strategies with their response.	
		l. All data must remain within the data center(s) designated by the customer.	
		m. For Government Community Cloud Services, access to Customer Content by Microsoft personnel who reside outside the United States, including access to Customer Content by authorized support staff in identified support centers, is prohibited except in very limited circumstances permitted by written Microsoft asset handling and access standards in accordance with applicable compliance programs, unless approved in advance by the State Chief Information Security Officer. Any such access permitted under the foregoing	

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
		Microsoft standards shall occur only after commercially reasonable efforts have been made by Microsoft to perform the function necessitating Customer Content access with employees who reside within the United States. (e.g. vacation or other specialist staff absence coverage). In cases when it occurs, all Customer Content access granted shall provide the minimum access necessary, for the minimum time necessary, to Microsoft personnel who reside outside the United States.	
15	IB.B.8	**Data Ownership** The State of California shall own all right, title and interest in its data that is related to the services provided by this contract. The Service Provider shall not access State of California User accounts, or State of California Customer Data, except: a. in the course of data center operations, b. in response to service or technical issues, c. as required by the express terms of this contract, or d. at State of California's written request. Respondent will restrict access to Customer data to only Respondent's personnel who require such access to perform their job function and will maintain a record of personnel authorized to access Respondent's systems that contain Customer Data. Respondent's IaaS and PaaS services shall use Customer Data that the State provides through its use of the IaaS and PaaS services only to provide and maintain those services for the customer. Respondent's IaaS and PaaS services shall not capture, maintain, scan, index, share or use customer data stored or transmitted by the service, or otherwise use any data-mining technology, for any non-authorized activity or non-government purpose. Respondent's IaaS and PaaS services shall not use customer data stored or transmitted by those services for any advertising or other commercial purpose of Respondent or any third party. Respondent's IaaS and PaaS services will be logically separate from its consumer online services. Customer Data in the IaaS and PaaS services, data in Respondent's consumer online services, and data created by or resulting from Respondent's scanning, indexing, or data-mining	**In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
		activities, will not be commingled unless expressly approved by the State in advance.	
15	IV.B.9	**Service Refresh** The State expects to update the services periodically as technology changes. The Contractor shall: a. Offer services during product refreshes that meet the minimum specifications of this solicitation b. Maintain discounts at the levels set forth in the contract. c. Make information available to the State CA, with as much advance notice as practicable, regarding changes in technology, and upon request will make recommendations for service updates. The State CA will review the substitute services and determine contract acceptability d. Deleted – section number reserved. If no substitute service is available that meets or exceeds the solicitation specifications due to fundamental technology or market change, the State may alter the minimum specifications to meet the updated standards. Obsolescence of a service may be determined at discretion of the State, and the State may cease its use of any service or service feature it deems to be obsolete. This is the State's only remedy for Microsoft's termination of a Service or feature.	**In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**
16	IV.B.10	**Service Level Agreement** The respondent shall submit one or more SLAs that cover those services proposed under this solicitation. The requirements and any terms and conditions of this solicitation take precedence over any SLA(s) provided by the Respondent. a. Deleted – section number reserved. b. The SLA for all services offered shall state the guaranteed availability percentage, applicable within a single physical data center, to each such available service's SLA. c. Deleted – section number reserved.	- **In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**
16	IV.C.1.c	**Conformance** The Contractor shall allow the CDT or its designated third party auditor to:	**In its separate agreement with Reseller, Microsoft has accepted flow down of this provision of the Solicitation.**

Solicitation Page(s)	Solicitation Section #	Final language of each applicable provision	Statement of Amendment or Acceptance
		(i) Audit the Reseller's conformance including but not limited to Reseller's contract terms, pricing, costing, ordering, invoicing, and reporting. Such audits shall not cover terms and conditions which pertaining to the Service Provider's design, operation, security, delivery, and operation of the IaaS and PaaS Services. Such audits shall be conducted with at least 30 days advance written notice and shall not unreasonably interfere with the Reseller's business. (ii) Review the findings of Microsoft's 3rd party auditors (including but not limited to the applicable FedRAMP audit findings), subject to a mutually-agreed non-disclosure agreement between the State and Microsoft.	

Exhibit 4
Additional Microsoft - CDT Terms

These Additional Microsoft - CDT Terms shall apply to CDT' (and its User Agencies') use of Permitted Services, and are hereby added to the Government Contract (as defined in this Exhibit 4, below).

In these Microsoft Customer Terms and Conditions, the following definitions apply:
"Affiliate" means

a) **with regard to the State, any User Agency** (as defined in the Government Contract). For clarity (and to conform with defined terms used in other parts of the Government Contract), the term "User Agency" has been substituted for "Affiliate" below, when adapting Microsoft's otherwise-written provisions for use in these Microsoft Customer Terms and Conditions. To whatever extent the applicable Use Rights use the term "Affiliate" in a context clearly applicable to a User Agency's use of Azure Government Services acquired hereunder, such word shall (for purposes of the Government Contract) be deemed synonymous with "User Agency"; and

b) with regard to Microsoft or Contractor, any legal entity that such party owns, or is owned by that party, or that is under common ownership with that party. "Ownership" means, for purposes of this definition, control of more than a 50% interest in an entity.

"Allocated Annual Commitment" means the portion of the Monetary Commitment allocated annually through the term of each Enrollment submitted separately by Reseller to Microsoft in support of the Government Contract.

"Azure Government Services" means, collectively, the Microsoft Azure branded IaaS and PaaS Services (as those terms are defined in the Government Contract), or features thereof, Microsoft makes available to Reseller for resale to the State under the Government Contract, each identified as available "Azure Government" at http://azure.microsoft.com/en-us/regions/#services. For clarity, the State will not purchase Azure Government Services from datacenter regions marked on the aforementioned URL as "DOD" (which apply solely to the US Department of Defense).

"Community" means the community consisting of one or more of the following: (1) a Government, (2) a company using eligible Government Community Cloud Services to provide solutions to a Government or a qualified member of the Community, or (3) a company with State Data that is subject to Government regulations for which the company determines and Microsoft agrees that the use of Government Community Cloud Services is appropriate to meet the company's regulatory requirements. Membership in the Community is ultimately at Microsoft's discretion, which may vary by Government Community Cloud Service. For clarity, all User Agencies are Governments and thereby qualify as members of the Community.

"Consumable Services" means those Azure Government Services that are (a) not Microsoft Azure Services Plans; and (b) are either billed in arrears or decremented from Monetary Commitment, at Consumption Rates, as applicable.

"Consumption Allowance" is, as measured separately for each Enrollment, equal to fifty percent of the Allocated Annual Commitment. For example, for an Enrollment with an Allocated Annual Commitment of $100,000, the Consumption Allowance for that year would be $50,000.

"Consumption Rates" means, as established separately for each Enrollment, the prices for Microsoft Azure Government Services or, for certain Microsoft Azure Government Service Plans, any usage in excess of a specified quantity. Consumption Rates may also be referred to as "Overage Rates" or "Overage" in other Microsoft or Microsoft Azure documents.

"Contractor" means the Reseller that has entered into the Government Contract with Customer. For clarity, Contractor is referred to as "Government Partner" in the Enterprise Agreement for Government Partners between Microsoft and Contractor, in which an exhibit containing the text of these Microsoft Customer Terms and Conditions is attached.

"Customer" means CDT, which has entered into the Government Contract with Contractor for the purchase of Azure Government Services, and into whose Government Contract these Microsoft Customer Terms and Conditions are incorporated. For clarity:

a) the terms "CDT" and "the State" are generally used in lieu of "Customer," below in these Microsoft Customer Terms and Conditions; and
b) to the extent that Microsoft uses the term "Customer" on its web pages and in other customer materials, and which apply expressly to the State's use of Azure Government Services, the term "Customer" will be synonymous with "the State," as defined below.

"Customer Data," means State Data, as defined in the Government Contract. For clarity

a) The term "State Data" is generally used in lieu of "Customer Data," below in these Microsoft Customer Terms and Conditions; and
b) To the extent that Microsoft uses the term "Customer Data" on its web pages and in other customer materials which apply expressly to the State's use of Azure Government Services, the term "Customer Data" shall be interpreted to mean "State Data" as defined in the General Provisions and Special Provisions.

"CDT" means the California Department of Technology.

"Enrollment" means the document that Contractor submits to Microsoft to place orders and be invoiced for each Enterprise's Azure Government Services.

"Enterprise" means, for each Enrollment, the User Agency (or group of User Agencies):

a) that CDT instructs Contractor to identify on that Enrollment; and
b) whose use of Azure Government Services acquired under the Government Contract requires separate State administrators (apart from administrators for other Enterprises established pursuant to other Enrollments).

For clarity, the State must instruct Reseller to establish a unique Enrollment (and thereby establish a unique Enterprise) whenever separate administration is required, in accordance with Microsoft's public user documentation.

"Fixes" means fixes, modifications or enhancements, or their derivatives, that Microsoft either releases generally (such as service packs) or provides to the Enterprise for the Azure Government Services.

"Federal Agency" means a bureau, office, agency, department or other entity of the United States Government.

"Government" means a Federal Agency, State/Local Entity, or Tribal Entity acting in its governmental capacity.

"Government Community Cloud Services" means Microsoft Online Services (including but not limited to Azure Government Services) that are provisioned in Microsoft's multi-tenant data centers for exclusive use by or for the Community and offered in accordance with the National Institute of Standards and Technology ("NIST") Special Publication 800-145. For clarity:

a) Azure Government Services constitute one of several varieties of Government Community Cloud Service; and
b) Azure Government Services shall be the only variety of Government Community Cloud Service (or Online Service, in general) used by the State under the Government Contract, unless the Government Contract is later amended in writing between the State and Reseller, with Microsoft's concurrence.

"Government Contract" means the binding agreement between Contractor and Customer, pursuant to California solicitation Event ID 0000003775, under which Customer orders or otherwise uses and pays for Azure Government Services from Contractor, and into which these Microsoft Customer Terms and Conditions have been incorporated.

"License" means each Enterprise's right to access and use an Azure Government Service. Azure Government Services sold hereunder are available solely on a subscription basis as "Subscription Licenses", and are billed either

a) annually in advance, if made available as "Plans" or
b) according to Consumption Rates and/or Monetary Commitment, in accordance with the terms and conditions of Section 2, below.

"Microsoft" means the entity that:

a) is the Service Provider for Azure Government Services; and
b) has entered with Contractor into a Government Partner Licensing Agreement (and one or more Enrollments on the State's behalf), under which Contractor may place orders and be invoiced for Azure Government Services used by CDT and other User Agencies.

"MS OST" means the document which contains the use rights for Azure Government Services. Notwithstanding Microsoft's periodic changes to the MS OST posted to the Volume License Site, Microsoft will establish a "Locked OST" for applicable Services in accordance with the terms and conditions of Section 1.c, below. For clarity, the MS OST contains general and product-specific terms and conditions for both:

a) component services and features of Azure Government Services applicable to the Government Contract; and
b) other Microsoft Online Services not applicable to the Government Contract.

"MS SLA" means Service Level Agreement that specifies the minimum service levels for Azure Government Services. Notwithstanding Microsoft's periodic changes to the MS SLA posted to the Volume License Site, Microsoft will establish a "Locked SLA" for applicable Services in accordance with the terms and conditions of Section 1.c, below. For clarity, the MS SLA contains service levels for both:

a) component services and features of Azure Government Services applicable to the Government Contract, along with;
b) other Microsoft Online Services not applicable to the Government Contract.

"Online Services" means the Microsoft-hosted services identified as Online Services in the Product Terms. For clarity:

a) the only Online Services which may be purchased under this Agreement are those included in the definition of "Azure Government Services," above, and
b) all references to Online Services in these Microsoft Customer Terms and Conditions refer solely to Azure Government Services.

"Product" means all products identified in the Product Terms, such as all software, Online Services and other web-based services, including pre-release or beta versions. For clarity:

a) the terms "Azure Government" and "Online Service" are generally used in lieu of "Product," below in these Microsoft Customer Terms and Conditions; and
b) to the extent that Microsoft uses the term "Product" on its web pages and in other customer materials, and which is not otherwise intended based upon context to include Azure Government Services, the term "Product" will be deemed to include Azure Government Services.

"Product Terms" means the document that provides information about Microsoft Products available through Microsoft volume licensing agreements. For clarity:

a) Products include, but are not limited to, Microsoft Azure Services in general and some Azure Government Services specifically;

b) The Product Terms document is available on the Volume Licensing Site and is updated from time to time;

c) Those terms and conditions of the Product Terms which expressly apply to the methods and schedules applicable to Microsoft Azure Services (including Azure Government Services) have been adapted for the Government in Section 2 below, subject to the Government Contract's order of precedence section; and

d) Unlike the MS OST and MS SLA, the Product Terms may not be locked for the term of the Government Contract, to the extent that Microsoft uses the Product Terms both to:

i. identify available License Plans, and product-specific terms and conditions for such, and

ii. communicate limited-time promotional offers applicable to the State and Microsoft's other customers.

"Reseller" is defined in the Government Contract, and is a Microsoft-authorized Licensing Solutions Partner ("LSP").

"State" means the State of California and its User Agencies, acting by and through CDT.

"State/Local Entity" means (1) any agency of a state or local government in the United States, or (2) any United States county, borough, commonwealth, city, municipality, town, township, special purpose district, or other similar type of governmental instrumentality established by the laws of Customer's state and located within Customer's state's jurisdiction and geographic boundaries. For clarity, this definition is included to describe both (i) the State and its User Agencies; and (ii) other State/Local Entities in the United States that are Community Members, and which share the use (in logically-isolated environments) of Microsoft's multitenant IaaS and PaaS Services.

"Tribal Entity" means a federally-recognized tribal entity performing tribal governmental functions and eligible for funding and services from the U.S. Department of Interior by virtue of its status as an Indian tribe.

"use" or **"run"** means to copy, install, use, access, display, run or otherwise interact with.

"Use Rights" means the use rights or terms of service for each component and feature of Azure Government Services, as identified in Section 1.c of these Microsoft Customer Terms and Conditions. The Use Rights supersede the terms of any end user license agreement ("EULA") that accompanies a Product. For clarity:

- Use Rights do not supersede any click-to-accept terms of service for Microsoft websites and administrative portals; and
- Microsoft does not anticipate presenting click-to-accept EULA terms and conditions for any Azure Government Services purchased hereunder. However, if this were to change during the term of the Government Contract, then any such click-to-accept EULA would be superseded by the Use Rights, in accordance with this definition.

"Volume Licensing Site" means http://www.microsoft.com/licensing/contracts or a successor site.

1. LICENSES FOR AZURE GOVERNMENT SERVICES.

a) **License grant.** By accepting an Enrollment, Microsoft authorizes Contractor to grant (and Contractor hereby grants the applicable Enterprise) a non-exclusive, worldwide and limited right to use Azure Government Services.

- Each Azure Government Service Plan (as such term is used in Section 2, below, titled "Commitment" and "Consumption") may be used by a number of individual users, in each applicable Enterprise, equal to the quantity of Licenses ordered from Microsoft under the corresponding Enrollment.
- For other Azure Government Services consumed hereunder, the paragraphs of Section 2, below, shall apply as appropriate.

- The rights granted hereby are subject to the terms of this Government Contract (and its order of precedence section), the Use Rights and the Product Terms. Microsoft reserves all rights not expressly granted in these Microsoft Customer Terms and Conditions.

b) **Duration of Licenses.** Subscription Licenses for Azure Government Services Plans are temporary and expire when the applicable Enrollment is terminated or expires unless the Enrollment is renewed. The term of Monetary Commitment is set in accordance with the terms and conditions of Section 2, below.

c) **Applicable Use Rights and Service Level Agreement.**

i. The MS OST and MS SLA applicable throughout the term of the Government Contract, for Azure Government Services available as of the effective date of the Government Contract, shall be the MS OST and MS SLA shown as Exhibits 4 and 5, respectively, to these Microsoft Customer Terms and Conditions, respectively (hereafter, the "Locked OST" and "Locked SLA"), except as noted below. The Locked OST and Locked SLA are incorporated into this Government Contract, subject to it order of precedence section.

ii. The MS OST and MS SLA applicable throughout the term of the Government Contract for Azure Government Services released after the effective date of the Government Contract ("Later-Released Services") shall be the then-current MS OST and MS SLA, respectively, posted to the Volume License Site. Such then-current MS OST and MS SLA shall be incorporated by reference into this Government Contract, subject to its order of precedence section, upon the State's first use of Later-Released Services, subject to subsection (iii), below.

iii. As an exception to the foregoing, at any time during the term of the Government Contract, the State may submit a written request to Contractor, and Contractor shall submit such request to Microsoft, to supersede the MS OST and MS SLA shown as Exhibits 4 and 5, respectively, with a later-issued MS OST and MS SLA. Such written request will be deemed effective on a prospective basis (and the requested MS OST and MS SLA shall become the new "Locked OST" and "Locked SLA," respectively, for then-available Azure Government Services), as of the date Contractor notifies Microsoft of the request. The State's request shall reference the specific dated version of MS OST and MS SLA it wishes to become the new Locked OST and Locked SLA, and Contractor will as soon as practicable following the request provide (and execute with the State) an amendment to memorialize such change.

For clarity, unless the MS OST expressly establishes an exception to the contrary, those provisions in the MS OST which apply to components of Microsoft's commercial Azure Services shall apply to the same-named services when provided as part of Azure Government Services.

d) **License confirmation.** The Government Contract, including any order Customer places to Contractor under the Government Contract, and Customer's order confirmation from Reseller, if any, and evidence of Customer's payment to Contractor for Azure Government License Plans, Monetary Commitment and Consumption, will be Customer's evidence of all Subscription Licenses ordered under the Government Contract.

e) **Modification or termination of an Online Service for regulatory reasons.** Microsoft may modify or terminate one or more components or features of Azure Government Services (and Contractor may terminate the State's Subscription Licenses, if necessary) if there is any current or future government requirement or obligation that: (1) subjects Microsoft to any regulation or requirement not generally applicable to businesses operating in the United States or California; (2) presents a hardship for Microsoft to continue operating the applicable Service(s), component(s) or feature(s) without modification; and/or (3) causes Microsoft to believe the Government Contract (including but not limited to these Microsoft Customer Terms and Conditions) or the Service, component or feature, may be in conflict with any such requirement or obligation.

f) **Program updates.** Microsoft may make a change to the Enterprise Agreement program that will, upon renewal of the Government Contract after its original term and extension terms, make it necessary for the State to accept revisions to these Microsoft Customer Terms and Conditions in its follow-on contract with the Reseller.

2. ORDERING AND PAYING RESELLER FOR AZURE GOVERNMENT SERVICES.

a) **Subscription Term**
The State may only subscribe to Microsoft Azure Government Services (including Azure Government Services Plans) for a subscription term that ends on the end date of (is "coterminous" with) the Government Contract. The State must have at least two months remaining in the Government Contract term in order to subscribe to Microsoft Azure Government Services, or to add orders for Monetary Commitment. Microsoft and Reseller will establish one or more coterminous Enrollments for CDT on behalf of all or certain User Agencies. For clarity, if the State requires two or more logically-isolated Azure Government Services environments that do not share the same State administrators, then the State must instruct Reseller to submit two or more Enrollments to Microsoft for this purpose.

b) **Purchasing Services**
Microsoft Azure Government Services may be purchased in one or a combination of the following ways:

i. **Monetary Commitment:** Monetary Commitments are allocated proportionally through each Enrollment's term. The State may increase its Monetary Commitment for an Enterprise at any time by placing additional orders. When an additional order is placed, an Enrollment's Allocated Annual Commitment will be increased for that year by the amount of the order. For each subsequent year remaining in the Enrollment term, Allocated Annual Commitments will be increased by the amount of the additional order, multiplied by twelve, divided by the number of full months between when the additional order was placed and the anniversary date following the additional order.

Customers may reduce their Enrollment's Monetary Commitment for any future anniversary of the Government Contract Term by notifying their reseller, who must process the reduction with Microsoft prior to the anniversary date.
Each Enrollment's Enterprise must consume its Allocated Annual Commitment by the last day of the month preceding the anniversary each year, after which any unused portion of the Allocated Annual Commitment will be forfeited. The State may utilize its annual Consumption Allowance for each Enrollment by the last day of the month preceding the anniversary each year, after which any unused portion of that Enrollment's Consumption Allowance will be forfeited.

ii. **Consumption:** Customers pay based on the amount of Microsoft Azure Government Services consumed during a billing period. Certain features of the Microsoft Azure Government Services may only be available for purchase on a consumption basis.

iii. **Azure Government Services Plans:** If identified as such in the Product Terms, an Enterprise may be able to subscribe to a Microsoft Azure Government Service as an Azure Government Services Plan.

For clarity, as of the effective date of the Government Contract, certain Microsoft Azure Plans (and License Suite Plans) that contain “public cloud” versions of Microsoft Azure Services (with FedRAMP Moderate ATO), may be purchased under the State’s Enterprise Agreement for the purpose of managing or enhancing one or more other Microsoft Online Services. Examples include, but are not limited to, SKUs for the Microsoft Enterprise Mobility and Security suite (“EMS”). Terms and conditions pertaining to FedRAMP readiness for any non-Azure-branded service (e.g. Microsoft Intune), if any, will be contained in the State’s separate Enterprise Agreement. For clarity, Microsoft:

1. Does not represent such public cloud version of Azure Services, as described in the previous paragraph, as “FedRAMP High” (they have FedRAMP Moderate ATO);
2. Does not represent such services to be “Azure Government Services” for sale under the Government Contract.

Notwithstanding (a) and (b), some same-named Services (not sold as “Plans”) may be available for the State to consume for other purposes under the Government Contract as Azure Government Services. Such Services may include, but not be limited to, Azure Active Directory Premium.

c) **Payment and Fees**

Enterprises whose Enrollments have been provisioned for Azure Government Services without a Monetary Commitment will be invoiced by Reseller quarterly at Consumption Rates.

For Enterprises whose Enrollments have a Monetary Commitment, the first Allocated Annual Commitment for the Enrollment will be invoiced immediately, and future Allocated Annual Commitments will be invoiced on the anniversary of the Government Contract effective date. Alternatively, The State may choose to pay its entire Monetary Commitment for each Enterprise upon placing the initial order for its Enrollment.

Each month, Microsoft will (through Reseller) deduct from each Enterprise’s Allocated Annual Commitment the monetary value of the Enterprise’s usage of eligible Microsoft Azure Government Services. Once the Enterprise’s Allocated Annual Commitment balance has been exhausted, any additional usage will be invoiced at Consumption Rates.

All usage exceeding the Allocated Annual Commitment will be invoiced at Consumption Rates to the Reseller at the end of each quarterly period following the Government Contract’s effective date.

All usage of the Microsoft Azure Government Services after the expiration or termination of the Government Contract, for example during any grace period or short-term contract extension, will be invoiced by Microsoft to Reseller at then-current Consumption Rates on a quarterly basis.

The purchase of an Azure Government Services Plan will be invoiced to Reseller (and Reseller will invoice the State) according to the terms of the Resellers' volume licensing agreement with Microsoft, which governs Reseller's payment terms for the order of Microsoft Online Services generally, which follow the same rules as generally applicable to all Enterprise Agreements (including the State's separate Enterprise Agreement) regarding advance payment and annual billing schedules for such Online Services.
Monetary Commitment cannot be applied to the purchase of a Microsoft Azure Government Services Plan; provided, however, that if an Azure Government Services Plan includes the purchase of an initial quantity of a service ("Initial Quantity"), each Enterprise's usage that exceeds the Initial Quantity will be billed at Consumption Rates, and the Enterprise's Allocated Annual Commitment can be applied to such usage.

Microsoft may offer lower prices to Reseller for individual Microsoft Azure Government Services during the Government Contract term on a permanent or temporary (promotional) basis.

d) **Microsoft Azure Hybrid Use Benefit**
Under the Microsoft Azure Hybrid Use Benefit ("HUB"), a customer with Microsoft Windows Server Licenses covered with Software Assurance ("SA") (on a separate "State License Agreement," such as the State's Enterprise Agreement) may upload to and use its own Windows Server image on Azure Government Services.
Azure HUB enables Customers' use of Windows Server on Azure Government Services through Azure Virtual Machines ("Base Instances"). HUB does not include the cost of Base Instances, and Base instances do not include Windows Server. Each Windows Server processor License with SA, and each set of 16 Windows Server core Licenses with SA, entitles Customer to use Windows Server on Microsoft Azure on up to 16 Virtual Cores allocated across two or fewer Azure Base Instances. Each additional set of 8 core Licenses with SA entitles use on up to 8 Virtual Cores and one Base Instance.

The State's administrator must indicate that it is using Windows Server under the HUB when configuring the uploaded image(s) on Azure. The State may use its uploaded image(s) subject to the Online Services Terms and the terms of the applicable State License Agreement.

The HUB provides additive rights to deploy and use the software when exercised in connection with Windows Server Datacenter Edition Licenses and alternative rights when exercised in connection with Windows Server Standard Edition Licenses. Standard Licenses are deemed "assigned to Azure" when the State uses Windows Server under the HUB, and are subject to the License reassignment limitations in the Universal License Terms section of the Online Services Terms.

3. TRANSFERRING AND ASSIGNING LICENSES.

a) **License transfers.** License transfers for Azure Services Licensing Plans outside of each Enterprise are not permitted.

b) **Internal assignment of Licenses.** Subscription Licenses for each Azure Services Licensing Plan must be assigned to a single user within each Enterprise. Licenses may be reassigned within an Enterprise as described in the Use Rights.

4. USE, OWNERSHIP, RIGHTS, AND RESTRICTIONS.

a) **Products.** Use of any Azure Government Service is governed by the Use Rights specific to each such Service and by the Government Contract, subject to its order of precedence section.

b) **Fixes.** Any Fix for an Azure Government Service is licensed under the same terms as the Service to which it applies. If a Fix is not provided for a specific Service, any use terms Microsoft provides with the Fix will apply.

c) **Non-Microsoft software and technology.** Customer is solely responsible for any non-Microsoft software or technology the Enterprise installs or uses with the Azure Government Services or Fixes.

d) **Restrictions.** The Enterprise must not (and must not attempt to) (1) reverse engineer, decompile or disassemble any Product or Fix, (2) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to obligations beyond those included in this Government Contract; or (3) work around any technical limitations in the Products or restrictions in Product documentation. Except as expressly permitted in this Government Contract, the Enterprise must not (1) separate and run parts of a Product on more than one computer, upgrade or downgrade parts of a Product at different times, or transfer parts of a Product separately; or (2) distribute, sublicense, rent, lease, lend, or use any Product or Fix to offer hosting services to a third party.

e) **No transfer of ownership; Reservation of rights.** Products and Fixes are protected by copyright and other intellectual property rights laws and international treaties. Microsoft (1) does not transfer any ownership rights in any Products or Fixes and (2) reserves all rights not expressly granted to Customer or the Enterprise in this Government Contract.

5. CONFIDENTIALITY.

“Confidential Information” is non-public information that is designated “confidential” or that a reasonable person should understand to be confidential, including State Data and the terms of this Government Contract and other agreements. The MS OST may provide additional obligations for, and limitations on disclosure and use of, State Data. Confidential Information does not include information that (1) becomes publicly available without a breach of this agreement, (2) the receiving party received lawfully from another source without an obligation to keep it confidential, (3) is independently developed, or (4) is a comment or suggestion one party volunteers about the other’s business, products or services.

The State, each Enterprise, Contractor and Microsoft will all take reasonable steps to protect the other’s Confidential Information and will use the other’s Confidential Information only for purposes of the business relationship. Neither the State, any Enterprise, Contractor nor Microsoft will disclose that information to third parties, except to its employees, Affiliates, User Agencies, contractors, advisors and consultants (collectively, “Representatives”) and then only on a need-to-know basis under nondisclosure obligations at least as protective as this Government Contract. The State, each Enterprise, Contractor and Microsoft remain responsible for the use of the Confidential Information by their Representatives and, in the event of the discovery of any unauthorized use or disclosure, must promptly notify the other.
The State, each Enterprise, Contractor or Microsoft may disclose the other’s Confidential Information if required by law; but only after it notifies the non-disclosing entity (if legally permissible) to enable it to seek a protective order.

Neither the State, any Enterprise, Contractor nor Microsoft is required to restrict work assignments of Representatives who have had access to Confidential Information. The State, each Enterprise, Contractor and Microsoft all agree that use of information in Representatives' unaided memories in the development or deployment of products or services does not create liability under the Government Contract or trade secret laws and agree to limit what they disclose to each other accordingly.

These obligations are subject to Section 26 of the General Provisions (titled "Confidentiality of Data") and apply (1) for State Data until it is deleted from the Azure Government Services, and (2) for all other Confidential Information, for a period of five years after the Confidential Information is received.

6. PRIVACY AND COMPLIANCE WITH LAWS.

a) The State and each Enterprise consent to the processing of personal information by Microsoft and its agents to facilitate the subject matter of this agreement. The State and each Enterprise will obtain all required consents from third parties (including each Enterprise's contacts, resellers, distributors, administrators, and employees) under applicable privacy and data protection law before providing personal information to Microsoft.

b) Except as otherwise stated in the MS OST, personal information collected by Microsoft (1) may be transferred, stored and processed in the United States or any other country in which Microsoft or its contractors maintain facilities and (2) will be subject to the privacy terms specified in the Use Rights.

For clarity, both the General Provisions, Special Provisions, and the section of the MS OST titled "Data Processing Terms" establish terms and conditions for the at-rest storage of State Data in Azure Government Services solely in the United States.

c) **U.S. Export.** Azure Government Services (and all Microsoft Products) and Fixes, are subject to U.S. export jurisdiction. The State and each Enterprise must comply with all applicable international and national laws, including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end use and destination restrictions by U.S. and other governments related to Microsoft products, services, and technologies.

7. WARRANTIES.

RESERVED. Microsoft's warranties for Azure Government Services are in the General Provisions.

8. DEFENSE OF THIRD PARTY CLAIMS.

a) **Microsoft's agreement to protect.** Microsoft will defend the State against any claims made by an unaffiliated third party that any Product (including but not limited to Azure Government Services) or Fix that is made available by Microsoft for a fee infringes that party's patent, copyright, or trademark or makes intentional unlawful use of its Trade Secret. Microsoft will also pay the amount of any resulting adverse final judgment or settlement to which Microsoft consents. This section provides the State's exclusive remedy for these claims.

b) **Limitations on defense obligation.** Microsoft's obligations will not apply to the extent that the claim or award is based on:

   i. State Data, code, or materials provided by the State as part of an Online Service;
   ii. The State's use of the Product or Fix after Microsoft notifies it to discontinue that use due to a third party claim;
   iii. The State's combination of the Product or Fix with a non-Microsoft product, data or business process;
   iv. Damages attributable to the value of the use of a non-Microsoft product, data or business process;
   v. Modifications that the State makes to the Product or Fix;
   vi. The State's redistribution of the Product or Fix to, or its use for the benefit of, any unaffiliated third party, except as expressly permitted by the Use Rights;
   vii. The State's use of Microsoft's trademark(s) without express written consent to do so; or
   viii. Any Trade Secret claim, where the State acquires the Trade Secret:

      1. through improper means;
      2. under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
      3. from a person (other than Microsoft or its Affiliates) who owed to the party asserting the claim a duty to maintain the secrecy or limit the use of the Trade Secret.

   The State will be responsible for any costs or damages that result from any of these actions.

c) **Specific rights and remedies in case of infringement.**

   i. **Microsoft's rights in addressing possible infringement.** If Microsoft receives information concerning an infringement claim related to a Product or Fix, Microsoft may, at its expense and without obligation to do so, either:

      1. procure for the State the right to continue to use the allegedly infringing Product or Fix; or
      2. modify the Product or Fix, or replace it with a functional equivalent, to make it non-infringing, in which case the State will immediately cease use of the allegedly infringing Product or Fix after receiving notice from Microsoft.

   ii. **The State's specific remedy in case of injunction.** If, as a result of an infringement claim, the State's use of a Product or Fix that is made available by Microsoft for a fee is enjoined by a court of competent jurisdiction, Microsoft will, at its option:

      1. procure the right to continue its use;
      2. replace it with a functional equivalent;
      3. modify it to make it non-infringing; or
      4. refund the amount paid (or, for Online Services, refund any amounts paid in advance for unused Online Services) and terminate the license or right to access the infringing Product or Fix.

d) **State's Responsibility**. The State will be responsible for any costs or damages arising from any claims made by an unaffiliated third party that:

i. any State Data or non-Microsoft software Microsoft hosts on the State's behalf infringes the third party's patent, copyright, or trademark or makes intentional unlawful use of its Trade Secret; or
ii. arise from the State's or its end user's violation of the Use Rights or these Microsoft Customer Terms and Conditions.

The State must pay the amount of any resulting adverse final judgment (or settlement to which the State consents).

e) **Immunities of the State.** Pursuant to Government Code section 815 et seq., the State of California has immunity for specific legal claims. The State does not waive any such immunities for purposes of this Government Contract, including but not limited to this Section 8 of the Microsoft Customer Terms and Conditions. Further, any claim under this Section 8 are subject to the claims presentation requirements of Government Code section 900 et seq. The State shall not be liable under this Section 8, or any other section of this Government Contract, unless these prerequisites are satisfied.

f) **OBLIGATIONS OF PROTECTED PARTY. THE STATE MUST NOTIFY MICROSOFT PROMPTLY IN WRITING OF A CLAIM SUBJECT TO THE SUBSECTION TITLED "MICROSOFT'S AGREEMENT TO PROTECT" AND MICROSOFT MUST NOTIFY THE STATE PROMPTLY IN WRITING OF A CLAIM SUBJECT TO THE SUBSECTION TITLED "STATE'S RESPONSIBILITY." TO THE EXTENT PERMITTED BY APPLICABLE LAW, WHERE THE STATE INVOKES ITS RIGHT TO PROTECTION IT MUST:**

i. give Microsoft sole control over the defense or settlement; and
ii. provide reasonable assistance in defending the claim. Microsoft will reimburse the State for reasonable out of pocket expenses that it incurs in providing assistance.

9. LIMITATION OF LIABILITY.

RESERVED. The parties' limitations of liability are in Section 20 of the General Provisions.

10. GOVERNMENT COMMUNITY CLOUD.

***A.* AZURE GOVERNMENT SERVICES CONSTITUTE GOVERNMENT COMMUNITY CLOUD SERVICES, AS DEFINED ABOVE. AS SUCH, THE FOLLOWING TERMS AND CONDITIONS SHALL APPLY:**

a) **Community requirements.** The State is a member of the Community, and agrees to use Government Community Cloud Services solely in its capacity as a member of the Community and for the benefit of User Agencies that are members of the Community. Use of Government Community Cloud Services by an entity that is not a member of the Community, or to provide services to non-Community, members is strictly prohibited and could result in termination of the Government Contract. The State acknowledges that only Community members may use Government Community Cloud Services.

b) All terms and conditions applicable to non-Government Community Cloud Services also apply to their corresponding Government Community Cloud Services, except as otherwise noted in the Use Rights, Product Terms, and these Microsoft Customer Terms and Conditions.

c) Customer may not deploy or use Government Community Cloud Services and corresponding non-Government Community Cloud Services in the same domain. For clarity, non-Government Community Cloud Services, if any, would not be purchased under this Government Contract, so this subsection c. is provided for informational purposes only.

d) **Use Rights for Government Community Cloud Services.** For Government Community Cloud Services, notwithstanding anything to the contrary in the Use Rights:

i. Government Community Cloud Services will be offered only within the United States.

ii. Additional European Terms, as set forth in the Use Rights, will not apply.

iii. References to geographic areas (each, a “Geo”) in the MS OST with respect to the location of Customer Data at rest, as set forth in the Use Rights, refer only to the United States.

11. Miscellaneous.

a) **Assignment.** CDT may assign all its rights under this Government Contract to a User Agency, but it must notify Contractor in writing of the assignment, and Contractor must notify Microsoft. Any other proposed assignment must be approved by the non-assigning party and Contractor in writing, subject to Microsoft’s written consent. Assignment will not relieve the assigning party of its obligations under this Government Contract. Any attempted assignment without required approval will be void.

b) **Severability.** If any provision of this Government Contract is found unenforceable, the balance of the agreement will remain in full force and effect.

c) **Waiver.** A waiver of any breach of any provision of the Government Contract, the Use Rights or these Microsoft Customer Terms and Conditions is not a waiver of any other breach. Any waiver must be in writing and signed by an authorized representative of the waiving party.

d) **Dispute resolution.** Disputes relating to the Government Contract (including but not limited to these Microsoft Customer Terms and Conditions) will be subject to applicable dispute resolution laws of California. Notwithstanding the foregoing, Microsoft may seek injunctive relief in any appropriate jurisdiction with respect to a violation of intellectual property rights or confidentiality obligations.

e) **Survival.** All provisions survive termination or expiration of this Government Contract, except those requiring performance only during the term of this Government Contract.

f) **This agreement is not exclusive.** The State is free to enter into agreements to license, use, or promote non-Microsoft products or services.

g) **Applicable law.** Any dispute between the State and a Microsoft Affiliate related to this Government Contract will be governed by and construed in accordance with the laws of California and federal laws of the United States, without giving effect to its conflict of laws.

h) **Microsoft as independent contractor.** Microsoft and Customer are independent contractors. Microsoft and the State each may develop products independently without using the other’s Confidential Information.

i) **Use of contractors.** Microsoft may use contractors to perform services but will be responsible for their performance subject to the terms of this Government Contract.

j) **Amendments.** Any amendment to this Government Contract that affects Microsoft's rights under this Government Contract must be approved by Microsoft and executed between Microsoft and Contractor before Contractor provides a corresponding Amendment to Customer, except that Microsoft may (1) change the Product Terms from time to time; and (2) update the MS OST in accordance with both the terms and conditions of Section 1.c of these Microsoft Customer Terms and Conditions and other terms of this Government Contract. Any conflicting terms and conditions contained in the State's purchase order to Contractor will not apply to Microsoft.

k) **Free Products.** Any free Product provided to an Enterprise (for example, a preview service) is for the sole use and benefit of the Enterprise's purposes only, and is not provided for use by or personal benefit of any specific government employee.

l) **Third party beneficiary.** Microsoft is a third party beneficiary of this Government Contract and may enforce its terms.

m) **Natural disaster.** In the event of a natural disaster, Microsoft may provide additional assistance or rights to the State than are set forth in this agreement by posting them on http://www.microsoft.com at such time.

n) **Calendar days.** Any reference in this agreement to "day" will be a calendar day, except references that specify "business day."

Except for changes made by these Microsoft Customer Terms and Conditions, the Government Contract remains unchanged and in full force and effect. If there is any conflict between any provision in these Microsoft Customer Terms and Conditions and any provision in the Government Contract, the Government Contract's order of precedence section shall control.

Remainder of page intentionally left blank.

Amendment 1 to Exhibit 4
Microsoft CJIS Amendment

This Microsoft Online Services Criminal Justice Information Services (CJIS) Amendment ("Microsoft CJIS Amendment") shall apply to CDT' (and its User Agencies') storage and processing of CJI in Microsoft's CJIS Covered Services (as each such term is defined below), and is hereby added to the Government Contract (as defined in this Exhibit 4, above). The parties agree that this CJIS Amendment supplements the Government Contract and applies to only the CJIS Covered Services the State buys under the Government Contract.

By performing in accordance with the terms of this CJIS Amendment, Microsoft also satisfies its obligations under Appendix A to this CJIS Amendment, below (the Private Contractor Management Control Agreement for CLETS).

Defined Terms.

Capitalized terms used but not defined in this CJIS Amendment will have the meanings provided in the Government Contract (including other Exhibits thereto) and CJIS Policy. The following definitions are used in this CJIS Amendment:

"CJI" means Criminal Justice Information, as such term is defined in CJIS Policy.

"CJIS Policy" means the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy that is in effect as of the effective date of the Enrollment related to this Agreement and any successor versions brought into effect by the FBI during the term of the Enrollment, but excluding draft versions of CJIS Policy, versions of CJIS Policy released for comment or review and similar proposed policy versions that may be released by the FBI but not finally adopted.

"**CJIS Covered Services**" means each of the Azure Government Services listed as being in the scope of the CJIS Policy at http://azure.microsoft.com/en-us/support/trust-center/services.

> Microsoft may, from time to time, add new CJIS Covered Services, in which case Microsoft will work in good faith with CSA and The State to amend both CSA's separate agreement with Microsoft and this Enrollment to add such new CJIS Covered Services. In that case, CSA's agreement with Microsoft must be amended before the Enrollment will be amended.

"CSA" means the State of California, Department of Justice, or a successor agency as determined by the State of California, acting in its capacity as the CJIS Systems Agency for the State of California.

"End User" means an individual that accesses the CJIS Covered Services.

Term and Conditions.

1. CJIS Security Addendum

The CJIS Covered Services are Government Community Cloud Services (as defined in Exhibit 1). Subject to the Agreement, this Amendment, and the separate agreement reached with the CSA, Microsoft will deliver the CJIS Covered Services subject to the CJIS Security Addendum as set forth in the CJIS Policy.

Role of CSA. Microsoft has entered into an agreement with the CSA, including the CJIS Security Addendum, to facilitate use of CJIS Covered Services by public entities in the State of California that are subject to CJIS Policy. The State and its User Agencies will rely on the CSA, acting in its capacity as the CJIS Systems Officer (CSO) for the State of California, to perform personnel screening of Microsoft personnel engaged in the delivery of the CJIS Covered Services and to exercise certain other functions under the CJIS Policy as described in this CJIS Amendment.

2. State and User Agency Responsibilities

2.1 The State acknowledges that the CJIS Covered Services enable User Agencies and their End Users optionally to access and use a variety of additional resources, applications, or services that are (a) provided by third parties, or (b) provided by Microsoft subject to their own terms of use or privacy policies (collectively, for convenience, "add-ons"), as described in services documentation and/or in the portal through which CDT' administrator(s) will manage and configure the CJIS Covered Services.

2.2 The State is responsible to review services documentation and CJIS implementation guidance. The State is responsible to establish, adopt and implement such policies and practices for its User Agencies and End Users' use of CJIS Covered Services, together with any add-ons, as the State determines are appropriate to ensure the State's compliance with the CJIS Policy or other legal or regulatory requirements applicable to the State and not generally applicable to Microsoft as an IT service provider. The State's and its User Agencies' compliance with the CJIS Policy will be dependent, in part, upon the State's (and/or its User Agencies') configuration of the Services and the State's compliance with authoritative guidance from sources other than Microsoft (e.g., NCIC 2000 Operating Manual). The State is responsible to confirm the CJIS Covered Services environment is prepared and appropriate for CJI prior to its processing or storing such data in the CJIS Covered Services.

2.3 The State acknowledges that only CJIS Covered Services will be delivered subject to the terms of this CJIS Amendment. Microsoft does not recommend processing and storage of CJI in other services. Without limiting the foregoing, data that the State elects to provide to the Microsoft technical support organization, if any, or data provided by or on behalf of the State to Microsoft's billing or commerce systems in connection with purchasing/ordering CJIS Covered Services, if any, is not subject to the provisions of this CJIS Amendment or the CJIS Addendum.

3. Approach to Compliance with CJIS Security Policy

This Section 3 contains additional information about how certain requirements of the CJIS Policy will be fulfilled. For convenient reference, provisions are numbered to conform to section numbering in the CJIS Policy. Microsoft and CDT will each rely on the CSA to perform certain functions as described below, and the State and its Authorized Users are responsible to confirm the approach with the CSA to the extent the State deems appropriate.

3.1 CJIS Section 5.2 Policy Area 2: Security Awareness Training

Microsoft will supplement its existing security training program as required to meet the requirements of Section 5.2 of the CJIS Policy. Required training will be delivered to personnel identified as in scope for CJIS Personnel Screening within six (6) months of the date the CSA notifies Microsoft that personnel have passed required personnel screening. Microsoft will refresh training for in scope personnel on at least a biennial basis thereafter.

Microsoft will maintain training records, which will be available to the CSA upon written request.

3.2 CJIS Section 5.3 Policy Area 3: Incident Response

In the event of an information security incident affecting the CJIS Covered Services, Microsoft will address such incident with the State as follows:

(a) Microsoft will comply with the terms and conditions of Section 5 of the Special Provisions (Security Breach or Data Breach Notification)

(b) Notification of Security Incidents, if any, will be delivered to one or more State Identified Contacts, in accordance with the aforementioned Section 5 of the Special Provisions, by any means Microsoft selects, including via email. It is the State's sole responsibility to ensure State Identified Contacts maintain accurate contact information on the Online Services portal at all times.

(e) Effective investigation or mitigation of a Security Incident (Data Breach) may be dependent upon information or services configurations within the State's control. Accordingly, compliance with CJIS Policy Incident Response requirements will be a joint obligation of Microsoft and the State.

(f) In the event Microsoft reasonably anticipates that a Security Incident (Data Breach) may require legal action against involved individual(s), or where the Security Incident (Data Breach) involves either civil or criminal action, Microsoft will conduct its investigative activities under guidance of legal staff and in accordance with general evidentiary principles, to the extent consistent with both (i) CJIS Policy; and (ii) the primary incident response objectives of containing, resolving, and mitigating the impact of a Security Incident (Data Breach) to customers including the State.

3.3 CJIS Section 5.11 Policy Area 11: Formal Audits

(a) Audits by FBI CJIS Division. In the event the FBI CJIS Division desires to perform an audit of the CJIS Covered Services, Microsoft will cooperate with such audit in good faith. The FBI may be permitted to access State Data in connection with such audit, but not data belonging to other customers in the multi-tenant environment from which the CJIS Covered Services are delivered. If the FBI identifies what it believes to be deficiencies in the CJIS Covered Services as a result of an audit, Microsoft is committed to working in good faith to resolve the FBI's concerns through discussion and interaction between Microsoft, the CSA, and the FBI. The State (CDT and other User Agencies) will assist in this process if and as requested, but will otherwise rely on the CSA to act on behalf of all similarly situated entities that have purchased the CJIS Covered Services.

(b) Audits by the State. In the event that the CDT or any User Agency other than the CSA desires to audit the CJIS Covered Services pursuant to the CJIS Policy, CDT and/or such User Agency appoints the CSA to act on the State's behalf to conduct such audit activities, and the State agrees to rely on the CSA's audit in full satisfaction of any right to audit the CJIS Covered Services.

The State acknowledges the CSA will exercise this right by attempting to satisfy its requirements for information via reference to Microsoft's services documentation, including audit reports prepared by Microsoft's qualified third party auditors and FedRAMP 3rd Party Assessment Organization. Along with other customers for the CJIS Covered Services, the CSA will be provided access to information generated by Microsoft's regular monitoring of security, privacy, and operational controls in place to afford applicable customers an ongoing view into effectiveness of such controls, and the CSA may communicate with Microsoft subject matter experts. In the event the CSA reasonably determines this information is not sufficient for the CSA's or the State's audit objectives, then, upon the CSA's written request, Microsoft will provide the CSA or its qualified third party auditor the opportunity to communicate with Microsoft's auditor at the CSA's or CDT's expense and, if required, a direct right to examine the CJIS Covered Services, including examination on premises. The CSA or its auditor may only access data belonging to the State or other entities in the State of California that have purchased the CJIS Covered Services and rely on the CSA for purposes of audit. The State will be responsible for Microsoft's reasonable additional costs associated with any examination it requests or appoints the CSA to perform, unless the CSA agrees to pay for such costs on the State's behalf.

(c) Confidentiality of Audit Materials. Information provided by Microsoft to the FBI CJIS Division or CSA in connection with audit activities consists of highly confidential proprietary or trade secret information of Microsoft. It is not expected that any State entity other than the CSA will require access to such information, and Microsoft may request reasonable assurances, written or otherwise, that information will be maintained as confidential and/or trade secret prior to providing such information to the State. If provided, the State will ensure Microsoft's audit materials, or report(s) created by the State based on a CSA audit of the CJIS Covered Services, are afforded the highest level of confidentiality available under applicable law. For clarity, the terms and conditions of the agreement between the CSA and Microsoft provide for the CSA' handling of Microsoft's audit materials.

3.4 CJIS Section 5.12 Policy Area 12: Personnel Security

(a) The State appoints the CSA to perform, and will rely upon CSA's completion of, personnel screening (i.e., background checks) for personnel in scope pursuant to Section 5.12 of the CJIS Policy. The State is responsible to confirm directly with the CSA that such personnel screening as the CSA or the State determines is required has been completed prior to initial processing of CJI in the CJIS Covered Services. Screening will be performed by the CSA on behalf of all entities in the State of California that onboard to the CJIS Covered Services. Adjudication by CDT, User Agencies other than the CSA, or other counties, cities, or other subdivisions or agencies of state government will not be permitted. To facilitate efficient and effective personnel screening:

- The CSA will define adjudication criteria for personnel screening.
- Microsoft and the CSA will jointly define the process by which Microsoft will deliver to the CSA relevant information regarding personnel who may in the anticipated scope of their duties have logical or physical access to CJI in the CJIS Covered Services.
- It is not anticipated that the CSA will deliver to CDT or other User Agencies confidential personal information pertaining to Microsoft personnel. However, if CDT or a User Agency receives such confidential personal information it will be afforded the highest level of confidentiality available under applicable law. For clarity, the terms and conditions of the agreement between the CSA and Microsoft provide for the CSA' handling of Microsoft's confidential personal information.
- If the State elects to obtain professional services from Microsoft in addition to the CJIS Covered Services (e.g. consulting services in connection with the State's migration and onboarding to the CJIS Covered Services), such personnel will not

be included in scope for personnel screening by the CSA unless separately agreed by the State, the CSA, and Microsoft.

(b) In the event the CSA approves a process under which a federal law enforcement agency or other suitable body conducts screening of personnel who have access to Customer Data in the CJIS Covered Services compliant with requirements of the CJIS Policy in lieu of CSA-conducted screening, the State will abide by the CSA's approval of personnel screening being conducted in this manner.

3.5. CJIS Policy Section 5.1 Policy Area 5.1.1.2: State and Federal Agency User Agreements

If in order to facilitate FBI penetration testing required under the State's (or any User Agency's) CJIS user agreement, the State or applicable User Agency (or CSA, on its behalf) determines it requires penetration testing information related to the CJIS Covered Services, the State or applicable User Agency (or CSA on its behalf) will rely on the following Microsoft processes and information:

a) General, Microsoft shall design, test and operate the CJIS Covered Services to ensure they are free of common security vulnerabilities. Microsoft shall regularly conduct penetration testing to evaluate the security controls at the platform level (PaaS components of Azure Government Services), host, and networks layers used to provide the CJIS Covered Services. Microsoft shall take commercially reasonable steps to remediate significant weaknesses discovered. Assessment of penetration testing will be done by independent third party auditors and included in the scope of audit relevant to the State's service certification or accreditation.

b) Azure CJIS Covered Services. Additionally, Microsoft has established a policy for Azure Government Services customers to carry out authorized penetration testing only on their applications hosted in Azure Government. Because such testing can be indistinguishable from a real attack, it is critical that customers conduct such penetration testing only after obtaining approval in advance from Azure Customer Support. Penetration testing must be conducted in accordance with Microsoft's terms and conditions. To learn more or to initiate penetration testing, please see https://security-forms.azure.com/penetration-testing/terms.

3.6. CJIS Policy Section 5.10 Policy Area 5.10.1.5: Cloud Computing

Microsoft uses State Data as set forth in the Government Contract (including but not limited to the MS OST) for provision of the CJIS Covered Services.

3.7 NCIC 2000 Operating Manual

The State acknowledges that the current NCIC 2000 Operating Manual consists of guidance and/or requirements for the State's use of the CJIS Covered Services. In the event the State determines the NCIC 2000 Operating Manual imposes obligations with respect to the CJIS Covered Services that can, in the State's opinion, only be satisfied via changes in the manner in which the CJIS Covered Services are operated or delivered to the State, the State may request that the CSA provide Microsoft with written notification of the specific changes it believes are required of Microsoft in order to enable the State's compliance with the NCIC 2000 Operating Manual, and Microsoft agrees to consider any such request(s) relayed to Microsoft by the CSA in good faith.

3.8 Notices

Any notices in connection with the CJIS Covered Services will be delivered by Microsoft to the State (and its State Identified Contacts). The State will determine whether these or any other notices regarding the CJIS Covered Services are required to be delivered to the

FBI, CJIS Division, and/or to the CSA, as contemplated in Section 6.05 of the Security Addendum and, if required, deliver such notices.

Remainder of page intentionally left blank.

Appendix A to CJIS Amendment
Private Contractor Management Control Agreement

Agreement to allow the California Law Enforcement Telecommunications System (CLETS) access by the State (on behalf of any User Agencies that are public law enforcement/criminal justice agencies) to Microsoft (Private Contractor) to deliver CJIS Covered Services (as defined above) on its behalf.
Before executing the Government Contract, the State shall enter its ORI number here:

____
Microsoft satisfies its obligations under this Private Contractor Management Control Agreement ("PCMCA") by performing in accordance with the CJIS Information Agreement between California Department of Justice (CA DOJ) and Microsoft, and the CJIS Amendment to which this PCMCA is attached. For purposes of this PCMCA, the State is referred to as "Subscribing Agency" and agrees that:

- Adjudication of Microsoft personnel and formal audits, whether under CJIS Policy or CLETS, will be conducted by CA DOJ in accordance with the CJIS Information Agreement;
- Microsoft personnel signatures on the CLETS employee/Volunteer Statement will be made available to CA DOJ upon its request and may be satisfied by signatures on the FBI CJIS Security Addendum Certification; and
- CLETS security controls are implemented solely by Subscribing Agency and solely through its operation of the CJIS Covered Services. Furthermore, Subscribing Agency agrees that Microsoft has met the minimum trainings and certifications necessary to provide the CJIS Covered Services. For purposes of clarity, CJIS Covered Services are not CLETS services.

Access to the CLETS is authorized to public law enforcement and criminal justice agencies only (hereinafter referred to as the CLETS subscribing agency), which may delegate the responsibility of performing the administration of criminal justice functions (e.g., dispatching functions or data processing/information services) in accordance with the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Addendum to a private contractor. The private contractor may access systems or networks that access the CLETS on behalf of the CLETS subscribing agency to accomplish the above-specified service(s). This Agreement must be received by the California Department of Justice (CA DOJ) prior to the subscribing agency permitting access to the CLETS. The performance of such delegated services does not convert that agency into a public criminal justice agency, nor automatically authorize access to state summary criminal history information. Information from the CLETS is confidential and may be used only for the purpose(s) for which it is authorized. Violation of confidentiality requirements or access authorizations may be subject to disciplinary action or criminal charges.

Pursuant to the policies outlined in the CLETS Policies, Practices and Procedures (PPP) and the FBI's CJIS Security Policy, it is agreed the CLETS subscribing agency will maintain responsibility for security control as it relates to the CLETS access. Security control is defined as the ability of the CLETS subscribing agency to set, maintain and enforce:

1. Standards for the selection, supervision and termination of personnel. This does not grant hiring/firing authority to the CLETS subscribing agency, only the authority to grant the CLETS systems access to personnel who meet these standards and deny it to those who do not; and
2. Policies governing the operation of computers, access devices, circuits, hubs, boundary protection devices and other components that make up and support a telecommunications network and related CA DOJ criminal justice databases used to process, store or transmit criminal justice information, guaranteeing the priority, integrity and availability of service needed by the criminal justice community.

Security control includes, but is not limited to, the supervision of applicable equipment, systems design, programming and operating procedures associated with the development, implementation and operation of any computerized message-switching or database systems utilized by the served law enforcement agency or agencies. Computer sites must have adequate physical security to protect against any unauthorized viewing or access to computer terminals, access devices or stored/printed data.

Additionally, it is the responsibility of the CLETS subscribing agency to ensure all private contractors receiving information from the CLETS meet the minimum training, certification and background requirements that are also imposed on the CLETS subscribing agency's staff. The minimum requirements are applicable also to staff having access to record storage areas containing information from the CLETS. The minimum requirements include, but are not limited to:

1. Prior to allowing the CLETS access, train, functionally test and affirm the proficiency of the CLETS computer operators to ensure compliance with the CLETS and the FBI's National Crime Information Center (NCIC) policies and regulations, if applicable. Biennially, provide retesting and reaffirm the proficiency of all the CLETS operators, if applicable;

2. State and FBI criminal offender record information searches must be conducted prior to allowing access to the CLETS computers, equipment or information. If the results of criminal offender record information search reveal a record of any kind, access will not be granted until the CLETS subscribing agency can review the matter to decide if access is appropriate. If a felony conviction of any kind is found, access shall not be granted; and

3. Each individual must sign an Employee/Volunteer Statement Form prior to operating or having access to the CLETS computers, equipment or information.

In accordance with the CLETS/NCIC policies, the CLETS subscribing agency has the responsibility and authority to monitor, audit and enforce the implementation of this agreement by the private contractor. The private contractor agrees to cooperate with the CLETS subscribing agency in the implementation of this agreement and to accomplish the directives for service under the provisions of this agreement. The Management Control Agreement shall be updated when the head of either agency changes or immediately upon request from the CA DOJ.

By signing this agreement, the vendors and private contractors certify they have read and are familiar with the contents of (1) the FBI's CJIS Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the FBI's CJIS Security Policy; (4) Title 28, Code of Federal Regulations, Part 20; and

(5) the CLETS PPP and agree to be bound by their provisions. Criminal offender record information and related data, by its very nature, is sensitive and has potential for great harm if misused. Access to criminal offender record information and related data is therefore limited to the purpose(s) for which the CLETS subscribing agency has entered into the contract. Misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or secondary dissemination of information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. Accessing the system for an appropriate purpose and then using, disseminating or secondary dissemination of information received for another purpose other than execution of the contract also constitutes misuse. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Contractor's signature on the Government Contract associated with the CJIS Amendment with Subscribing Agency, to which this Management Control Agreement is attached, shall constitute Microsoft's acceptance hereof.

The State's signature on the aforementioned Government Contract shall constitute Subscribing Agency's acceptance hereof, unless Subscribing Agency elects to sign separately where indicated below:

____
Signature (CLETS Subscribing Agency)

____
Print Name and Title

____
Date

Except for changes made by this CJIS Amendment, the Government Contract remains unchanged and in full force and effect. If there is any conflict between any provision in this CJIS Amendment and any provision in the Government Contract, the Government Contract's order of precedence section shall control.

Remainder of page intentionally left blank.

Amendment 2 to Exhibit 4
Microsoft IRS 1075 Amendment

This Microsoft Online Services IRS 1075 Amendment, including but not limited to the terms and conditions contained Appendix A to IRS 1075 Amendment, titled "Special Terms and Conditions to Safeguard Federal Tax Information") shall apply to CDT' (and its User Agencies') storage and processing of FTI in Microsoft's IRS 1075 Covered Services (as each such term is defined below), and is hereby added to the Government Contract (as defined in this Exhibit 4, above). The parties agree that this IRS 1075 Amendment supplements the Government Contract and applies to only the IRS 1075 Covered Services the State buys under the Government Contract.

---

1. Defined Terms

Capitalized terms used but not defined in this IRS 1075 Amendment will have the meanings provided in the Government Contract (including as applicable, the MS OST) or, if not defined in the Government Contract, in IRS Publication 1075. The following definitions are used in this IRS 1075 Amendment:

"IRS 1075 Covered Services" means the Azure Government Services listed as being in the scope for IRS 1075 at http://azure.microsoft.com/en-us/support/trust-center/compliance/irs1075/ or its successor site. Without limitation, IRS 1075 Covered Services to be purchased by the State under the Government Contract do not include any other Online Services.

"End User" means an individual that accesses the IRS 1075 Covered Services.

"FTI" is defined as in IRS Publication 1075.

"IRS Publication 1075" means the Internal Revenue Services (IRS) Publication 1075 effective January 1, 2014, including updates (if any) released by the IRS during the term of the Government Contract.

2. State Prerequisites

The State is responsible to ensure that the prerequisites established or required by IRS Publication 1075 are fulfilled prior to introducing FTI into the IRS 1075 Covered Services.

The State acknowledges that the IRS 1075 Covered Services ordered by the State under the Government Contract enable End Users optionally to access and use a variety of additional resources, applications, or services that are (a) provided by third parties, or (b) provided by Microsoft subject to their own terms of use or privacy policies (collectively, for convenience, "add-ons"), as described in services documentation and/or in the portal through which the State's administrator(s) will manage and configure the IRS 1075 Covered Services.

The State is responsible to review Online Services documentation, configure the services, and adopt and implement such policies and practices for its End Users' use of IRS 1075 Covered Services, together with any add-ons, as the State determines are appropriate in order for the State to comply with IRS Publication 1075 or other legal or regulatory requirements applicable to the State and not generally applicable to Microsoft as an IT service provider.

The State acknowledges that only IRS 1075 Covered Services will be delivered subject to the terms of this IRS 1075 Amendment. No other services are supported by the terms of this IRS 1075 Amendment. Without limiting the foregoing, data that the State elects to provide to the

Microsoft technical support organization (“Support Data”), if any, or data provided by or on behalf of the State to Microsoft’s billing or commerce systems in connection with purchasing/ordering IRS 1075 Covered Services (“Billing Data”), if any, is not subject to the provisions of this IRS 1075 Amendment. The State is solely responsible for ensuring that FTI is not provided as Support Data or Billing Data.

3. IRS Publication 1075 Special Terms.

3.1. IRS 1075 Covered Services. The IRS 1075 Covered Services are cloud services operated in a standardized manner with features and processes common across multiple customers. As part of the State’s preparation to use the services for FTI, the State should review applicable services documentation. The State’s compliance with IRS Publication 1075 will be dependent, in part, on the State’s configuration of the services and adoption and implementation of policies and practices for its End Users’ use of IRS 1075 Covered Services.

The State is solely responsible for determining the appropriate policies and practices needed for compliance with IRS Publication 1075.

Appendix A to this IRS 1075 Amendment contains the Safeguarding Contract Language for Technology Services specified by IRS Publication 1075. Microsoft and the State have agreed that certain requirements of the Safeguarding Contract Language and IRS Publication 1075 will be fulfilled as set forth in the remainder of this section 3.

3.2. Personnel Records and Training. Microsoft will maintain a list of screened personnel authorized to access Customer Data (that may include FTI) in the IRS 1075 Covered Services, which will be available to the State or to the IRS upon written request. The State will treat Microsoft personnel personally identifiable information (PII) as Microsoft trade secret or security-sensitive information exempt from public disclosure to the maximum extent permitted by applicable law, and, if required to provide such Microsoft personnel PII to the IRS, will require the IRS to treat such personnel PII the same.

3.3. Training Records. Microsoft will maintain security and disclosure awareness training records as required by IRS Publication 1075, which will be available to the State upon written request.

3.4. Confidentiality Statement. Microsoft will maintain a signed confidentiality statement, and will provide a copy for inspection upon request.

3.5 Cloud Computing Environment Requirements. The IRS 1075 Covered Services are provided in accordance with the FedRAMP System Security Plan for the applicable services. Microsoft’s compliance with controls required by IRS Publication 1075, including without limitation encryption and media sanitization controls, can be found in the applicable FedRAMP System Security Plan.

3.6. Use of Subcontractors. Notwithstanding anything to the contrary in Appendix A to this IRS 1075 Amendment, and as set forth in the OST, Microsoft may use subcontractors to provide services on its behalf. Any such subcontractors used in delivery of the IRS 1075 Covered Services will be permitted to obtain Customer Data (that may include FTI) only to deliver the services Microsoft has retained them to provide and will be prohibited from using Customer Data for any other purpose. Storage and processing of Customer Data in the IRS 1075 Covered Services is subject to Microsoft security controls at all times and, to the extent subcontractor personnel perform services in connection with IRS 1075 Covered Services, they are obligated to follow Microsoft's policies. Microsoft remains responsible for its subcontractors' compliance with Microsoft's obligations. Subject to the preceding, Microsoft may employ subcontractor personnel in the capacity of augmenting existing staff, and understands IRS Publication 1075 reference to employees to include employees and subcontractors acting in the manner specified herein. It is the responsibility of the State to gain approval of the IRS for the use of all subcontractors.

Microsoft maintains a list of subcontractor companies who may potentially provide personnel authorized to access Customer Data in the Online Services, published for Office 365 branded services at the Office 365 Trust Center Website (www.trustoffice365.com) and for Azure branded services at http://azure.microsoft.com/en-us/support/trust-center/, or successor locations identified by Microsoft. Microsoft will update these websites at least 14 days before authorizing any new subcontractor to access Customer Data, Microsoft will update the website and provide the State with a mechanism to obtain notice of that update.

3.7. Security Incident Notification. The Security Incident handling process defined in the Special Provisions and MS OST will apply to the IRS 1075 Covered Services. In addition, the parties agree to the following:

a. The State acknowledges that effective investigation or mitigation of a Security Incident may be dependent upon information or services configurations within the State's control. Accordingly, compliance with IRS Publication 1075 Incident Response requirements will be a joint obligation between Microsoft and the State.

b. If, subsequent to notification from Microsoft of a Security Incident, the State determines that FTI may have been subject to unauthorized inspection or disclosure, it is the State's responsibility to notify the appropriate Agent-in-Charge, TIGTA (Treasury Inspector General for Tax Administration) and/or the IRS of a Security Incident, or to notify impacted individuals, if the State determines this is required under IRS Publication 1075, other applicable law or regulation, or the State's internal policies.

3.8. State's Right to Inspect.

c. Audit by the State. The State will, (i) be provided quarterly access to information generated by Microsoft's regular monitoring of security, privacy, and operational controls in place to afford the State an ongoing view into the effectiveness of such controls, (ii) be provided a report mapping compliance of the IRS 1075 Covered Services with NIST 800-53 or successor controls, (iii) upon request, be afforded the opportunity to communicate with Microsoft's subject matter experts for clarification of the reports identified above, and (iv) upon request, and at The State's expense, be permitted to communicate with Microsoft's independent third party auditors involved in the preparation of audit reports. The State will use this information above to satisfy with any inspection requirements under IRS Publication 1075 and agree that the audit rights described in this section are in full satisfaction of any audit that may otherwise be requested by the State.

d. Confidentiality of Audit Materials. Audit information provided by Microsoft to the State will consist of highly confidential proprietary or trade secret information of Microsoft. Microsoft may request reasonable assurances, written or otherwise, that information will be maintained as confidential and/or trade secret information subject to this Agreement prior to providing such information to Agency, and Agency will ensure Microsoft's audit information is afforded the highest level of confidentiality available under applicable law.

This Section 3.8 is in addition to compliance information available to the State under the MS OST.

Appendix A to IRS 1075 Amendment

XXI. SPECIAL TERMS AND CONDITIONS TO SAFEGUARD FEDERAL TAX INFORMATION

In performance of its obligations to deliver the IRS 1075 Covered Services under the Government Contract, Microsoft agrees to comply with the requirements contained in Exhibit 7 (Safeguarding Contract Language for Technology Services) from IRS Publication 1075, as set forth below. For purposes of reconciling definition in this Appendix A with conflicting definitions in the Government Contract, "contractor" refers to Microsoft (also, the Service Provider), "agency" refers to the State, and "contract" refers to the Government Contract, inclusive of the IRS 1075 Amendment.

Federal statute, regulations and guidelines require that all contracts for services relating to the processing, storage, transmission, or reproduction of federal tax returns or return information, the programming, maintenance, repair, or testing of equipment or other property, or the providing of other services, for tax administration purposes include the provisions contained in this exhibit. (See 26 U.S.C. §6103(n); 26 C.F.R. §301.6103(n)-1(a)(2) and (d); Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies (Rev. 8-2010), Section 5.5 and Exhibit 7.)

The contractor agrees to comply with 26 U.S.C. §6103(n); 26 C.F.R. §301.6103(n)-1; IRS Publication 1075 (Rev. 8-2010); and all applicable conditions and restrictions as may be applicable. (See 26 C.F.R. §301.6103(n)-1(d); IRS Publication 1075 (Rev. 8-2010).)

XXII. I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the contractor or the contractor's employees.

(2) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(4) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(5) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(6) All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined in IRS Publication

1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal tax information.

(7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.

(8) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(9) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

XXIII. II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the

specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, *IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and* Exhibit 5, *IRC Sec. 7213 Unauthorized Disclosure of Information*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.[1]

XXIV. III. INSPECTION

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

XXV. REFERENCES

26 U.S.C. §6103(n)

Pursuant to regulations prescribed by the Secretary, returns and return information may be disclosed to any person, including any person described in section 7513 (a), to the extent necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other services, for purposes of tax administration.

26 C.F.R. §301.6103(n)-1 Disclosure of returns and return information in connection with procurement of property and services for tax administration purposes.

(a) *General rule.* Pursuant to the provisions of section 6103(n) of the Internal Revenue Code and subject to the requirements of paragraphs (b), (c), and (d) of this section, officers or employees of the Treasury Department, a State tax agency, the Social Security Administration, or the Department of Justice, are authorized to disclose returns and return information (as defined in section 6103(b)) to any person (including, in the case of the Treasury Department, any person described in section 7513(a)), or to an officer or employee of such person, to the extent necessary in connection with contractual procurement of—

(1) Equipment or other property, or

(2) Services relating to the processing, storage, transmission, or reproduction of such returns or return information, the programming, maintenance, repair, or testing of equipment or other property, or the providing of other services, for

[1] A 30 minute disclosure awareness training video produced by the IRS can be found at http://www.irsvideos.gov/Governments/Safeguards/DisclosureAwarenessTrainingPub4711

purposes of tax administration (as defined in section 6103(b)(4)).

No person, or officer or employee of such person, to whom a return or return information is disclosed by an officer or employee of the Treasury Department, the State tax agency, the Social Security Administration, or the Department of Justice, under the authority of this paragraph shall in turn disclose such return or return information for any purpose other than as described in this paragraph, and no such further disclosure for any such described purpose shall be made by such person, officer, or employee to anyone, other than another officer or employee of such person whose duties or responsibilities require such disclosure for a purpose described in this paragraph, without written approval by the Internal Revenue Service.

(b) *Limitations.* For purposes of paragraph (a) of this section, disclosure of returns or return information in connection with contractual procurement of property or services described in such paragraph will be treated as necessary only if such procurement or the performance of such services cannot otherwise be reasonably, properly, or economically carried out or performed without such disclosure.

Thus, for example, disclosures of returns or return information to employees of a contractor for purposes of programming, maintaining, repairing, or testing computer equipment used by the Internal Revenue Service or a State tax agency should be made only if such services cannot be reasonably, properly, or economically performed by use of information or other data in a form which does not identify a particular taxpayer. If, however, disclosure of returns or return information is in fact necessary in order for such employees to reasonably, properly, or economically perform the computer related services, such disclosures should be restricted to returns or return information selected or appearing at random. Further, for purposes of paragraph (a), disclosure of returns or return information in connection with the contractual procurement of property or services described in such paragraph should be made only to the extent necessary to reasonably, properly, or economically conduct such procurement activity. Thus, for example, if an activity described in paragraph (a) can be reasonably, properly, and economically conducted by disclosure of only parts or portions of a return or if deletion of taxpayer identity information (as defined in section 6103(b)(6) of the Code) reflected on a return would not seriously impair the ability of the contractor or his officers or employees to conduct the activity, then only such parts or portions of the return, or only the return with taxpayer identity information deleted, should be disclosed.

(c) *Notification requirements.* Persons to whom returns or return information is or may be disclosed as authorized by paragraph (a) of this section shall provide written notice to their officers or employees—

(1) That returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized by paragraph (a) of this section;

(2) That further inspection of any returns or return information for a purpose or to an extent unauthorized by paragraph (a) of this section constitutes a misdemeanor, punishable upon conviction by a fine of as much as $1,000, or imprisonment for as long as 1 year, or both, together with costs of prosecution;

(3) That further disclosure of any returns or return information for a purpose or

to an extent unauthorized by paragraph (a) of this section constitutes a felony, punishable upon conviction by a fine of as much as $5,000, or imprisonment for as long as 5 years, or both, together with the costs of prosecution;

(4) That any such unauthorized further inspection or disclosure of returns or return information may also result in an award of civil damages against any person who is not an officer or employee of the United States in an amount not less than $1,000 for each act of unauthorized inspection or disclosure or the sum of actual damages sustained by the plaintiff as a result of such unauthorized disclosure or inspection as well as an award of costs and reasonable attorneys fees; and

(5) If such person is an officer or employee of the United States, a conviction for an offense referenced in paragraph (c)(2) or (c)(3) of this section shall result in dismissal from office or discharge from employment.

(d) *Safeguards.* Any person to whom a return or return information is disclosed as authorized by paragraph (a) of this section shall comply with all applicable conditions and requirements which may be prescribed by the Internal Revenue Service for the purposes of protecting the confidentiality of returns and return information and preventing disclosures of returns or return information in a manner unauthorized by paragraph (a). The terms of any contract between the Treasury Department, a State tax agency, the Social Security Administration, or the Department of Justice, and a person pursuant to which a return or return information is or may be disclosed for a purpose described in paragraph (a) shall provide, or shall be amended to provide, that such person, and officers and employees of the person, shall comply with all such applicable conditions and restrictions as may be prescribed by the Service by regulation, published rules or procedures, or written communication to such person. If the Service determines that any person, or an officer or employee of any such person, to whom returns or return information has been disclosed as provided in paragraph (a) has failed to, or does not, satisfy such prescribed conditions or requirements, the Service may take such actions as are deemed necessary to ensure that such conditions or requirements are or will be satisfied, including—

(1) Suspension or termination of any duty or obligation arising under a contract with the Treasury Department referred to in this paragraph or suspension of disclosures by the Treasury Department otherwise authorized by paragraph (a) of this section, or

(2) Suspension of further disclosures of returns or return information by the Service to the State tax agency, or to the Department of Justice, until the Service determines that such conditions and requirements have been or will be satisfied.

(e) *Definitions.* For purposes of this section—

(1) The term *Treasury Department* includes the Internal Revenue Service and the Office of the Chief Counsel for the Internal Revenue Service;

(2) The term *State tax agency* means an agency, body, or commission described in section 6103(d) of the Code; and

(3) The term *Department of Justice* includes offices of the United States Attorneys.

IRS Publication 1075 (Rev. 8-2010) Section *5.5 Control over Processing*

Processing of FTI, in an electronic media format, including removable media, microfilms, photo impressions, or other formats (including tape reformatting or reproduction or conversion to punch cards, digital images or hard copy printout) will be performed pursuant to one of the following procedures:

5.5.1 Agency Owned and Operated Facility

Processing under this method will take place in a manner that will protect the confidentiality of the information on the electronic media. All safeguards outlined in this publication also must be followed and will be subject to IRS safeguard reviews.

5.5.2 Contractor or Agency Shared Facility – Consolidated Data Centers

Recipients of FTI are allowed to use a shared facility but only in a manner that does not allow access to FTI by employees, agents, representatives or contractors of other agencies using the shared facility.

Note: For purposes of applying sections 6103(l), (m) and (n), the term "agent" includes contractors. Access restrictions pursuant to the IRC authority by which the FTI is received continue to apply. For example, since human services agencies administering benefit eligibility programs may not allow contractor access to any FTI received, their data within the consolidated data center may not be accessed by any contractor of the data center.

The requirements in Exhibit 7, Contract Language for General Services, must be included in the contract in accordance with IRC Section 6103(n).

The contractor or agency-shared computer facility is also subject to IRS safeguard reviews.

Note: The above rules also apply to releasing electronic media to a private contractor or other agency office even if the purpose is merely to erase the old media for reuse.

Agencies utilizing consolidated data centers must implement appropriate controls to ensure the protection of FTI, including a service level agreement (SLA) between the agency authorized to receive FTI and the consolidated data center. The SLA should cover the following:

1. The consolidated data center is considered to be a "contractor" of the agency receiving FTI. The agency receiving FTI – whether it is a state revenue, workforce, child support enforcement or human services agency – is responsible for ensuring the protection of all FTI received. However, as the "contractor" for the agency receiving FTI, the consolidated data center shares responsibility for safeguarding FTI as well.

2. Provide written notification to the consolidated data center management that they are bound by the provisions of Publication 1075, relative to protecting all federal tax information within their possession or control. The SLA should also include details concerning the consolidated data center's responsibilities during a safeguard review and support required to resolve identified findings.

3. The agency will conduct an internal inspection of the consolidated data center every eighteen months (see section 6.3). Multiple agencies sharing a consolidated data center may partner together to conduct a single, comprehensive internal

inspection. However, care should be taken to ensure agency representatives do not gain unauthorized access to other agency's FTI during the internal inspection.

4. The employees from the consolidated data center with access to FTI, including system administrators and programmers, must receive disclosure awareness training prior to access to FTI and annually thereafter and sign a confidentiality statement. This provision also extends to any contractors hired by the consolidated data center that has access to FTI.

5. The specific data breach incident reporting procedures for all consolidated data center employees and contractors. The required disclosure awareness training must include a review of these procedures.

6. The Exhibit 7 language must be included in the contract between the recipient agency and the consolidated data center, including all contracts involving contractors hired by the consolidated data center.
7. Identify responsibilities for coordination of the 45-day notification of the use of contractors or sub-contractors with access to FTI.

Note: Generally, consolidated data centers are either operated by a separate state agency (example: Department of Information Services) or by a private contractor. If an agency is considering transitioning to either a state owned or private vendor consolidated data center, the Office of Safeguards strongly suggests the agency submit a request for discussions with Safeguards as early as possible in the decision-making or implementation planning process. The purpose of these discussions is to ensure the agency remains in compliance with safeguarding requirements during the transition to the consolidated data center.

26 U.S.C. §7213. Unauthorized disclosure of information

(a) Returns and return information

(1) Federal employees and other persons

It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)). Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) State and other employees

It shall be unlawful for any person (not described in paragraph (1)) willfully to disclose to any person, except as authorized in this title, any return or return information (as defined in section 6103(b)) acquired by him or another person under subsection (d), (i)(3)(B)(i) or (7)(A)(ii), (l)(6), (7), (8), (9), (10), (12), (15), (16), (19), or (20) or (m)(2), (4), (5), (6), or (7) of section 6103.

Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(3) Other persons

It shall be unlawful for any person to whom any return or return information (as defined in section 6103(b)) is disclosed in a manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(4) Solicitation

It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information (as defined in section 6103(b)) and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(5) Shareholders

It shall be unlawful for any person to whom a return or return information (as defined in section 6103(b)) is disclosed pursuant to the provisions of section 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not to exceed $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution.

(b) Disclosure of operations of manufacturer or producer

Any officer or employee of the United States who divulges or makes known in any manner whatever not provided by law to any person the operations, style of work, or apparatus of any manufacturer or producer visited by him in the discharge of his official duties shall be guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than $1,000, or imprisoned not more than 1 year, or both, together with the costs of prosecution; and the offender shall be dismissed from office or discharged from employment.

(c) Disclosures by certain delegates of Secretary

All provisions of law relating to the disclosure of information, and all provisions of law relating to penalties for unauthorized disclosure of information, which are applicable in respect of any function under this title when performed by an officer or employee of the Treasury Department are likewise applicable in respect of such function when performed by any person who is a "delegate" within the meaning of section 7701(a)(12)(B).

(d) Disclosure of software

Any person who willfully divulges or makes known software (as defined in section 7612(d)(1)) to any person in violation of section 7612 shall be guilty of a felony and, upon conviction thereof, shall be fined not more than $5,000, or imprisoned not more than 5 years, or both, together with the costs of prosecution.

(e) Cross references

(1) Penalties for disclosure of information by preparers of returns

For penalty for disclosure or use of information by preparers of returns, see section 7216.

(2) Penalties for disclosure of confidential information

For penalties for disclosure of confidential information by any officer or employee of the United States or any department or agency thereof, see 18 U.S.C. 1905.

26 U.S.C. §7213A. Unauthorized inspection of returns or return information

(a) Prohibitions
(1) Federal employees and other persons
It shall be unlawful for—
(A) any officer or employee of the United States, or
(B) any person described in subsection (l)(18) or (n) of section 6103 or an officer or employee of any such person,
willfully to inspect, except as authorized in this title, any return or return information.
(2) State and other employees
It shall be unlawful for any person (not described in paragraph (1)) willfully to inspect, except as authorized in this title, any return or return information acquired by such person or another person under a provision of section 6103 referred to in section 7213 (a)(2) or under section 6104 (c).
(b) Penalty
(1) In general
Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1,000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.
(2) Federal officers or employees
An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) Definitions
For purposes of this section, the terms “inspect”, “return”, and “return information” have the respective meanings given such terms by section 6103 (b).

26 U.S.C. §7431. Civil damages for unauthorized inspection or disclosure of returns and return information

(a) In general

(1) Inspection or disclosure by employee of United States

If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) Inspection or disclosure by a person who is not an employee of United States

If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) Exceptions

No liability shall arise under this section with respect to any inspection or disclosure -

(1) which results from a good faith, but erroneous, interpretation of section 6103, or

(2) which is requested by the taxpayer.

(c) Damages

In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of -

(1) the greater of -

(A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of -

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the costs of the action, plus

(3) in the case of a plaintiff which is described in section 7430(c)(4)(A)(ii), reasonable attorneys fees, except that if the defendant is the United States, reasonable attorneys fees may be awarded only if the plaintiff is the prevailing party (as determined under section 7430(c)(4)).

(d) Period for bringing action

Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

(e) Notification of unlawful inspection and disclosure

If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of -

(1) paragraph (1) or (2) of section 7213(a),

(2) section 7213A(a), or

(3) subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.

(f) Definitions

For purposes of this section, the terms "inspect", "inspection", "return", and "return information" have the respective meanings given such terms by section 6103(b).

(g) Extension to information obtained under section 3406

For purposes of this section -

(1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and

(2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in section 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103. For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 3406.

(h) Special rule for information obtained under section 6103(k)(9)

For purposes of this section, any reference to section 6103 shall be treated as including a reference to section 6311(e)

Exhibit 5 – Initial MS OST ("Locked OST" – see Section 1.c of Exhibit 1)

<Table of contents has been deleted>

Introduction

Beginning July 1, 2014 these Online Services Terms (OST) replace the Online Services Use Rights (OLSUR). The OST contains terms that apply to Customer's use of Online Services. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products (as defined below), as well as other products and services from Microsoft.

Most Online Services offer a Service Level Agreement (SLA). For more information regarding the Online Services SLAs, please refer to http://microsoft.com/licensing/contracts.

Prior Versions

The OST provides terms for Online Services that are currently available. For earlier versions Customer may refer to http://go.microsoft.com/?linkid=9840733 or contact its reseller or Microsoft Account Manager.

Clarifications and Summary of Changes

Additions	Deletions
Minecraft: Education Edition	

Privacy and Security Terms

Scope: The General Privacy and Security Terms now apply to the Parature, from Microsoft service.
Location of Customer Data at Rest: For Office 365 Services

1. OneDrive for Business has been added as a service where Customer Data at rest will be stored in the same Geo the tenant is provisioned, for the identified Geos; and
2. Canada has been added as a Geo where if a tenant is provisioned in Canada the Customer Data at rest will be stored in that Geo.

Attachment 2

Subscription License Suite: Skype for Business Online PSTN Conferencing has been added to the table.

Table of Contents / General Terms

General Terms

Customer may use the Online Services and related software as expressly permitted in Customer's volume licensing agreement. Microsoft reserves all other rights. Customer must acquire and assign the appropriate subscription licenses required for its use of each Online Service. Each user that accesses the Online Service must be assigned a User SL or access the Online Service only through a device that has been assigned a Device SL, unless specified otherwise in the Online Service-specific Terms. Attachment 2 describes SL Suites that also fulfill requirements for User SLs. Customer has no right to use an Online Service after the SL for that Online Service ends.

Definitions

If any of the terms below are not defined in Customer's volume licensing agreement, they have the definitions below.

"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service.

"External User" means a user of an Online Service that is not an employee, onsite contractor, or onsite agent of Customer or its Affiliates.

"Instance" means an image of software that is created by executing the software's setup or install procedure or by duplicating such an image.

“Licensed Device” means the single physical hardware system to which a license is assigned. For purposes of this definition, a hardware partition or blade is considered to be a separate device.

“Non-Microsoft Product” means any third-party-branded software, data, service, website or product.

“Online Service” means a Microsoft-hosted service to which Customer subscribes under a Microsoft volume licensing agreement, including any service identified in the Online Services section of the Product Terms. The Product Terms is located at http://go.microsoft.com/?linkid=9839207.

“Operating System Environment” (OSE) means all or part of an operating system Instance, or all or part of a virtual (or otherwise emulated) operating system Instance, that enables separate machine identity (primary computer name or similar unique identifier) or separate administrative rights, and Instances of applications, if any, configured to run on all or part of that operating system Instance. There are two types of OSEs, physical and virtual. A physical hardware system can have one physical OSE and/or one or more virtual OSEs. The operating system Instance used to run hardware virtualization software or to provide hardware virtualization services is considered part of the physical OSE.

“SL” means subscription license.

Online Services Terms Updates

When Customer renews or purchases a new subscription to an Online Service, the then-current OST will apply and will not change during Customer’s subscription for that Online Service. When Microsoft introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), Microsoft may provide terms or make updates to the OST that apply to Customer’s use of those new features, supplements or related software.

Online Services Changes and Availability

Microsoft may make commercially reasonable changes to each Online Service from time to time. Microsoft may terminate an Online Service in any country where Microsoft is subject to a government regulation, obligation or other requirement that is not generally applicable to businesses operating there. Availability, functionality, and language versions for each Online Service may vary by country. For information on availability, Customer may refer to www.microsoft.com/online/international-availability.aspx.

Data Retention

At all times during the term of Customer’s subscription, Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer’s subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer’s account and delete the Customer Data.

The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data as described in this section.

Use of Software with the Online Service

Customer may need to install certain Microsoft software in order to use the Online Service. If so, the following terms apply:

Microsoft Software License Terms

Customer may install and use the software only for use with the Online Service. The Online Service-specific Terms may limit the number of copies of the software Customer may use or the number of devices on which Customer may use it. Customer’s right to use the software begins when the Online Service is activated and ends when Customer’s right to use the Online Service ends. Customer must uninstall the software when Customer’s right to use it ends. Microsoft may disable it at that time.

Validation, Automatic Updates, and Collection for Software

Microsoft may automatically check the version of any of its software. Devices on which the software is installed may periodically provide information to enable Microsoft to verify that the software is properly licensed. This information includes the software version, the end user’s user account, product ID information, a machine ID, and the internet protocol address of the device. If the software is not properly licensed, its functionality will be affected. Customer may only obtain updates or upgrades for the software from Microsoft or authorized sources. By using the software, Customer consents to the transmission of the information described in this section. Microsoft may recommend or download to Customer's devices updates or supplements to this software, with or without notice. Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications) ("Apps"). The Apps may collect data about the use and performance of the Apps, which may be transmitted to Microsoft and used for the purposes described in this OST.

Third-party Software Components

The software may contain third party software components. Unless otherwise disclosed in that software, Microsoft, not the third party, licenses these components to Customer under Microsoft's license terms and notices.

Non-Microsoft Products

Microsoft may make Non-Microsoft Products available to Customer through Customer's use of the Online Services (such as through a store or gallery). If Customer installs or uses any Non-Microsoft Product with an Online Service, Customer may not do so in any way that would subject Microsoft's intellectual property or technology to obligations beyond those expressly included in Customer's volume licensing agreement. For Customer's convenience, Microsoft may include charges for the Non-Microsoft Product as part of Customer's bill for Online Services. Microsoft, however, assumes no responsibility or liability whatsoever for the Non-Microsoft Product. Customer is solely responsible for any Non-Microsoft Product that it installs or uses with an Online Service.

Acceptable Use Policy

Neither Customer, nor those that access an Online Service through Customer, may use an Online Service:

- in a way prohibited by law, regulation, governmental order or decree;
- to violate the rights of others;
- to try to gain unauthorized access to or disrupt any service, device, data, account or network;
- to spam or distribute malware;
- in a way that could harm the Online Service or impair anyone else's use of it; or
- in any application or situation where failure of the Online Service could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage.

Violation of the terms in this section may result in suspension of the Online Service. Microsoft will suspend the Online Service only to the extent reasonably necessary. Unless Microsoft believes an immediate suspension is required, Microsoft will provide reasonable notice before suspending an Online Service.

Technical Limitations

Customer must comply with, and may not work around, any technical limitations in an Online Service that only allow Customer to use it in certain ways. Customer may not download or otherwise remove copies of software or source code from an Online Service except as explicitly authorized.

Compliance with Laws

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 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.

Customer must comply with all laws and regulations applicable to its use of Online Services, including laws related to privacy, data protection and confidentiality of communications. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer's virtual machine or application), and for determining whether the Online Services are appropriate for storage and processing of information subject to any specific law or regulation. Customer is responsible for responding to any request from a third party regarding Customer's use of an Online Service, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

Import/Export Services

Customer’s use of any Import/Export Service is conditioned upon its compliance with all instructions provided by Microsoft regarding the preparation, treatment and shipment of physical media containing its data (“storage media”). Customer is solely responsible for ensuring the storage media and data are provided in compliance with all laws and regulations. Microsoft has no duty with respect to the storage media and no liability for lost, damaged or destroyed storage media. All storage media shipped to Microsoft must be shipped DAP Microsoft DCS Data Center (INCOTERMS 2010). Storage media shipped to Customer will be shipped DAP Customer Dock (INCOTERMS 2010).

Electronic Notices

Microsoft may provide Customer with information and notices about Online Services electronically, including via email, through the portal for the Online Service, or through a web site that Microsoft identifies. Notice is given as of the date it is made available by Microsoft.

License Reassignment

Most, but not all, SLs may be reassigned. Except as permitted in this paragraph or in the Online Service-specific Terms, Customer may not reassign an SL on a short-term basis (i.e., within 90 days of the last assignment). Customer may reassign an SL on a short-term basis to cover a user’s absence or the unavailability of a device that is out of service. Reassignment of an SL for any other purpose must be permanent. When Customer reassigns an SL from one device or user to another, Customer must block access and remove any related software from the former device or from the former user’s device.

Font Components

While Customer uses an Online Service, Customer may use the fonts installed by that Online Service to display and print content. Customer may only embed fonts in content as permitted by the embedding restrictions in the fonts and temporarily download them to a printer or other output device to print content.

Multiplexing

Hardware or software that Customer uses to pool connections; reroute information; reduce the number of devices or users that directly access or use the Online Service (or related software); or reduce the number of OSEs, devices or users the Online Service directly manages (sometimes referred to as “multiplexing” or “pooling”) does not reduce the number of licenses of any type (including SLs) that Customer needs.

XXVI. PRIVACY AND SECURITY TERMS

This section of the Online Services Terms has two parts:

- General Privacy and Security Terms, which apply to all Online Services; and
- Data Processing Terms, which are additional commitments for certain Online Services.

General Privacy and Security Terms

Scope

The terms in this section apply to all Online Services except Bing Maps Enterprise Platform, Bing Maps Mobile Asset Management Platform, and Translator API, which are governed by the privacy and/or security terms referenced below in the applicable Online Service-specific Terms.

Use of Customer Data

Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer. This paragraph does not affect Microsoft’s rights in software or services Microsoft licenses to Customer.

Disclosure of Customer Data

Microsoft will not disclose Customer Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in the OST, or (3) as required by law.

Microsoft will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third party request for Customer Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.

Microsoft will not provide any third party: (a) direct, indirect, blanket or unfettered access to Customer Data; (b) platform encryption keys used to secure Customer Data or the ability to break such encryption; or (c) access to Customer Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide Customer's basic contact information to the third party.

Educational Institutions

If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA) apply, Microsoft acknowledges that for the purposes of the OST, Microsoft is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials.

Customer understands that Microsoft may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Microsoft to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Microsoft's possession as may be required under applicable law.

HIPAA Business Associate

If Customer 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, execution of Customer's volume licensing agreement includes execution of the HIPAA Business Associate Agreement ("BAA"), the full text of which identifies the Online Services to which it applies and is available at http://aka.ms/BAA. Customer may opt out of the BAA by sending the following information to Microsoft in a written notice (under the terms of the Customer's volume licensing agreement):

- the full legal name of the Customer and any Affiliate that is opting out;
- if Customer has multiple volume licensing agreements, the volume licensing agreement to which the opt out applies.

Security

Microsoft is committed to helping protect the security of Customer's information. Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

Security Incident Notification

If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident;
(2) investigate the Security Incident and provide Customer 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 Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer'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.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

Location of Data Processing

Except as described elsewhere in the OST, Customer Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its affiliates or subcontractors maintain facilities. Customer appoints Microsoft to perform any such transfer of Customer Data to any such country and to store and process Customer Data in order to provide the Online Services. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of personal data from the European Economic Area and Switzerland.

Preview Releases

Microsoft may offer preview, beta or other pre-release features, data center locations, and services ("Previews") for optional evaluation. Previews may employ lesser or different privacy and security measures than those typically present in the Online Services. Unless otherwise provided, Previews are not included in the SLA for the corresponding Online Service.

Use of Subcontractors

Microsoft may hire subcontractors to provide services on its behalf. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services Microsoft has retained them to provide and will be prohibited from using Customer Data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with Microsoft's obligations in the OST. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the OST.

How to Contact Microsoft

If Customer believes that Microsoft is not adhering to its privacy or security commitments, Customer may contact customer support or use Microsoft's Privacy web form, located at http://go.microsoft.com/?linkid=9846224. Microsoft's mailing address is:

Microsoft Enterprise Service Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited is Microsoft's data protection representative for the European Economic Area and Switzerland. The privacy representative of Microsoft Ireland Operations Limited can be reached at the following address:

Microsoft Ireland Operations, Ltd.
Attn: Data Protection
Carmenhall Road
Sandyford, Dublin 18, Ireland

Table of Contents / General Terms

Data Processing Terms

The Data Processing Terms (DPT) include the terms in this section.

The Data Processing Terms also include the "Standard Contractual Clauses," pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the EU Data Protection Directive. The Standard Contractual Clauses are in Attachment 3. In addition,

- Execution of the volume licensing agreement includes execution of Attachment 3, which is countersigned by Microsoft Corporation;
- The terms in Customer's volume licensing agreement, including the DPT, constitute a data processing agreement under which Microsoft is the data processor; and
- The DPT control over any inconsistent or conflicting provision in Customer's volume licensing agreement and, for each subscription, will remain in full force and effect until all of the related Customer Data is deleted from Microsoft's systems in accordance with the DPT.

Customer may opt out of the "Standard Contractual Clauses" or the Data Processing Terms in their entirety. To opt out, Customer must send the following information to Microsoft in a written notice (under terms of the Customer's volume licensing agreement):

- the full legal name of the Customer and any Affiliate that is opting out;
- if Customer has multiple volume licensing agreements, the volume licensing agreement to which the Opt Out applies;
- if opting out of the entire DPT, a statement that Customer (or Affiliate) opts out of the entirety of the Data Processing Terms; and
- if opting out of only the Standard Contractual Clauses, a statement that Customer (or Affiliate) opts out of the Standard Contractual Clauses only.

In countries where regulatory approval is required for use of the Standard Contractual Clauses, the Standard Contractual Clauses cannot be relied upon under European Commission 2010/87/EU (of February 2010) to legitimize export of data from the country, unless Customer has the required regulatory approval.

In the DPT, the term "Online Services" applies only to the services in the table below, excluding any Previews, and "Customer Data" includes only Customer Data that is provided through use of those Online Services.

Online Services	
Microsoft Dynamics Online Services	The following services: Microsoft Dynamics CRM Online, Microsoft Dynamics Marketing, and Microsoft Social Engagement. Microsoft Dynamics Online Services do not include (1) Microsoft Dynamics CRM for supported devices, which includes but is not limited to Microsoft Dynamics CRM Online services for tablets and/or smartphones; or (2) any other separately-branded service made available with or connected to Microsoft Dynamics CRM Online, Microsoft Dynamics Marketing, or Microsoft Social Engagement.
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, Office 365 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	Active Directory, API Management, App Services (API Apps, Mobile Apps, Web Apps, Automation, Backup, Batch, BizTalk Services, Cloud Services, DocumentDB, Event Hubs, Express Route, HDInsight, Key Vault, Load Balancer, Machine Learning, Management Portal, Media Services, Multi-Factor Authentication, Notification Hub, Operational Insights, Redis Cache, RemoteApp, Rights Management Service, Scheduler, Service Bus, Site Recovery, SQL Database, Storage, StorSimple, Stream Analytics, Traffic Manager, Virtual Machines, Virtual Network, Visual Studio Team Services, and Workflow Manager.
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.
Microsoft Power BI Services	The cloud service portion of Microsoft Power BI offered as a standalone service or as included in an Office 365-branded plan or suite, but excluding data catalog functionality, the Power BI mobile applications, or Power BI Desktop.

Location of Customer Data at Rest

Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as follows:

- **Office 365 Services.** If Customer provisions its tenant in Australia, Canada, the European Union, India, Japan or the United States (each of the foregoing a Geo), Microsoft will store the following Customer Data at rest only within that

Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site and (3) files uploaded to OneDrive for Business.

- **Microsoft Intune Online Services**. When Customer provisions a tenant account, Customer selects an available Geo where Customer Data at rest will be stored. Microsoft will not transfer the Customer Data outside of Customer's selected Geo except as noted in the "Data Location" section of the Microsoft Intune Trust Center.
- **Microsoft Power BI**. If Customer provisions its tenant in Australia, the European Union, or the United States, Microsoft will store Microsoft Power BI Customer Data at rest only within that Geo.
- **Microsoft Azure Core Services**. If Customer configures a particular service to be deployed within a Geo then, for that service, Microsoft will store Customer Data at rest within the specified Geo. Certain services may not enable Customer to configure deployment in a particular Geo or outside the United States and may store backups in other locations, as detailed in the Microsoft Azure Trust Center (which Microsoft may update from time to time, but Microsoft will not add exceptions for existing Services in general release).
- **Microsoft Dynamics CRM Online**. For entities managed by the Microsoft Dynamics CRM Online Service, if Customer provisions its instance in the United States or the EU, Microsoft will store Customer Data at rest in the United States or the EU, as applicable.

Microsoft does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

Privacy

- **Customer Data Deletion or Return**. No more than 180 days after expiration or termination of Customer's use of an Online Service, Microsoft will disable the account and delete Customer Data from the account.
- **Transfer of Customer Data**. Unless Customer has opted out of the Standard Contractual Clauses, all transfers of Customer Data out of the European Union, European Economic Area, and Switzerland shall be governed by the Standard Contractual Clauses. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of personal data from the European Economic Area and Switzerland.
- **Microsoft Personnel**. Microsoft personnel will not process Customer Data without authorization from Customer. Microsoft personnel are obligated to maintain the security and secrecy of any Customer Data as provided in the DPT and this obligation continues even after their engagements end.
- **Subcontractor Transfer**. Microsoft may hire subcontractors to provide certain limited or ancillary services on its behalf. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the DPT. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the DPT. Except as set forth in the DPT, or as Customer may otherwise authorize, Microsoft will not transfer to any third party (not even for storage purposes) personal data Customer provides to Microsoft through the use of the Online Services. Each Online Service has a website that lists subcontractors that are authorized to access Customer Data as well as the limited or ancillary services they provide. At least 14 days before authorizing any new subcontractor to access Customer Data, Microsoft will update the applicable website and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent Customer invoices.

Additional European Terms.

These Additional European Terms apply only if Customer has end users in the European Economic Area ("EEA") or Switzerland.

- **End Users in EEA or Switzerland**. Terms used in the DPT that are not specifically defined will have the meaning in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "EU Data Protection Directive").
- **Intent of the Parties**. For the Online Services, Microsoft is a data processor (or sub-processor) acting on Customer's behalf. As data processor (or sub-processor), Microsoft will only act upon Customer's instructions. The

OST and Customer's volume licensing agreement (including the terms and conditions incorporated by reference therein), along with Customer's use and configuration of features in the Online Services, are Customer's complete and final instructions to Microsoft for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's volume licensing agreement.

- **Duration and Object of Data Processing**. The duration of data processing shall be for the term designated under Customer's volume licensing agreement. The objective of the data processing is the performance of the Online Services.
- **Scope and Purpose of Data Processing**. The scope and purpose of processing of Customer Data, including any personal data included in the Customer Data, is described in the DPT and Customer's volume licensing agreement.
- **Customer Data Access**. For the term designated under Customer's volume licensing agreement Microsoft will, at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide Customer with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on Customer's behalf.

Security

- **General Practices**. Microsoft has implemented and will maintain and follow for the Online Services the following security measures, which, in conjunction with the security commitments in the OST, are Microsoft's only responsibility with respect to the security of Customer Data.

Domain	Practices
Organization of Information Security	**Security Ownership**. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. Microsoft personnel with access to Customer Data are subject to confidentiality obligations. **Risk Management Program**. Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory**. Microsoft maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. **Asset Handling** - Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities.
Human Resources Security	**Security Training**. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals. **Physical Access to Components**. Microsoft maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain. **Protection from Disruptions**. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

Domain	Practices
	Component Disposal. Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered. - Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. - Microsoft has specific procedures in place governing access to copies of Customer Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services , which are reviewed every twelve months. - Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries** - Microsoft encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. - Microsoft restricts access to Customer Data in media leaving its facilities. **Event Logging**. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Microsoft ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data when needed. - Microsoft restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended.

Domain	Practices
	- Microsoft stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without unreasonable delay and, in any event, within 30 calendar days. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data are located. - Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

Online Services Information Security Policy

Each Online Service follows a written data security policy ("Information Security Policy") that complies with the control standards and frameworks shown in the table below.

Online 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 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

Online 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
Microsoft Power BI Services	Yes	Yes	Yes	No	No

**Does not include Microsoft Dynamics Marketing or Microsoft Social Engagement.*
***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 Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.

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

If the Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses.

Microsoft Audits of Online Services

For each Online 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 Online 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 Customer requests, Microsoft will provide Customer with each Microsoft Audit Report so that Customer 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.

If the Standard Contractual Clauses apply, then (1) Customer agrees to exercise its audit right by instructing Microsoft to execute the audit as described in this section of the DPT, and (2) if Customer desires to change this instruction, then Customer has the right to do so as set forth in the Standard Contractual Clauses, which shall be requested in writing.

If the Standard Contractual Clauses apply, then nothing in this section of the DPT varies or modifies the Standard Contractual Clauses or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses. Microsoft Corporation is an intended third-party beneficiary of this section.

Online Service Specific Terms

If an Online Service is not listed below, it does not have any Online Service-specific terms.

Microsoft Azure Services

Notices

The Bing Maps, Professional Services, Azure Media Services H.265/HEV Encoding, and H.264/AVC Visual Standard, VC-1 Video Standard, and MPEG-4 Part 2 Visual Standard and MPEG-2 Video Standard Notices in Attachment 1 apply.

Service Level Agreement

Refer to http://azure.microsoft.com/support/legal/sla/.

Definitions

"Azure Government Services" means one or more of the services or features Microsoft makes available to Customer as Government Community Cloud Services in the "US Gov" regions identified at http://azure.microsoft.com/en-us/regions/#services.

"Customer Solution" means an application or any set of applications that adds primary and significant functionality to the Microsoft Azure Services and that is not primarily a substitute for the Microsoft Azure Services.

"Microsoft Azure Services" means one or more of the Microsoft services and features identified at http://azure.microsoft.com/services/, except where identified as licensed separately.

Limitations

Customer may not

- resell or redistribute the Microsoft Azure Services, or
- allow multiple users to directly or indirectly access any Microsoft Azure Service feature that is made available on a per user basis (e.g., Active Directory Premium). Specific reassignment terms applicable to a Microsoft Azure Service feature may be provided in supplemental documentation for that feature.

Retirement of Services or Features

Microsoft will provide Customer with 12 months' notice before removing any material feature or functionality or discontinuing a service, unless security, legal or system performance considerations require an expedited removal. This does not apply to Previews

Data Retention after Expiration or Termination

The expiration or termination of Customer's Online Service subscription will not change Customer's obligation to pay for hosting of Customer Data during any Extended Term.

Hosting Exception

Customer may create and maintain a Customer Solution and, despite anything to the contrary in Customer's volume licensing agreement, combine Microsoft Azure Services with Customer Data owned or licensed by Customer or a third party, to create a Customer Solution using the Microsoft Azure Service and the Customer Data together. Customer may permit third parties to access and use the Microsoft Azure Services in connection with the use of that Customer Solution. Customer is responsible for that use and for ensuring that these terms and the terms and conditions of Customer's volume licensing agreement are met by that use.

Use of Software within Microsoft Azure

For Microsoft software available within a Microsoft Azure Service, Microsoft grants Customer a limited license to use the software only within the Microsoft Azure Service.

Data Center Availability

Usage of data centers in certain regions may be restricted to Customers located in or near that region. For information on service availability by region, please refer to http://azure.microsoft.com/en-us/regions.

Sharing

The Microsoft Azure Services may provide the ability to share a Customer Solution and/or Customer Data with other Azure users and communities, or other third parties. If Customer chooses to engage in such sharing, Customer agrees that it is giving a license to all authorized users, including the rights to use, modify, and repost its Customer Solution and/or the Customer Data, and Customer is allowing Microsoft to make them available to such users in a manner and location of its choosing.

Marketplace

Microsoft Azure enables Customer to access or purchase Non-Microsoft Products through features such as the Microsoft Azure Marketplace and the Virtual Machine Gallery, subject to separate terms available at http://azure.microsoft.com/en-us/support/legal/store-terms.

Microsoft Azure StorSimple

StorSimple Monetary Commitment – 1 (8100 device)
StorSimple Monetary Commitment – 2 (8600 device)

Table of Contents / General Terms

Microsoft Cloud App Security

Cloud App Security (User SL)
Cloud App Security K (User SL)

Table of Contents / General Terms

Enterprise Mobility Suite

Notices

The Bing Maps Notices in Attachment 1 apply.

Subscription License Suites

In addition to User SLs, refer to Attachment 2 for other SLs that fulfill requirements for Azure Active Directory Premium (P1 and P2), Azure Rights Management, and Microsoft Intune.

Azure Active Directory Basic

Customer may, using Single Sign-On, pre-integrate up to 10 SAAS Applications/Custom Applications per User SL. All Microsoft as well as third party applications count towards this application limit.

Table of Contents / General Terms

Azure Active Directory Premium

Customer may, using Single Sign-On, pre-integrate SaaS Applications/Custom Applications. Customer may not copy or distribute any data set (or any portion of a data set) included in the Forefront Identity Manager software that is included with a Microsoft Azure Active Directory Premium (P1 and P2) User SL.

Table of Contents / General Terms

Azure Rights Management Premium

Notices

The Bing Maps Notices in Attachment 1 applies.
Any deployment services provided to Customer are subject to the Professional Services Notice in Attachment 1.

Table of Contents / General Terms

Azure RemoteApp

Table of Contents / General Terms

Microsoft Multifactor Authentication

Table of Contents / General Terms

Microsoft Intune

Microsoft Intune (per user)
Microsoft Intune Add-on for System Center Configuration
Windows Intune Add-on for System Center Configuration
Manager and System Center Endpoint Protection (per
user)
("Microsoft Intune Add-On")

Notices

Any deployment services provided to Customer are subject to the Professional Services Notice in Attachment 1.

Manage Devices

Each user to whom Customer assigns a User SL may access and use the Online Service and related software (including System Center software) to manage up to five devices.

Storage Add-on SL

A Storage Add-on SL is required for each gigabyte of storage in excess of the storage provided with the base subscription.

Windows Software Components in System Center Software

The System Center software includes one or more of the following Windows Software Components: Microsoft .NET Framework, Microsoft Data Access Components, Powershell software and certain .dlls related to Microsoft Build, Windows Identity Foundation, Windows Library for JAVAScript, Debghelp.dll, and Web Deploy technologies. The license terms governing use of the Windows Software Components are in the Windows 8.1 Pro and Enterprise section of the Product Terms. The Product Terms is located at http://go.microsoft.com/?linkid=9839206.

SQL Server Technology and Benchmarking

The Software included with the Online Service includes SQL Server-branded components other than a SQL Server Database. Those components are licensed to Customer under the terms of their respective licenses, which can be found in the installation directory or unified installer of the software. Customer must obtain Microsoft's prior written approval to disclose to a third party the results of any benchmark test of these components or the software that includes them.

Table of Contents / General Terms

Microsoft Dynamics Online Services

Notices

The Bing Maps and Professional Services Notices in Attachment 1 apply.

Subscription License Suites

In addition to User SLs, refer to Attachment 2 for other offerings that fulfill SL requirements

Microsoft Dynamics AX

Microsoft Dynamics AX Self-Serve
Microsoft Dynamics AX Task
Microsoft Dynamics AX Enterprise
Microsoft Dynamics AX Device

External Users

External Users of Microsoft Dynamics AX do not need an SL to access the Online Service. This exemption does not apply to contractors or agents of Customer or its Affiliates.

Modifications

Customer may modify Microsoft Dynamics AX to allow extension of its functionality, but only for Customer's internal use purposes.

Table of Contents / General Terms

Microsoft Dynamics CRM Online

Microsoft Dynamics CRM Online Essentials
Microsoft Dynamics CRM Online Basic
Microsoft Dynamics CRM Online Professional
Microsoft Dynamics CRM Online Enterprise
Microsoft Dynamics Employee Self Service

External Users

External Users of all editions of Microsoft Dynamics CRM Online and Parature, from Microsoft do not need an SL to access the Online Service unless using Microsoft Dynamics CRM clients. This exemption does not apply to contractors or agents of Customer or its Affiliate.

Table of Contents / General Terms

Microsoft Dynamics Marketing

Microsoft Dynamics Marketing Enterprise
Microsoft Dynamics Marketing Sales Collaboration

Service Level Agreement

There is no SLA for Microsoft Dynamics Marketing.

Web User Profile

Users configured and accessing this Online Service as Web Portal Users do not need User SLs.

Mobile Text Messaging

Customer will be solely responsible for the content, creation, initiation and transmittal of all mobile text messages facilitated by Microsoft and will comply with all applicable industry codes of conduct provided by Microsoft from time to time. Third party aggregators or carriers engaged in the transmittal of mobile text messages are not Microsoft subcontractors.

Table of Contents / General Terms

Microsoft Social Engagement

Microsoft Social Engagement Professional
Microsoft Social Engagement Enterprise

Service Level Agreement

There is no SLA for Microsoft Social Engagement.

Social Content Obtained through Microsoft Social Engagement

Social Content is publicly-available content collected from social media networks (such as Twitter, Facebook and YouTube) and data indexing or data aggregation services in response to Customer's search queries executed in Microsoft Social Engagement. Social Content is not Customer Data. Customer Data used in configuring or initiating search queries executed on Customer's behalf may be shared with third parties for purposes of collecting Social Content. Customer may use Social Content for its internal business purposes only. Microsoft reserves the right to:

- store Social Content in a database commingled with content aggregated from other sources by other licensees;
- access, edit or delete Social Content in response to a request from a social media network, data indexing or data aggregation service, Social Content owner or a takedown request under the Digital Millennium Copyright Act;
- instruct Customer to edit or delete Social Content, if Customer exports Social Content; and
- delete or restrict further access to Social Content after the Online Service has been terminated or expires.

Table of Contents / General Terms

Parature, from Microsoft

Parature Enterprise

Service Level Agreement

There is no SLA for Parature, from Microsoft.

Office 365 Services

Notices

The Bing Maps Notices in Attachment 1 apply. Any onboarding, migration, or deployment services provided to Customer are subject to the Professional Services Notice in Attachment 1.

Core Features for Office 365 Services

During the term of Customer's subscription, the Office 365 Services will substantially conform to the Core Features description provided (if any) in the Office 365 service-specific sections below, subject to Product restrictions or external factors (such as the recipient, message rate, message size and mailbox size limits for e-mail; default or Customer-imposed data retention policies; search limits; storage limits; Customer or end user configurations; and meeting capacity limits). Microsoft may permanently eliminate a functionality specified below only if it provides Customer a reasonable alternative functionality.

Administration Portal

Customer will be able to add and remove end users and domains, manage licenses, and create groups through the Microsoft Online Services Portal or its successor site.

Subscription License Suites

In addition to User SLs, refer to Attachment 2 for other SLs that fulfill requirements for Office 365 Services.

Exchange Online

Office 365 Advanced Threat Protection
Data Loss Prevention
Exchange Online Archiving for Exchange Online
Exchange Online Archiving for Exchange Server
Exchange Online Kiosk
Exchange Online Plan 1
Exchange Online Plan 2

Core Features for Office 365 Services – Exchange Online

Exchange Online or its successor service will have the following Core Features capabilities:

Emails

An end user will be able to send email messages, receive email messages that originate from within and outside of Customer's organization, and access the end user's mailbox.

Mobile and Web Browser Access

Through the Microsoft Exchange ActiveSync protocol or a successor protocol or technology, Exchange Online will enable an end user to send and receive emails and update and view calendars from a mobile device that adequately supports such a protocol or technology. An end user will be able to send email messages, receive email messages that originate from within and outside of Customer's organization, and access the end user's mailbox, all from within a compatible web browser.

Retention Policies

Customer will be able to establish archive and deletion policies for email messages.

Deleted Item and Mailbox Recovery

Customer will be able to recover the contents of a deleted non-shared mailbox and an end user will be able to recover an item that has been deleted from one of the end user's email folders.

Multi-Mailbox Search

Customer will be able to search for content across multiple mailboxes within its organization.

Calendar

An end user will be able to view a calendar and schedule appointments, meetings, and automatic replies to incoming email messages.

Contacts

Through an Exchange Online-provided user interface, Customer will be able to create and manage distribution groups and an organization-wide directory of mail-enabled end users, distribution groups, and external contacts.

Core Features for Office 365 Services – Exchange Online Archiving

Exchange Online Archiving or its successor service will have the following Core Features capabilities:

Storage

Customer will be able to allow an end user to store email messages.

Retention Policies

Customer will be able to establish archive and deletion policies for email messages distinct from policies that an end user can apply to the end user's own mailbox.

Deleted Item and Mailbox Recovery

Customer, through Office 365 support services, will be able to recover a deleted archive mailbox, and an end user will be able to recover an item that has been deleted from one of the end user's email folders in the end user's archive.

Multi-Mailbox Search

Customer will be able to search for content across multiple mailboxes within its organization.

Legal Hold

Customer will be able to place a "legal hold" on an end user's primary mailbox and archive mailbox to preserve the content of those mailboxes.

Archiving

Archiving may be used for messaging storage only with Exchange Online Plans 1 and 2.

Archiving for Exchange Server

Users licensed for Exchange Server 2013 Standard Client Access License may access the Exchange Server 2013 Enterprise Client Access License features necessary to support use of Exchange Online Archiving for Exchange Server.

Exchange Online Plan 2 from Exchange Hosted Archive Migration

Exchange Online Plan 2 is a successor Online Service to Exchange Hosted Archive. If Customer renews from Exchange Hosted Archive into Exchange Online Plan 2 and has not yet migrated to Exchange Online Plan 2, Customer's licensed users may continue to use the Exchange Hosted Archive service subject to the terms of the March 2011 Product Use Rights until the earlier of Customer's migration to Exchange Online Plan 2 or the expiration of Customer's Exchange Online Plan 2 User SLs. The Product Use Rights is located at http://go.microsoft.com/?linkid=9839206.

Data Loss Prevention Device License

If Customer is licensed for Data Loss Prevention by Device, all users of the Licensed Device are licensed for the Online Service.

Service Level Agreement

There is no SLA for Office 365 Advanced Threat Protection.

Table of Contents / General Terms

Office 365 Applications

Office 365 Business Office 365 ProPlus	Visio Pro for Office 365

Service Level Agreement

There is no SLA for Visio Pro for Office 365.

Installation and Use Rights

Each user to whom Customer assigns a User SL must have a Microsoft Account in order to use the software provided with the subscription. These users:

- may activate the software provided with the SL on up to five concurrent OSEs for local or remote use;
- may also install and use the software, with shared computer activation, on a shared device, a network server, or on shared servers with a qualified cloud partner. A list of qualified cloud partners and additional deployment requirements is available at www.office.com/sca. For the purpose of this use right "network server" means a physical hardware server solely dedicated to Customer use. This shared computer activation provision does not apply to Customers license for Office 365 Business; and
- must connect each device upon which user has installed the software to the Internet at least once every 30 days or the functionality of the software may be affected.

The following terms apply only to Office 365 Business and Office 365 ProPlus

Smartphone and Tablet Devices

Each user to whom Customer assigns a User SL may also activate Microsoft Office Mobile software to use on up to five smartphones and five tablets.

The following terms apply only to Office 365 ProPlus

Office Home & Student 2013 RT Commercial Use

Each User SL for Office 365 ProPlus modifies the user's right to use the software under a separately acquired Office Home & Student 2013 RT license by waiving the prohibition against commercial use. Except for this allowance for commercial use of the software, all use is subject to the terms and use rights provided with the Office Home & Student 2013 RT License.

Office Online Server

For each Office 365 ProPlus subscription, Customer may install any number of copies of Office Online Server on any Server dedicated to Customer's use. Each Office 365 ProPlus user may use the Office Online Server software. This provision does not apply to Customers that license this Product under the Microsoft Online Subscription Agreement or other Microsoft agreement that cover Online Services only.

Subscription License Suites

In addition to Office 365 ProPlus User SLs, Customer may fulfill the SL requirement for this Product by purchasing a Suite SL (refer Attachment 2).

Table of Contents / General Terms

Office 365 Delve Analytics

Service Level Agreement

There is no SLA for Office 365 Delve Analytics.

Table of Contents / General Terms

Office 365 Advanced eDiscovery

Service Level Agreement

There is no SLA for Office 365 Advanced eDiscovery.

Table of Contents / General Terms

Office Online

Core Features for Office 365 Services

Office Online or its successor service will have the following Core Features capabilities:
An end user will be able to create, view, and edit documents in Microsoft Word, Excel, PowerPoint, and OneNote file types that are supported by Office Online or its successor service.

External Users

External Users invited to site collections via Share-by-Mail functionality do not need User SLs with Office Online.

Table of Contents / General Terms

OneDrive for Business

External Users

External Users invited to site collections via Share-by-Mail functionality do not need User SLs with OneDrive for Business.

Table of Contents / General Terms

Project Online

Project Online Essentials
Project Online Professional
Project Online Premium

Installation and Use Rights for Project application

Each user to whom Customer assigns a Project Online Professional or Project Online Premium User SL must have a Microsoft Account in order to use the software provided with the subscription. These users:

- may activate the software provided with the SL on up to five concurrent OSEs for local or remote use;
- may also install and use the software, with shared computer activation, on a shared device, a network server, or on shared servers with a qualified cloud partner. A list of qualified cloud partners and additional deployment requirements is available at www.office.com/sca. For the purpose of this use right "network server" means a physical hardware server solely dedicated to Customer use; and
- must connect each device upon which user has installed the software to the Internet at least once every 30 days or the functionality of the software may be affected.

Table of Contents / General Terms

SharePoint Online

Duet Enterprise Online for Microsoft SharePoint and SAP
SharePoint Online Kiosk
SharePoint Online Plan 1
SharePoint Online Plan 2

Core Features for Office 365 Services

SharePoint Online or its successor service will have the following Core Features capabilities:

Collaboration Sites

An end user will be able to create a web browser-accessible site through which the end user can upload and share content and manage who has permission to access that site.

Storage

Customer will be able to set storage capacity limits for a site created by an end user.

External Users

External Users invited to site collections via Share-by-Mail functionality do not need User SLs with SharePoint Online Kiosk, Plan 1 and Plan 2.

Storage Add-on SLs

Office 365 Extra File Storage is required for each gigabyte of storage in excess of the storage provided with User SLs for SharePoint Online Plans 1 and 2.

Table of Contents / General Terms

Skype for Business Online

Skype for Business Online Plan 1 Skype for Business Online Plan 2	Skype for Business Online Cloud PBX

Notices

The H.264/MPEG-4 AVC and/or VC-1 Notices in Attachment 1 apply.

Core Features for Office 365 Services

Skype for Business Online Plan 1 and Plan 2or their successor services will have the following Core Features capabilities:

Instant Messaging

An end user will be able to transfer a text message to another end user in real time over an Internet Protocol network.

Presence

An end user will be able to set and display the end user’s availability and view another end user’s availability.

Online Meetings

An end user will be able to conduct an Internet-based meeting that has audio and video conferencing functionality with other end users.

External Users and users not authenticated by Skype for Business Online

User SLs are not required for External Users and users not authenticated by the Skype for Business Online service.

Table of Contents / General Terms

Skype for Business Online PSTN Services

Skype for Business Online PSTN Calling Skype for Business Online PSTN Conferencing	Skype for Business PSTN Consumption

PSTN Services

Skype for Business Online PSTN Services (“PSTN Services”) enable users to communicate with others via the worldwide voice telephone network known generally as the Public Switched Telephone Network. PSTN Services are provided by the Microsoft Affiliate authorized to provide them. Pricing for PSTN Services may include applicable taxes and fees. All included taxes and fees are disclosed on the Volume Licensing site (http://go.microsoft.com/fwlink/?LinkId=690247)

Important Information About Emergency Services

Customer must notify each user of Skype for Business Online PSTN Calling that Emergency Services operate differently than on traditional telephone services in the following ways: (i) Skype for Business may not know the actual location of an Emergency Services caller, which could result in the call being routed to the wrong Emergency Services call center and/or emergency services being dispatched to the wrong location; (ii) if the user’s device has no power, is experiencing a power outage or, for any reason, cannot otherwise access the Internet, the user cannot make an Emergency Services call through Skype for Business PSTN Calling services; and (iii) although Skype for Business Online PSTN Calling services can be used anywhere in the world where an Internet connection is available, users should not make an Emergency Services call from a location outside their home country because the call likely will not be routed to the appropriate call center in that location.

Limitations on use

Customer may not exceed the usage limitations for the applicable PSTN Service subscription plan. Doing so may result in suspension of the services. Microsoft will provide reasonable notice before suspending PSTN Services, and customer will be able to make emergency calls during any period of suspension.

Table of Contents / General Terms

Other Online Services

Bing Maps Enterprise Platform and Bing Maps Mobile Asset Management Platform

Service SLs

A Service SL is required to provide access to the services. Each Service SL must be purchased with at least one of the following qualifying Add-On SLs:

- a Website usage Add-On SL, which is required for unauthenticated users to access Bing Maps Enterprise Platform and Bing Maps Mobile Asset Management Platform through Customer's programs based on the number of billable transactions per month,
- a public website usage SL, which is available for a specified number of billable transactions for use on a website that is available publicly without restriction,
- an Internal Website Usage Add-on, which is available for a specified number of billable transactions for use on an internal website (e.g., intranet) on a private network,
- Bing Maps Platinum Add-on,
- Bing Maps Known User SL, or
- Bing Maps Light Known User SL.

Qualifying Bing Maps Mobile Asset Management Platform Service SL Add-on SLs

For the Bing Maps Mobile Asset Management Platform, an Add-on SL is required for each tracked Asset whose GPS or other sensor based position can be monitored, displayed, reverse geocoded or used to perform calculations using Bing Maps Mobile Asset Management Platform. "Asset" is defined as any vehicle, device or other mobile object. These Add-on SLs are for a specified number of tracked Assets.

Authenticated Users

Users that are authenticated by Customer's programs that access Bing Maps Enterprise Platform and Bing Maps Mobile Asset Management Platform must have a SL.

Bing Maps APIs

Customer may use all Bing Maps APIs in accordance with the Microsoft Bing Maps Platform API Terms of Use and Bing Maps Platform SDKs, including any successors thereto, located at http://go.microsoft.com/fwlink/p/?LinkID=66121 and http://go.microsoft.com/fwlink/p/?LinkID=223436.

Bing Maps Privacy

The Bing Privacy Statement and privacy terms in the Microsoft Bing Maps Platform API Terms of Use located at: http://go.microsoft.com/fwlink/?LinkID=248686 apply to Customer's use of the Bing Maps Services.

Table of Contents / General Terms

Microsoft Learning

Microsoft Learning E-Reference Library

Any person that has valid access to Customer's computer or internal network may copy and use the documentation for Customer's internal reference purposes. Documentation does not include electronic books.

Microsoft Learning Imagine Academy Service SL

A Service SL is required for each Location that accesses or uses any Microsoft Imagine Academy service or benefit. Location is defined as a physical site with staff under the same administrator, such as a principal, in a single building or group of buildings located on the same campus.

Microsoft Learning Imagine Academy Program Guidelines

The Imagine Academy program guidelines, located at http://www.microsoft.com/itacademy, apply to Customer's use of the Microsoft Learning Imagine Academy and its benefits.

Microsoft Learning Imagine Academy Program Benefits Provided by Third-Party

Program benefits may only be used by a licensed institution's faculty, staff and students currently enrolled in the licensed institution.

Table of Contents / General Terms

Microsoft Power BI Pro

Notices

The Bing Maps Notices in Attachment 1 apply.

Table of Contents / General Terms

Minecraft: Education Edition

Notices

The Bing Maps Notices in Attachment 1 apply.

Table of Contents / General Terms

Office 365 Developer

No Production Use of Office 365 Developer

Each user to whom Customer assigns a User SL may use the Online Service to design, develop, and test Customer's applications to make them available for Customer's Office 365 Online Services, on-premises deployments or for the Microsoft Office Store. The Online Service is not licensed for production use.

Office 365 Developer End Users

Customer's end users do not need a SL to access Office 365 Developer to perform acceptance tests or provide feedback on Customer programs.

Table of Contents / General Terms

Translator API

Customer may use Translator API in accordance with the Translator API Terms of Use, including successor Terms, located at http://aka.ms/translatortou and the Translator Privacy Statement located at http://aka.ms/translatorprivacy.

Table of Contents / General Terms

Windows Desktop Operating System

Data Retention

The Windows Defender Advanced Threat Protection portion of the product does not contain extractable Customer Data therefore the Customer Data extraction terms in the OST do not apply.

Table of Contents / General Terms

Yammer Enterprise

Notices

Any onboarding, migration, or deployment services provided to Customer are subject to the Professional Services Notice in Attachment 1

External Users

External Users invited to Yammer via external network functionality do not need User SLs.

Table of Contents / General Terms

Attachment 1 – Notices

Bing Maps

The Online Service or its included software includes use of Bing Maps. Any content provided through Bing Maps, including geocodes, can only be used within the product through which the content is provided. Customer's use of Bing Maps is governed by the Bing Maps End User Terms of Use available at go.microsoft.com/?linkid=9710837 and the Bing Maps Privacy Statement available at go.microsoft.com/fwlink/?LinkID=248686.

Table of Contents / General Terms

Professional Services

Customer may be eligible for Microsoft customer support and consulting services related to this Online Service. These services are "Professional Services" under Customer's volume licensing agreement. If Customer's volume licensing agreement covers Online Services only (and does not define Professional Services), then these services are provided subject to the "Professional Services Terms" below.

The Professional Services to which this Notice applies are not Online Services, and the rest of the Online Services Terms, as well as any data processing amendment or HIPAA Business Associate Agreement signed by the parties, do not apply. Any information provided to Microsoft in connection with these Professional Services is protected under the confidentiality terms of Customer's volume licensing agreement.

Additional terms may apply to these Professional Services, but only to the extent those terms don't conflict with this Notice.

Professional Services Terms

Definition

Any services to which this notice applies are defined, collectively, as "Professional Services".

Obligations of the Parties

Microsoft warrants that all Professional Services will be performed with professional care and skill. If Microsoft fails to do so and Customer notifies Microsoft within 90 days of the date of performance, then Microsoft will either re-perform the Professional Services or return the price paid for them as Customer's sole remedy for breach of the Professional Services warranty.

Customer will perform its applicable responsibilities and obligations to support Microsoft's performance of the Professional Services, as specified in the description of each Professional Service.

Limitation of Liability

To the extent permitted by applicable law, each party's total liability for all claims relating to Professional Services will be limited to the amounts Customer was required to pay for the Professional Services or the limitation of liability for the Online Service with which the Professional Services are offered, whichever is greater. **In no event will either party be liable for indirect, incidental, special, punitive, or consequential damages, including loss of use, loss of profits, or interruption of business, however caused or on any theory of liability in relation to the Professional Services. No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations; or (2) violation of the other party's intellectual property rights.**

Fixes

"Fixes" are Product fixes, modifications or enhancements, or their derivatives, that Microsoft either releases generally (such as service packs) or that Microsoft provides to Customer to address a specific issue. Each Fix, is licensed under the same terms as the Product to which it applies. If a Fix is not provided for a specific Product, any use terms Microsoft provides with the Fix will apply.

Pre-Existing Work

"Pre-Existing Work" means any computer code or non-code based written materials developed or otherwise obtained independent of Customer's volume licensing agreement. All rights in Pre-Existing Work shall remain the sole property of the party providing the Pre-Existing Work. Each party may use, reproduce and modify the other party's Pre-Existing Work only as needed to perform obligations related to Professional Services.

Services Deliverables

"Services Deliverables" means any computer code or materials other than Products or Fixes that Microsoft leaves with Customer at the conclusion of Microsoft's performance of Professional Services. Microsoft grants Customer a non-exclusive, non-transferable, perpetual license to reproduce, use, and modify the Services Deliverables solely for Customer's internal business purposes, subject to the terms and conditions in Customer's volume licensing agreement.

Non-Microsoft Technology

Customer is solely responsible for any non-Microsoft software or technology that it installs or uses with the Online Services, Fixes, or Services Deliverables.

Affiliates' Rights

Customer may sublicense the rights to use Services Deliverables to its Affiliates, but Customer's Affiliates may not sublicense these rights. Customer is liable for ensuring its Affiliates' compliance with the terms of this Notice and Customer's volume licensing agreement.

Government Customers.

If Customer is a government entity, then the following terms apply to any Professional Services provided at no charge to Customer. Microsoft waives any and all entitlement to compensation from Customer for the Professional Services. In compliance with applicable laws and regulations, Microsoft and Customer acknowledge that the Professional Services are for the sole benefit and use of Customer and not provided for the personal use or benefit of any individual government employee.

Table of Contents / General Terms

Notice about Azure Media Services H.265/HEVC Encoding

Customer must obtain its own patent license(s) from any third party H.265/HEVC patent pools or rights holders before using Azure Media Services to encode or decode H.265/HEVC media.

Table of Contents / General Terms

Notice about H.264/AVC Visual Standard, VC-1 Video Standard, MPEG-4 Part Visual Standard and MPEG-2 Video Standard

This software may include H.264/AVC, VC-1, MPEG-4 Part 2, and MPEG-2 visual compression technology. MPEG LA, L.L.C. requires this notice:
THIS PRODUCT IS LICENSED UNDER THE AVC, THE VC-1, THE MPEG-4 PART 2 AND MPEG-2 VISUAL PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE (VIDEO STANDARDS) AND/OR (ii) DECODE AVC, VC-1, MPEG-4 PART 2 AND MPEG-2 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. REFER TO www.mpegla.com.

For clarification purposes, this notice does not limit or inhibit the use of the software for normal business uses that are personal to that business which do not include (i) redistribution of the software to third parties, or (ii) creation of content compliant with the VIDEO STANDARDS technologies for distribution to third parties.

Table of Contents / General Terms

Attachment 2 – Subscription License Suites

Online Services may be available for purchase as Suites of Online Services. If, in the table below, a cell is shaded blue in an Online Service's row, the Suite SL for the column the cell is in fulfills the SL requirements for the cell's Online Services.

	Office 365 Enterprise [1,4]				Office 365 Government				Office 365 Education		Office 365 Business Essentials	Office 365 Business Premium	Office 365 Midsize Business	Enterprise Mobility Suite	Enterprise Cloud Suite [2]	Microsoft Dynamics CRM Online[3]	
Online Service	K1	E1	E3	E5	K1	E1	E3	E4	Edu	E5						Pro.	Ent.
Exchange Online											■	■					
Exchange Online Kiosk	■				■												
Exchange Online Plan 1		■				■			■				■				
Exchange Online Plan 2			■	■			■	■		■					■		
SharePoint Online											■	■					
SharePoint Online Kiosk	■				■												
SharePoint Online Plan 1		■				■			■				■				
SharePoint Online Plan 2			■	■			■	■		■					■		
Skype for Business Online											■	■					
Skype for Business Online Plan 1																	
Skype for Business Online Plan 2		■	■	■		■	■	■	■	■			■		■		
Skype for Business Online Cloud PBX				■						■							
Skype for Business Online PSTN Conf.				■						■							
Yammer Enterprise	■	■	■	■					■	■	■	■	■		■		
Office Online	■	■	■	■	■	■	■	■	■	■	■	■	■		■		
Office 365 Business												■					
Office 365 ProPlus			■	■			■	■		■			■		■		
Office 365 Customer Lockbox				■						■							
Office 365 Delve Analytics				■						■							
Office 365 Advanced eDiscovery				■						■							
Office 365 Advanced Security Management				■						■							
Power BI Pro				■						■							
Office 365 Advanced Threat Protection				■						■							
Microsoft Intune														■	■		
Azure Rights Management Premium														■	■		
Azure Active Directory Premium P1														■	■		

Microsoft Dynamics Marketing Sales Collaboration																🟦	
Microsoft Dynamics Marketing Enterprise																	🟦
Microsoft Social Engagement Professional																🟦	🟦
Parature Enterprise																	🟦

[1] Add-on Suite SLs that include “without ProPlus” in the title do not include rights to Office 365 ProPlus.

[2] In addition to the Online Services identified above, the Enterprise Cloud Suite fulfills the SL requirement for Windows SA per User as described in the Product Terms.

[3] Microsoft Dynamics CRM Online Professional EDU and Microsoft Dynamics CRM Online Enterprise EDU fulfil the same SL requirements as Microsoft Dynamics CRM Online Professional and Microsoft Dynamics CRM Online Enterprise respectively

[4] Inclusion of Skype for Business Online PSTN Conferencing with Office 365 Enterprise E5 is dependent on regional availability

Exhibit 6 – Initial MS SLA ("Locked SLA"– see Section 1.c of Exhibit 1)

<Table of contents has been deleted>

Introduction

About this Document

This Service Level Agreement for Microsoft Online Services (this "SLA") is a part of your Microsoft volume licensing agreement (the "Agreement"). Capitalized terms used but not defined in this SLA will have the meaning assigned to them in the Agreement. This SLA applies to the Microsoft Online Services listed herein (a "Service" or the "Services"), but does not apply to separately branded services made available with or connected to the Services or to any on-premise software that is part of any Service.

If we do not achieve and maintain the Service Levels for each Service as described in this SLA, then you may be eligible for a credit towards a portion of your monthly service fees. We will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, the version of this SLA that is current at the time of renewal will apply throughout your renewal term. We will provide at least 90 days' notice for adverse material changes to this SLA. You can review the most current version of this SLA at any time by visiting http://www.microsoftvolumelicensing.com/SLA.

Prior Versions of this Document

This SLA provides information on Services currently available. Earlier versions of this document are available at http://www.microsoftvolumelicensing.com. To find the needed version, a customer may contact its reseller or Microsoft Account Manager.

Clarifications and Summary of Changes to this Document

Below are recent additions, deletions and other changes to this SLA. Also listed below, are clarifications of Microsoft policy in response to common customer questions.

Additions	Deletions
Minecraft: Education Edition	

Table of Contents / Definitions

General Terms

Definitions

"**Applicable Monthly Period**" means, for a calendar month in which a Service Credit is owed, the number of days that you are a subscriber for a Service.

"**Applicable Monthly Service Fees**" means the total fees actually paid by you for a Service that are applied to the month in which a Service Credit is owed.

"**Downtime**" is defined for each Service in the Services Specific Terms below. Except for Microsoft Azure Services, Downtime does not include Scheduled Downtime. Downtime does not include unavailability of a Service due to limitations described below and in the Services Specific Terms.

"**Error Code**" means an indication that an operation has failed, such as an HTTP status code in the 5xx range.

"**External Connectivity**" is bi-directional network traffic over supported protocols such as HTTP and HTTPS that can be sent and received from a public IP address.

"**Incident**" means (i) any single event, or (ii) any set of events, that result in Downtime.

"**Management Portal**" means the web interface, provided by Microsoft, through which customers may manage the Service.

“**Scheduled Downtime**” means periods of Downtime related to network, hardware, or Service maintenance or upgrades. We will publish notice or notify you at least five (5) days prior to the commencement of such Downtime.

“**Service Credit**” is the percentage of the Applicable Monthly Service Fees credited to you following Microsoft’s claim approval.

“**Service Level**” means the performance metric(s) set forth in this SLA that Microsoft agrees to meet in the delivery of the Services.

“**Service Resource**” means an individual resource available for use within a Service.

“**Success Code**” means an indication that an operation has succeeded, such as an HTTP status code in the 2xx range.

“**Support Window**” refers to the period of time during which a Service feature or compatibility with a separate product or service is supported.

“**User Minutes**” means the total number of minutes in a month, less all Scheduled Downtime, multiplied by the total number of users.

Terms

Claims

In order for Microsoft to consider a claim, you must submit the claim to customer support at Microsoft Corporation including all information necessary for Microsoft to validate the claim, including but not limited to: (i) a detailed description of the Incident; (ii) information regarding the time and duration of the Downtime; (iii) the number and location(s) of affected users (if applicable); and (iv) descriptions of your attempts to resolve the Incident at the time of occurrence.

For a claim related to Microsoft Azure, we must receive the claim within two months of the end of the billing month in which the Incident that is the subject of the claim occurred. For claims related to all other Services, we must receive the claim by the end of the calendar month following the month in which the Incident occurred. For example, if the Incident occurred on February 15th, we must receive the claim and all required information by March 31st.

We will evaluate all information reasonably available to us and make a good faith determination of whether a Service Credit is owed. We will use commercially reasonable efforts to process claims during the subsequent month and within forty-five (45) days of receipt. You must be in compliance with the Agreement in order to be eligible for a Service Credit. If we determine that a Service Credit is owed to you, we will apply the Service Credit to your Applicable Monthly Service Fees.

If you purchased more than one Service (not as a suite), then you may submit claims pursuant to the process described above as if each Service were covered by an individual SLA. For example, if you purchased both Exchange Online and SharePoint Online (not as part of a suite), and during the term of the subscription an Incident caused Downtime for both Services, then you could be eligible for two separate Service Credits (one for each Service), by submitting two claims under this SLA. In the event that more than one Service Level for a particular Service is not met because of the same Incident, you must choose only one Service Level under which to make a claim based on the Incident.

Service Credits

Service Credits are your sole and exclusive remedy for any performance or availability issues for any Service under the Agreement and this SLA. You may not unilaterally offset your Applicable Monthly Service Fees for any performance or availability issues.

Service Credits apply only to fees paid for the particular Service, Service Resource, or Service tier for which a Service Level has not been met. In cases where Service Levels apply to individual Service Resources or to separate Service tiers, Service Credits apply only to fees paid for the affected Service Resource or Service tier, as applicable. The Service Credits awarded in any billing month for a particular Service or Service Resource will not, under any circumstance, exceed your monthly service fees for that Service or Service Resource, as applicable, in the billing month.

If you purchased Services as part of a suite or other single offer, the Applicable Monthly Service Fees and Service Credit for each Service will be pro-rated.

If you purchased a Service from a reseller, you will receive a service credit directly from your reseller and the reseller will receive a Service Credit directly from us. The Service Credit will be based on the estimated retail price for the applicable Service, as determined by us in our reasonable discretion.

Limitations

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centers, including at your site or between your site and our data center);
2. That result from the use of services, hardware, or software not provided by us, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services;
3. Caused by your use of a Service after we advised you to modify your use of the Service, if you did not modify your use as advised;
4. During or with respect to preview, pre-release, beta or trial versions of a Service, feature or software (as determined by us) or to purchases made using Microsoft subscription credits;
5. That result from your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;
6. That result from your failure to adhere to any required configurations, use supported platforms, follow any policies for acceptable use, or your use of the Service in a manner inconsistent with the features and functionality of the Service (for example, attempts to perform operations that are not supported) or inconsistent with our published guidance;
7. That result from faulty input, instructions, or arguments (for example, requests to access files that do not exist);
8. That result from your attempts to perform operations that exceed prescribed quotas or that resulted from our throttling of suspected abusive behavior;
9. Due to your use of Service features that are outside of associated Support Windows; or
10. For licenses reserved, but not paid for, at the time of the Incident.

Services purchased through Open, Open Value, and Open Value Subscription volume licensing agreements, and Services in an Office 365 Small Business Premium suite purchased in the form of a product key are not eligible for Service Credits based on service fees. For these Services, any Service Credit that you may be eligible for will be credited in the form of service time (i.e., days) as opposed to service fees, and any references to “Applicable Monthly Service Fees” is deleted and replaced by “Applicable Monthly Period.”

Table of Contents / Definitions

Service Specific Terms

Microsoft Dynamics

Microsoft Dynamics AX

Additional Definitions:

"**Active Tenant**" means a tenant with an active high availability production topology in the Management Portal that (A) has been deployed to a Partner Application Service; and (B) has an active database that users can log into.

“**Partner Application Service**” means a partner application built on top of and combined with the Platform that (A) is used for processing your organization’s actual business transactions; and (B) has reserve compute and storage resources equal to or greater than one of the Scale Units your partner selected for the applicable partner application.

“**Maximum Available Minutes**” means the total accumulated minutes during a billing month in which an Active Tenant was deployed in a Partner Application Service using an active high availability production topology.

“**Platform**” means the Service’s client forms, SQL server reports, batched operations, and API endpoints, or the Service’s retail APIs that are used for commerce or retail purposes only.

“**Scale Unit**” means the increments by which compute and storage resources are added to or removed from a Partner Application Service.

“**Service Infrastructure**” means the authentication, computing, and storage resources that Microsoft provides in connection with the Service.

Downtime: Any period of time when end users are unable to login to their Active Tenant, due to a failure in the unexpired Platform or the Service Infrastructure as Microsoft determines from automated health monitoring and system logs. Downtime does not include Scheduled Downtime, the unavailability of Service add-on features, the inability to access the Service due to your modifications of the Service, or periods where the Scale Unit capacity is exceeded.

Monthly Uptime Percentage: The Monthly Uptime Percentage for a given Active Tenant in a calendar month is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.5%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Microsoft Dynamics CRM

Downtime: Any period of time when end users are unable to read or write any Service data for which they have appropriate permission but this does not include non-availability of Service add-on features.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Office 365 Services

Duet Enterprise Online

Downtime: Any period of time when users are unable to read or write any portion of a SharePoint Online site collection for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%

Monthly Uptime Percentage	Service Credit
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply when the inability to read or write any portion of a SharePoint Online site is caused by any failure of third party software, equipment, or services that are not controlled by Microsoft, or Microsoft software that is not being run by Microsoft itself as part of the Service.

Additional Terms: You will be eligible for a Service Credit for Duet Enterprise Online only when you are eligible for a Service Credit for the SharePoint Online Plan 2 User SLs that you have purchased as a prerequisite for your Duet Enterprise Online User SLs.

Table of Contents / Definitions

Exchange Online

Downtime: Any period of time when users are unable to send or receive email with Outlook Web Access. There is no Scheduled Downtime for this service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Additional Terms: See Appendix 1 – Service Level Commitment for Virus Detection and Blocking, Spam Effectiveness, or False Positive.

Table of Contents / Definitions

Exchange Online Archiving

Downtime: Any period of time when users are unable to access the email messages stored in their archive. There is no Scheduled Downtime for this service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to the Enterprise CAL suite purchased through Open Value and Open Value Subscription volume licensing agreements.

Table of Contents / Definitions

Exchange Online Protection

Downtime: Any period of time when the network is not able to receive and process email messages. There is no Scheduled Downtime for this service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to the Enterprise CAL suite purchased through Open Value and Open Value Subscription volume licensing agreements.

Additional Terms: See (i) Appendix 1 – Service Level Commitment for Virus Detection and Blocking, Spam Effectiveness, or False Positive and (ii) Appendix 2 – Service Level Commitment for Uptime and Email Delivery.

Table of Contents / Definitions

Office 365 Business

Downtime: Any period of time when Office applications are put into reduced functionality mode due to an issue with Office 365 activation.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Office 365 Customer Lockbox

Downtime: Any period of time when Customer Lockbox is put into reduced functionality mode due to an issue with Office 365.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Office 365 ProPlus

Downtime: Any period of time when Office applications are put into reduced functionality mode due to an issue with Office 365 activation.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Office Online

Downtime: Any period of time when users are unable to use the Web Applications to view and edit any Office document stored on a SharePoint Online site for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Office 365 Video

Downtime: Any period of time when users are unable to upload, view or edit videos in the video portal when they have appropriate permissions and valid content.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Level Commitment:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

OneDrive for Business

Downtime: Any period of time when users are unable to view or edit files stored on their personal OneDrive for Business storage.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Project Online

Downtime: Any period of time when users are unable to read or write any portion of a SharePoint Online site collection with Project Web App for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%

Monthly Uptime Percentage	Service Credit
< 99%	50%
< 95%	100%

Table of Contents / Definitions

SharePoint Online

Downtime: Any period of time when users are unable to read or write any portion of a SharePoint Online site collection for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Skype for Business Online

Downtime: Any period of time when end users are unable to see presence status, conduct instant messaging conversations, or initiate online meetings.[1]

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

[1] Online meeting functionality applicable only to Skype for Business Online Plan 2 Service.

Table of Contents / Definitions

Skype for Business Online – PSTN Calling and PSTN Conferencing

Downtime: Any period of time when end users are unable to initiate a PSTN call or unable to dial into a PSTN conference.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ -Downtime}{User\ Minutes}\ x\ 100$$

Where Downtime is measured in user-minutes; that is, for each month Downtime is the sum of the length (in minutes) of each incident that occurs during that month multiplied by the number of users impacted by that incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Skype for Business Online – Voice Quality

This SLA applies to any eligible call placed by any voice service user within the subscription (enabled for making any type of call VOIP or PSTN).

Additional Definitions:
"**Eligible Call**" is a Skype for Business placed call (within a subscription) that meets both conditions below:

- The call was placed from a Skype for Business Certified IP Desk phones on wired Ethernet
- Packet Loss, Jitter and Latency issues on the call were due to networks managed by Microsoft.

"**Total Calls**" is the total number of Eligible Calls
"**Poor Quality Calls**" is the total number of Eligible Calls that are classified as poor based on numerous factors that could impact call quality in the networks managed by Microsoft. While the current Poor Call classifier is built primarily on network parameters like RTT (Roundtrip Time), Packet Loss Rate, Jitter and Packet Loss-Delay Concealment Factors, it is dynamic and continually updated based on new learnings from analysis using millions of Skype and Skype for Business calls and evolution of Devices, Algorithms and end user ratings.

Monthly Good Call Rate: The Monthly Good Call Rate is calculated using the following formula:

$$\frac{Total\ Calls\ -Poor\ Quality\ Calls}{Total\ Calls}\ x\ 100$$

Service Credit:

Monthly Good Call Rate	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Yammer Enterprise

Downtime: Any period of time greater than ten minutes when more than five percent of end users are unable to post or read messages on any portion of the Yammer network for which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ -Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Enterprise Mobility Services

Azure Active Directory Basic

Downtime: Any period of time when users are not able to log in to the service, log in to the Access Panel, access applications on the Access Panel and reset passwords; or any period of time IT administrators are not able to create, read, write and delete entries in the directory and/or provision/de-provision users to applications in the directory.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Azure Active Directory B2C

Additional Definitions:
"**Deployment Minutes**" is the total number of minutes for which an Azure AD B2C directory has been deployed during a billing month.
"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Azure AD B2C directories in a given Microsoft Azure subscription during a billing month.

Downtime: is the total accumulated minutes across all Azure AD B2C directories deployed by Customer in a given Microsoft Azure subscription during which the Azure AD B2C service is unavailable. A minute is considered unavailable if either all attempts to process user sign-up, sign-in, profile editing, password reset and multi-factor authentication requests, or all attempts by developers to create, read, write and delete entries in a directory, fails to return tokens or valid Error Codes, or do not return responses within two minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\ - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: No SLA is provided for the Free tier of Azure Active Directory B2C.

Table of Contents / Definitions

Azure Active Directory Premium

Downtime: Any period of time when users are not able to log in to the service, log in to the Access Panel, access applications on the Access Panel and reset passwords; or any period of time IT administrators are not able to create, read, write and delete entries in the directory and/or provision/de-provision users to applications in the directory.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Azure Rights Management Premium

Downtime: Any period of time when end users cannot create or consume IRM documents and email.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Microsoft Intune

Downtime: Any period of time when the Customer's IT administrator or users authorized by Customer are unable to log on with proper credentials. Scheduled Downtime will not exceed 10 hours per calendar year.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ - Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This Service Level does not apply to any: (i) On-premises software licensed as part of the Service subscription, or (ii) Internet-based services (excluding Microsoft Intune Service) that provide updates to any on-premise software licensed as part of the Service subscription.

Table of Contents / Definitions

Microsoft Azure Services

API Management Services

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given API Management instance has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all API Management instances deployed by you in a given Microsoft Azure subscription during a billing month.

"**Proxy**" is the component of the API Management Service responsible for receiving API requests and forwarding them to the configured dependent API.

Downtime: The total accumulated Deployment Minutes, across all API Management instances deployed by you in a given Microsoft Azure subscription, during which the API Management Service is unavailable. A minute is considered unavailable for a given API Management instance if all continuous attempts to perform operations through the Proxy throughout the minute result in either an Error Code or do not return a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit for Standard Tier:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Credit for Premium Tier deployments scaled across two or more regions:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Table of Contents / Definitions

App Service

Additional Definitions:

"**App**" is an API App, Logic App, Web App or Mobile App deployed by Customer within the App Service, excluding web apps in the Free and Shared tiers.

"**Deployment Minutes**" is the total number of minutes that a given App has been set to running in Microsoft Azure during a billing month. Deployment Minutes is measured from when the App was created or the Customer initiated an action that would result in running the App to the time the Customer initiated an action that would result in stopping or deleting the App.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Apps deployed by Customer in a given Microsoft Azure subscription during a billing month

Downtime: is the total accumulated Deployment Minutes, across all Apps deployed by Customer in a given Microsoft Azure subscription, during which the App is unavailable. A minute is considered unavailable for a given App when there is no connectivity between the App and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Additional Terms: Service Credits are applicable only to fees attributable to your use of Web Apps or Mobile Apps and not to fees attributable to other types of apps available through the App Service, which are not covered by this SLA.

Table of Contents / Definitions

Application Gateway

Additional Definitions:

"**Application Gateway Cloud Service**" refers to a collection of one or more Application Gateway instances configured to perform HTTP load balancing services.

"**Maximum Available Minutes**" is the total accumulated minutes during a billing month during which an Application Gateway Cloud Service comprising two or more medium or larger Application Gateway instances has been deployed in a Microsoft Azure subscription.

Downtime: is the total accumulated Maximum Available Minutes during a billing month for a given Application Gateway Cloud Service during which the Application Gateway Cloud Service is unavailable. A given minute is considered unavailable if all attempts to connect to the Application Gateway Cloud Service throughout the minute are unsuccessful.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Automation Service – Desired State Configuration (DSC)

Additional Definitions:

"**Deployment Minutes"** is the total number of minutes that a given Automation account has been deployed in Microsoft Azure during a billing month.

"**DSC Agent Service**" is the component of the Automation Service responsible for receiving and responding to pull, registration, and reporting requests from DSC nodes.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Automation accounts deployed in a given Microsoft Azure subscription during a billing month

Downtime: The total accumulated Deployment Minutes, across all Automation accounts deployed in a given Microsoft Azure subscription, during which the DSC Agent Service is unavailable. A minute is considered unavailable for a given Automation account if all continuous pull, registration, and reporting requests from DSC nodes associated with the Automation account to the DSC Agent Service throughout the minute either result in an Error Code or do not return a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Automation Service – Process Automation

Additional Definitions:

"**Delayed Jobs**" is the total number of Jobs, for a given Microsoft Azure subscription, that fail to start within thirty (30) minutes of their Planned Start Times.

"**Job**" means the execution of a Runbook.

"**Planned Start Time**" is a time at which a Job is scheduled to begin executing.

"**Runbook**" means a set of actions specified by you to execute within Microsoft Azure.

"**Total Jobs**" is the total number of Jobs scheduled for execution during a given billing month, for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Jobs - Delayed\ Jobs}{Total\ Jobs}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Azure Security Center

Additional Definitions:

"**Protected Node**" is a Microsoft Azure resource, counted as a node for billing purposes that is configured for the Azure Security Center Standard Tier

"**Security Monitoring**" is the assessment of a Protected Node resulting in potential findings such as security health status, recommendations, and security alerts, exposed in Azure Security Center.

"**Maximum Available Minutes**" is the total number of minutes during a billing month that a given Protected Node has been deployed and configured for Security Monitoring.

"**Downtime**" is the total accumulated minutes during a billing month for which Security Monitoring information of a given Protected Node is unavailable. A minute is considered unavailable for a given Protected Node if all continuous attempts to retrieve Security Monitoring information throughout the minute result in either an Error Code or do not return a Success Code within two minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Batch Service

Additional Definitions:

“**Average Error Rate**“ for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

“**Error Rate**“ is the total number of Failed Requests divided by Total Requests during a given one-hour interval. If the Total Requests in a given one-hour interval is zero, the Error Rate for that interval is 0%.

“**Excluded Requests**” are requests within Total Requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

“**Failed Requests**“ is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or fail to return a Success Code within 5 seconds.

“**Total Requests**” is the total number of authenticated REST API requests, other than Excluded Requests, to perform operations against Batch accounts attempted within a one-hour interval within a given Azure subscription during a billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

100% - Average Error Rate

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Backup Service

Additional Definitions:

“**Backup**” or “**Back Up**” is the process of copying computer data from a registered server to a Backup Vault.

“**Backup Agent**” refers to the software installed on a registered server that enables the registered server to Back Up or Restore one or more Protected Items.

“**Backup Vault**” refers to a container in which you may register one or more Protected Items for Backup.

“**Deployment Minutes**” is the total number of minutes during which a Protected Item has been scheduled for Backup to a Backup Vault.

“**Failure**” means that either the Backup Agent or the Service fails to fully complete a properly configured Backup or Recovery operation due to unavailability of the Backup Service.

“**Maximum Available Minutes**” is the sum of all Deployment Minutes across all Protected Items for a given Microsoft Azure subscription during a billing month.

“**Protected Item**” refers to a collection of data, such as a volume, database, or virtual machine that has been scheduled for Backup to the Backup Service such that it is enumerated as a Protected Item in the Protected Items tab in the Recovery Services section of the Management Portal.

"**Recovery**" or "**Restore**" is the process of restoring computer data from a Backup Vault to a registered server.

Downtime: The total accumulated Deployment Minutes across all Protected Items scheduled for Backup by you in a given Microsoft Azure subscription during which the Backup Service is unavailable for the Protected Item. The Backup Service is considered unavailable for a given Protected Item from the first Failure to Back Up or Restore the Protected Item until the initiation of a successful Backup or Recovery of a Protected Item, provided that retries are continually attempted no less frequently than once every thirty minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

BizTalk Services

Additional Definitions:

"**BizTalk Service Environment**" refers to a deployment of the BizTalk Services created by you, as represented in the Management Portal, to which you may send runtime message requests.

"**Deployment Minutes**" is the total number of minutes that a given BizTalk Service Environment has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all BizTalk Service Environments deployed by you in a given Microsoft Azure subscription during a billing month.

"**Monitoring Storage Account**" refers to the Azure Storage account used by the BizTalk Services to store monitoring information related to the execution of the BizTalk Services.

Downtime: The total accumulated Deployment Minutes, across all BizTalk Service Environments deployed by you in a given Microsoft Azure subscription, during which the BizTalk Service Environment is unavailable. A minute is considered unavailable for a given BizTalk Service Environment when there is no connectivity between your BizTalk Service Environment and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Basic, Standard, and Premium tiers of the BizTalk Services. The Developer tier of the Microsoft Azure BizTalk Services is not covered by this SLA.

Additional Terms: When submitting a claim, you must ensure that complete monitoring data is maintained within the Monitoring Storage Account and is made available to Microsoft.

Table of Contents / Definitions

Cache Services

Additional Definitions:

"**Cache**" refers to a deployment of the Cache Service created by you, such that its Cache Endpoints are enumerated in the Cache tab in the Management Portal.

"**Cache Endpoints**" refers to endpoints through which a Cache may be accessed.

"**Deployment Minutes**" is the total number of minutes that a given Cache has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Caches deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Caches deployed by you in a given Microsoft Azure subscription, during which the Cache is unavailable. A minute is considered unavailable for a given Cache when there is no connectivity throughout the minute between one or more Cache Endpoints associated with the Cache and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Cache Service, which includes the Azure Managed Cache Service or the Standard tier of the Azure Redis Cache Service. The Basic tier of the Azure Redis Cache Service is not covered by this SLA.

Table of Contents / Definitions

CDN Service

Downtime: To assess Downtime, Microsoft will review data from any commercially reasonable independent measurement system used by you.

You must select a set of agents from the measurement system's list of standard agents that are generally available and represent at least five geographically diverse locations in major worldwide metropolitan areas (excluding PR of China).

Measurement System tests (frequency of at least one test per hour per agent) will be configured to perform one HTTP GET operation according to the model below:

1. A test file will be placed on your origin (e.g., Azure Storage account).
2. The GET operation will retrieve the file through the CDN Service, by requesting the object from the appropriate Microsoft Azure domain name hostname.
3. The test file will meet the following criteria:
   i. The test object will allow caching by including explicit "Cache-control: public" headers, or lack of "Cache-Control: private" header.
   ii. The test object will be a file at least 50KB in size and no larger than 1MB.
   iii. Raw data will be trimmed to eliminate any measurements that came from an agent experiencing technical problems during the measurement period.

Monthly Uptime Percentage: The percentage of HTTP transactions in which the CDN responds to client requests and delivers the requested content without error. Monthly Uptime Percentage of the CDN Service is calculated as the number of times the object was delivered successfully divided by the total number of requests (after removing erroneous data).

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99.5%	25%

Table of Contents / Definitions

Cloud Services

Additional Definitions:
"**Cloud Services**" refers to a set of compute resources utilized for Web and Worker Roles.
"**Maximum Available Minutes**" is the total accumulated minutes during a billing month for all Internet facing roles that have two or more instances deployed in different Update Domains. Maximum Available Minutes is measured from when the Tenant has been deployed and its associated roles have been started resultant from action initiated by you to the time you have initiated an action that would result in stopping or deleting the Tenant.
"**Tenant**" represents one or more roles each consisting of one or more role instances that are deployed in a single package.
"**Update Domain**" refers to a set of Microsoft Azure instances to which platform updates are concurrently applied.
"**Web Role**" is a Cloud Services component run in the Azure execution environment that is customized for web application programming as supported by IIS and ASP.NET.
"**Worker Role**" is a Cloud Services component run in the Azure execution environment that is useful for generalized development, and may perform background processing for a Web Role.

Downtime: The total accumulated minutes that are part of Maximum Available Minutes that have no External Connectivity.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Table of Contents / Definitions

Data Catalog

Additional Definitions:
"**Deployment Minutes**" is the total number of minutes for which a Data Catalog has been purchased during a billing month.

"**Entries**" means any catalog object registration in the Data Catalog (such as a table, view, measure, cluster or report).
"**Maximum Available Minutes**" is the sum of all Deployment Minutes for the Data Catalog associated with a given Microsoft Azure subscription during a billing month.

Downtime: is the total accumulated Deployment minutes, during which the Data Catalog is unavailable. A minute is considered unavailable for a given Data Catalog if all attempts by administrators to add or remove users to the Data Catalog or all attempts by users to execute API calls to the Data Catalog for registering, searching, or deleting Entries either result in an Error Code or do not return a response within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Data Factory – Activity Runs

Additional Definitions:

"**Activity Run**" means the execution or attempted execution of an activity

"**Delayed Activity Runs**" is the total number of attempted Activity Runs in which an activity fails to begin executing within four (4) minutes after the time at which it is scheduled for execution and all dependencies that are prerequisite to execution have been satisfied.

"**Total Activity Runs**" is the total number of Activity Runs attempted during in a billing month for a given Microsoft Azure Subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Activity\ Runs - Delayed\ Activty\ Runs}{Total\ Activity\ Runs}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Data Factory – API Calls

Additional Definitions:

"**Excluded Requests**" is the set of requests within Total Requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

"**Failed Requests**" is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or otherwise fail to return a Success Code within two minutes.

"**Resources**" means pipelines, data sets, and linked services created within a Data Factory.

"**Total Requests**" is the set of all requests, other than Excluded Requests, to perform operations against Resources within active pipelines during a billing month for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Requests - Failed\ Requests}{Total\ Requests}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

DocumentDB

Additional Definitions:

"**Average Error Rate**" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"**Database Account**" is a DocumentDB account containing one or more databases.

"**Error Rate**" is the total number of Failed Requests divided by Total Requests, across all Resources in a given Azure subscription, during a given one-hour interval. If the Total Requests in a given one-hour interval is zero, the Error Rate for that interval is 0%.

"**Excluded Requests**" are requests within Total Requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

"**Failed Requests**" is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or fail to return a Success Code within 5 seconds.

"**Resource**" is a set of URI addressable entities associated with a Database Account.

"**Total Request**" is the set of all requests, other than Excluded Requests, to perform operations issued against Resources attempted within a one-hour interval within a given Azure subscription during a billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

100% - Average Error Rate

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Table of Contents / Definitions

ExpressRoute

Additional Definitions:

"**Dedicated Circuit**" means a logical representation of connectivity offered through the ExpressRoute Service between your premises and Microsoft Azure through an exchange provider or a network service provider, where such connectivity does not traverse the public Internet.

"**Maximum Available Minutes**" is the total number of minutes that a given Dedicated Circuit is linked to one or more Virtual Networks in Microsoft Azure during a billing month in a given Microsoft Azure subscription.

"**Virtual Network**" refers to a virtual private network that includes a collection of user-defined IP addresses and subnets that form a network boundary within Microsoft Azure.

"**VPN Gateway**" refers to a gateway that facilitates cross-premises connectivity between a Virtual Network and a customer on-premises network.

Downtime: The total accumulated minutes during a billing month for a given Microsoft Azure subscription during which the Dedicated Circuit is unavailable. A minute is considered unavailable for a given Dedicated Circuit if all attempts by you within the minute to establish IP-level connectivity to the VPN Gateway associated with the Virtual Network fail for longer than thirty seconds.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Additional Terms: Monthly Uptime Percentage and Service Credits are calculated for each Dedicated Circuit used by you.

Table of Contents / Definitions

HDInsight

Additional Definitions:

"**Cluster Internet Gateway**" means a set of virtual machines within an HDInsight Cluster that proxy all connectivity requests to the Cluster.

"**Deployment Minutes**" is the total number of minutes that a given HDInsight Cluster has been deployed in Microsoft Azure.

"**HDInsight Cluster**" or "**Cluster**" means a collection of virtual machines running a single instance of the HDInsight Service.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Clusters deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes when the HDInsight Service is unavailable. A minute is considered unavailable for a given Cluster if all continual attempts within the minute to establish a connection to the Cluster Internet Gateway fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

HockeyApp

Additional Definitions:

"**HockeyApp Dashboard**" means the web interface provided to developers to view and manage applications using the HockeyApp Service.

"**Maximum Available Minutes**" is the total number of minutes in a billing month.

Downtime: is the total accumulated minutes in a billing month during which the HockeyApp Service is unavailable. A minute is considered unavailable if all continuous HTTP requests to the HockeyApp Dashboard or to the HockeyApp API throughout the minute either result in an Error Code or do not return a response within one minute. For purposes of the HockeyApp API, HTTP response codes 408, 429, 500, 503, and 511 are not considered Error Codes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

IoT hub

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given IoT hub has been deployed in Microsoft Azure during a billing month.

"**Device Identity Operations**" refers to create, read, update, and delete operations performed on the device identity registry of an IoT hub.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all IoT hubs deployed in a given Microsoft Azure subscription during a billing month.

"**Message**" refers to any content sent by a deployed IoT hub to a device registered to the IoT hub or received by the IoT hub from a registered device, using any protocol supported by the Service.

Downtime: The total accumulated Deployment Minutes, across all IoT hubs deployed in a given Microsoft Azure subscription, during which the IoT hub is unavailable. A minute is considered unavailable for a given IoT hub if all continuous attempts to send or receive Messages or perform Device Identity Operations on the IoT hub throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Key Vault

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given key vault has been deployed in Microsoft Azure during a billing month.

"**Excluded Transactions**" are transactions for creating, updating, or deleting key vaults, keys, or secrets.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Key Vaults deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: is the total accumulated Deployment Minutes, across all key vaults deployed by Customer in a given Microsoft Azure subscription, during which the key vault is unavailable. A minute is considered unavailable for a given key vault if all continuous attempts to perform transactions, other than Excluded Transactions, on the key vault throughout the minute either return an Error Code or do not result in a Success Code within 5 seconds from Microsoft's receipt of the request.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} \; x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Log Analytics

Additional Definitions:

"**Batch**" means a group of Log Data entries that are either uploaded to the Log Analytics Service or read from storage by the Log Analytics Service within a given period of time. Batches queued for indexing are displayed in the usage section of the Management Portal.

"**Log Data**" refers to information regarding a supported event, such as IIS and Windows events, that is logged by a computer and for which the Log Analytics Service has been configured to be processed by the Service index.

"**Delayed Batches**" is the total number of Batches within Total Queued Batches that fail to complete indexing within six hours of the Batch being queued.

"**Total Queued Batches**" is the total number of Batches queued for indexing by the Log Analytics Service during a given billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\boldsymbol{Total\ Queued\ Batches - Delayed\ Batches}}{\boldsymbol{Total\ Queued\ Batches}} \; \boldsymbol{x\ 100}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Logic Apps

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Logic App has been set to running in Microsoft Azure during a billing month. Deployment Minutes is measured from when the Logic App was created or Customer initiated an action that would result in running the Logic App to the time Customer initiated an action that would result in stopping or deleting the Logic App.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Logic Apps deployed by Customer in a given Microsoft Azure subscription during a billing month.

"**Downtime**" The total accumulated Deployment Minutes, across all Logic Apps deployed by Customer in a given Microsoft Azure subscription, during which the Logic App is unavailable. A minute is considered unavailable for a given Logic App when there is no connectivity between the Logic App and Microsoft's Internet gateway.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\boldsymbol{Maximum\ Available\ Minutes - Downtime}}{\boldsymbol{Maximum\ Available\ Minutes}} \; \boldsymbol{x\ 100}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Machine Learning – Batch Execution Service (BES) and Management APIs Service

Additional Definitions:
"**Failed Transactions**" is the set of all requests within Total Transaction Attempts that return an Error Code.

"**Total Transaction Attempts**" is the total number of authenticated REST BES and Management API requests by you during a billing month for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\,Transaction\,Attempts - Failed\,Transactions}{Total\,Transaction\,Attempts}\,x\,100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: Service Levels and Service Credits are applicable to your use of the Machine Learning BES and Management API Service. The Free Machine Learning tier is not covered by this SLA.

Table of Contents / Definitions

Machine Learning – Request Response Service (RRS)

Additional Definitions:
"**Failed Transactions**" is the set of all requests within Total Transaction Attempts that return an Error Code.

"**Total Transaction Attempts**" is the total number of authenticated REST RRS and Management API requests by you during a billing month for a given Microsoft Azure subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\,Transaction\,Attempts - Failed\,Transactions}{Total\,Transaction\,Attempts}\,x\,100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Service Level Exceptions: Service Levels and Service Credits are applicable to your use of the Machine Learning RRS and Management API Service. The Free Machine Learning tier is not covered by this SLA.

Table of Contents / Definitions

Media Services – Content Protection Service

Additional Definitions:

“**Failed Transactions**” are all Valid Key Requests included in Total Transaction Attempts that result in an Error Code or otherwise do not return a Success Code within 30 seconds after receipt by the Content Protection Service.

“**Total Transaction Attempts**” are all Valid Key Requests made by you during a billing month for a given Azure subscription.

“**Valid Key Requests**” are all requests made to the Content Protection Service for existing content keys in a Customer's Media Service.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Total Transaction Attempts} - \textit{Failed Transactions}}{\textit{Total Transaction Attempts}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Media Services – Encoding Service

Additional Definitions:

“**Encoding**” means the processing of media files per subscription as configured in the Media Services Tasks.

“**Failed Transactions**” is the set of all requests within Total Transaction Attempts that do not return a Success Code within 30 seconds from Microsoft’s receipt of the request.

“**Media Service**” means an Azure Media Services account, created in the Management Portal, associated with your Microsoft Azure subscription. Each Microsoft Azure subscription may have more than one associated Media Service.

“**Media Services Task**” means an individual operation of media processing work as configured by you. Media processing operations involve encoding and converting media files.

“**Total Transaction Attempts**” is the total number of authenticated REST API requests with respect to a Media Service made by you during a billing month for a subscription. Total Transaction Attempts does not include REST API requests that return an Error Code that are continuously repeated within a five-minute window after the first Error Code is received.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Total Transaction Attempts} - \textit{Failed Transactions}}{\textit{Total Transaction Attempts}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Media Services – Indexer Service

Additional Definitions:

“**Encoding Reserved Unit**” means encoding reserved units purchased by the customer in an Azure Media Services account

"**Failed Transactions**" is the set of Indexer Tasks within Total Transaction Attempts that either, a) do not complete within a time period that is 3 times the duration of the input file, or b) do not start processing within 5 minutes of the time that an Encoding Reserved Unit becomes available for use by the Indexer Task.
"**Indexer Task**" means a Media Services Task that is configured to index an MP3 input file with a minimum five-minute duration.

"**Total Transaction Attempts**" is the total number of Indexer Tasks attempted to be executed using an available Encoding Reserved Unit by Customer during a billing month for a subscription.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\boldsymbol{Total\,Transaction\,Attempts - Failed\,Transactions}}{\boldsymbol{Total\,Transaction\,Attempts}}\ \boldsymbol{x\ 100}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Media Services – Live Channels

Additional Definitions:
"**Channel**" means an end point within a Media Service that is configured to receive media data.

"**Deployment Minutes**" is the total number of minutes that a given Channel has been purchased and allocated to a Media Service and is in a running state during a billing month.
"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Channels purchased and allocated to a Media Service during a billing month.
"**Media Service**" means an Azure Media Services account, created in the Management Portal, associated with your Microsoft Azure subscription. Each Microsoft Azure subscription may have more than one associated Media Service.

Downtime: The total accumulated Deployment Minutes when the Live Channels Service is unavailable. A minute is considered unavailable for a given Channel if the Channel has no External Connectivity during the minute.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Media Services – Streaming Service

Additional Definitions:
"**Deployment Minutes**" is the total number of minutes that a given Streaming Unit has been purchased and allocated to a Media Service during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Streaming Units purchased and allocated to a Media Service during a billing month.

"**Media Service**" means an Azure Media Services account, created in the Management Portal, associated with your Microsoft Azure subscription. Each Microsoft Azure subscription may have more than one associated Media Service.

"**Media Service Request**" means a request issued to your Media Service.

"**Streaming Unit**" means a unit of reserved egress capacity purchased by you for a Media Service.

"**Valid Media Services Requests**" are all qualifying Media Service Requests for existing media content in a customer's Azure Storage account associated with its Media Service when at least one Streaming Unit has been purchased and allocated to that Media Service. Valid Media Services Requests do not include Media Service Requests for which total throughput exceeds 80% of the Allocated Bandwidth.

Downtime: The total accumulated Deployment Minutes when the Streaming Service is unavailable. A minute is considered unavailable for a given Streaming Unit if all continuous Valid Media Service Requests made to the Streaming Unit throughout the minute result in an Error Code.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ Transaction\ Attempts - Failed\ Transactions}{Total\ Transaction\ Attempts}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Microsoft Cloud App Security

Downtime: Any period of time when the Customer's IT administrator or users authorized by Customer are unable to log on with proper credentials. Scheduled Downtime will not exceed 10 hours per calendar year.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{User Minutes - Downtime}}{\textit{User Minutes}}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: This Service Level does not apply to any: (i) On-premises software licensed as part of the Service subscription, or (ii) Internet-based services (excluding Microsoft Cloud App Security) that provide updates via API (application programming interface) to any services licensed as part of the Service subscription.

Table of Contents / Definitions

Mobile Engagement

Additional Definitions:

"**Average Error Rate**" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"**Error Rate**" is the total number of Failed Requests divided by Total Requests during a given one-hour interval. If the Total Requests in a given one-hour interval is zero, the Error Rate for that interval is 0%.

"**Excluded Requests**" is the set of REST API requests that result in an HTTP 4xx status code, other than an HTTP 408 status code.

“**Failed Requests**” is the set of all requests within Total Requests that either return an Error Code or an HTTP 408 status code or fail to return a Success Code within 30 seconds.

“**Mobile Engagement Application**" is an Azure Mobile Engagement service instance.

“**Total Requests**” is the total number of authenticated REST API requests, other than Excluded Requests, made to Mobile Engagement Applications within a given Azure subscription during a billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% - Average\ Error\ Rate$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

The Free Mobile Engagement tier is not covered by this SLA.

Table of Contents / Definitions

Mobile Services

Additional Definitions:

“**Failed Transactions**” include any API calls included in Total Transaction Attempts that result in either an Error Code or do not return a Success Code.

“**Total Transaction Attempts**" are the total accumulated API calls made to the Azure Mobile Services during a billing month for a given Microsoft Azure subscription for which the Azure Mobile Services are running.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\boldsymbol{Total\ Transaction\ Attempts - Failed\ Transactions}}{\boldsymbol{Total\ Transaction\ Attempts}}\ \boldsymbol{x\ 100}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Standard and Premium Mobile Services tiers. The Free Mobile Services tier is not covered by this SLA.

Table of Contents / Definitions

Multi-Factor Authentication Service

Additional Definitions:

“**Deployment Minutes**” is the total number of minutes that a given Multi-Factor Authentication provider has been deployed in Microsoft Azure during a billing month.

“**Maximum Available Minutes**” is the sum of all Deployment Minutes across all Multi-Factor Authentication providers deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Multi-Factor Authentication providers deployed by you in a given Microsoft Azure subscription, during which the Multi-Factor Authentication Service is unable to receive or process authentication requests for the Multi-Factor Authentication provider.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

RemoteApp

Additional Definitions:

"**Application**" means a software application that is configured for streaming to a device using the RemoteApp Service.

"**Maximum Available Minutes**" is the sum of all User Application Minutes across all Users granted access to one or more Applications in a given Azure subscription during a billing month.

"**User**" means a specific user account that is able to stream an Application using the RemoteApp Service, as enumerated in the Management Portal.

"**User Application Minutes**" is the total number of minutes in a billing month during which you have granted a User access to an Application.

Downtime: The total accumulated User Minutes during which the RemoteApp Service is unavailable. A minute is considered unavailable for a given User when the User is unable to establish connectivity to an Application.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the RemoteApp Service. The RemoteApp free trial is not covered by this SLA.

Table of Contents / Definitions

Scheduler

Additional Definitions:

"**Maximum Available Minutes**" is the total number of minutes in a billing month.

"**Planned Execution Time**" is a time at which a Scheduled Job is scheduled to begin executing.

"**Scheduled Job**" means an action specified by you to execute within Microsoft Azure according to a specified schedule.

Downtime: The total accumulated minutes in a billing month during which one or more of your Scheduled Jobs is in a state of delayed execution. A given Scheduled Job is in a state of delayed execution if it has not begun executing after a Planned Execution Time, provided that such delayed execution time shall not be considered Downtime if the Scheduled Job begins executing within thirty (30) minutes after a Planned Execution Time.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Search

Additional Definitions:

"**Average Error Rate**" for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"**Error Rate**" is the total number of Failed Requests divided by Total Requests, across all Search Service Instances in a given Azure subscription, during a given one-hour interval. If the Total Requests in a one-hour interval is zero, the Error Rate for that interval is 0%.

"**Excluded Requests**" are all requests that are throttled due to exhaustion of resources allocated for a Search Service Instance, as indicated by an HTTP 503 status code and a response header indicating the request was throttled.

"**Failed Requests**" is the set of all requests within Total Requests that fail to return either a Success Code or HTTP 4xx response.

"**Replica**" is a copy of a search index within a Search Service Instance.

"**Search Service Instance**" is an Azure Search service instance containing one or more search indexes.

"**Total Requests**" is the set of (i) all requests to update a Search Service Instance having three or more Replicas, plus (ii) all requests to query a Search Service Instance having two or more Replicas, other than Excluded Requests, within a one-hour interval within a given Azure subscription during a billing month.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$100\% - \boldsymbol{Average\ Error\ Rate}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Free Search tier is not covered by this SLA.

Table of Contents / Definitions

Service-Bus Service – Event Hubs

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Event Hub has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Event Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Event Hubs tiers during a billing month.

"**Message**" refers to any user-defined content sent or received through Service Bus Relays, Queues, Topics, or Notification Hubs, using any protocol supported by Service Bus.

Downtime: The total accumulated Deployment Minutes, across all Event Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Event Hubs tiers, during which the Event Hub is unavailable. A minute is considered unavailable for a given Event Hub if all continuous attempts to send or receive Messages or perform other operations on the Event Hub throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} \; x\;100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Basic and Standard Event Hubs tiers. The Free Event Hubs tier is not covered by this SLA.

Table of Contents / Definitions

Service-Bus Service – Notification Hubs

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Notification Hub has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Notification Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Notification Hubs tiers during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Notification Hubs deployed by you in a given Microsoft Azure subscription under the Basic or Standard Notification Hubs tiers, during which the Notification Hub is unavailable. A minute is considered unavailable for a given Notification Hub if all continuous attempts to send notifications or perform registration management operations with respect to the Notification Hub throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} \; x\;100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: The Service Levels and Service Credits are applicable to your use of the Basic and Standard Notification Hubs tiers. The Free Notification Hubs tier is not covered by this SLA.

Table of Contents / Definitions

Service-Bus Service – Queues and Topics

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Queue or Topic has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Queues and Topics deployed by you in a given Microsoft Azure subscription during a billing month.

"**Message**" refers to any user-defined content sent or received through Service Bus Relays, Queues, Topics, or Notification Hubs, using any protocol supported by Service Bus.

Downtime: The total accumulated Deployment Minutes, across all Queues and Topics deployed by you in a given Microsoft Azure subscription, during which the Queue or Topic is unavailable. A minute is considered unavailable for a given Queue or Topic if all continuous attempts to send or receive Messages or perform other operations on the Queue or Topic throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes-Downtime}}{\text{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Service-Bus Service – Relays

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Relay has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Relays deployed by you in a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes, across all Relays deployed by you in a given Microsoft Azure subscription, during which the Relay is unavailable. A minute is considered unavailable for a given Relay if all continuous attempts to establish a connection to the Relay throughout the minute either return an Error Code or do not result in a Success Code within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\text{Maximum Available Minutes-Downtime}}{\text{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Site Recovery Service – On-Premises-to-Azure

Additional Definitions:

"**Failover**" is the process of transferring control, either simulated or actual, of a Protected Instance from a primary site to a secondary site.

"**On-Premises-to-Azure Failover**" is the Failover of a Protected Instance from a non-Azure primary site to an Azure secondary site. You may designate a particular Azure datacenter as a secondary site, provided that if Failover to the designated datacenter is not possible, Microsoft may replicate to a different datacenter in the same region.

"**Protected Instance**" refers to a virtual or physical machine configured for replication by the Site Recovery Service from a primary site to a secondary site. Protected Instances are enumerated in the Protected Items tab in the Recovery Services section of the Management Portal.

"**Recovery Time Objective (RTO)**" means the period of time beginning when you initiate a Failover of a Protected Instance experiencing either a planned or unplanned outage for On-Premises-to-Azure replication to the time when the Protected Instance is running as a virtual machine in Microsoft Azure, excluding any time associated with manual action or the execution of your scripts.

Monthly Recovery Time Objective: The Monthly Recovery Time Objective for a specific Protected Instance configured for On-Premises-to-Azure replication in a given billing month is four hours for an unencrypted Protected Instance and six hours for an encrypted Protected Instance. One hour will be added to the monthly Recovery Time Objective for each additional 25GB over the initial 100GB Protected Instance size.

Service Credit (Assuming Protected Instance of 100GB, or less):

Protected Instance	Monthly Recovery Time Objective	Service Credit
Unencrypted	> 4 hours	100%
Encrypted	> 6 hours	100%

Additional Terms: Monthly Recovery Time Objective and Service Credits are calculated for each Protected Instance used by you.

Table of Contents / Definitions

Site Recovery Service – On-Premises-to-On-Premises

Additional Definitions:

"**Failover**" is the process of transferring control, either simulated or actual, of a Protected Instance from a primary site to a secondary site.

"**Failover Minutes**" is the total number of minutes in a billing month during which a Failover of a Protected Instance configured for On-Premises-to-On-Premises replication has been attempted but not completed.

"**Maximum Available Minutes**" is the total number of minutes that a given Protected Instance has been configured for On-Premises-to-On-Premises replication by the Site Recovery Service during a billing month.

"**On-Premises-to-On-Premises Failover**" is the Failover of a Protected Instance from a non-Azure primary site to a non-Azure secondary site.

"**Protected Instance**" refers to a virtual or physical machine configured for replication by the Site Recovery Service from a primary site to a secondary site. Protected Instances are enumerated in the Protected Items tab in the Recovery Services section of the Management Portal.

Downtime: The total accumulated Failover Minutes in which the Failover of a Protected Instance is unsuccessful due to unavailability of the Site Recovery Service, provided that retries are continually attempted no less frequently than once every thirty minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Additional Terms: Monthly Recovery Time Objective and Service Credits are calculated for each Protected Instance used by you.

Table of Contents / Definitions

SQL Data Warehouse Database

Additional Definitions:

"**Database**" means any SQL Data Warehouse Database.

"**Maximum Available Minutes**" is the total number of minutes that a given Database has been deployed in Microsoft Azure during a billing month in a given Microsoft Azure subscription.

"**Client Operations**" is the set of all documented operations supported by SQL Data Warehouse.

Downtime: is the total accumulated minutes during a billing month for a given Microsoft Azure subscription during which a given Database is unavailable. A minute is considered unavailable for a given Database if more than 1% of all Client Operations completed during the minute return an Error Code.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

SQL Database Service (Basic, Standard and Premium Tiers)

Additional Definitions:

"**Database**" means any single or elastic Basic, Standard, or Premium Microsoft Azure SQL Database.

"**Maximum Available Minutes**" is the total number of minutes that a given Database has been deployed in in Microsoft Azure during a billing month in a given Microsoft Azure subscription.

Downtime: is the total accumulated minutes during a billing month for a given Microsoft Azure subscription during which a given Database is unavailable. A minute is considered unavailable for a given Database if all continuous attempts to establish a connection to the Database within the minute fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

Table of Contents / Definitions

SQL Database Service (Web and Business Tiers)

Additional Definitions:

"**Database**" means any Web or Business Microsoft Azure SQL Database.

"**Deployment Minutes**" is the total number of minutes that a given Web or Business Database has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Web and Business Databases for a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated Deployment Minutes across all Web and Business Databases deployed by you in a given Microsoft Azure subscription during which the Database is unavailable. A minute is considered unavailable for a given Database if all continuous attempts by you to establish a connection to the Database within the minute fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

SQL Server Stretch Database

Additional Definitions:
"**Database**" means one instance of SQL Server Stretch Database.

"**Maximum Available Minutes**" is the total number of minutes that a given Database has been deployed in a given Microsoft Azure subscription during a billing month.

Downtime: is the total accumulated minutes across all Databases deployed by Customer in a given Microsoft Azure subscription during which the Database is unavailable. A minute is considered unavailable for a given Database if all continuous attempts by Customer to establish a connection to the Database within the minute fail.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} \, x \, 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Storage Service

Additional Definitions:
"**Average Error Rate"** for a billing month is the sum of Error Rates for each hour in the billing month divided by the total number of hours in the billing month.

"Blob Storage Account" is a storage account specialized for storing data as blobs and provides the ability to specify an access tier indicating how frequently the data in that account is accessed.

"Cool Access Tier" is an attribute of a Blob Storage Account indicating that the data in the account is infrequently accessed and has a lower availability service level than data in other access tiers.

"**Excluded Transactions**" are storage transactions that do not count toward either Total Storage Transactions or Failed Storage Transactions. Excluded Transactions include pre-authentication failures; authentication failures; attempted transactions for storage accounts over their prescribed quotas; creation or deletion of containers, tables, or queues; clearing of queues; and copying blobs between storage accounts.

"**Error Rate**" is the total number of Failed Storage Transactions divided by the Total Storage Transactions during a set time interval (currently set at one hour). If the Total Storage Transactions in a given one-hour interval is zero, the error rate for that interval is 0%.

"**Failed Storage Transactions**" is the set of all storage transactions within Total Storage Transactions that are not completed within the Maximum Processing Time associated with their respective transaction type, as specified in the table below. Maximum Processing Time includes only the time spent processing a transaction request within the Storage Service and does not include any time spent transferring the request to or from the Storage Service.

Request Types	Maximum Processing Time
PutBlob and GetBlob (includes blocks and pages) Get Valid Page Blob Ranges	Two (2) seconds multiplied by the number of MBs transferred in the course of processing the request
Copy Blob	Ninety (90) seconds (where the source and destination blobs are within the same storage account)

Request Types	Maximum Processing Time
PutBlockList GetBlockList	Sixty (60) seconds
Table Query List Operations	Ten (10) seconds (to complete processing or return a continuation)
Batch Table Operations	Thirty (30) seconds
All Single Entity Table Operations All other Blob and Message Operations	Two (2) seconds

These figures represent maximum processing times. Actual and average times are expected to be much lower.

Failed Storage Transactions do not include:

1. Transaction requests that are throttled by the Storage Service due to a failure to obey appropriate back-off principles.
2. Transaction requests having timeouts set lower than the respective Maximum Processing Times specified above.
3. Read transactions requests to RA-GRS Accounts for which you did not attempt to execute the request against Secondary Region associated with the storage account if the request to the Primary Region was not successful.
4. Read transaction requests to RA-GRS Accounts that fail due to Geo-Replication Lag.

"**Geo Replication Lag**" for GRS and RA-GRS Accounts is the time it takes for data stored in the Primary Region of the storage account to replicate to the Secondary Region of the storage account. Because GRS and RA-GRS Accounts are replicated asynchronously to the Secondary Region, data written to the Primary Region of the storage account will not be immediately available in the Secondary Region. You can query the Geo Replication Lag for a storage account, but Microsoft does not provide any guarantees as to the length of any Geo Replication Lag under this SLA.

"**Geographically Redundant Storage (GRS) Account**" is a storage account for which data is replicated synchronously within a Primary Region and then replicated asynchronously to a Secondary Region. You cannot directly read data from or write data to the Secondary Region associated with GRS Accounts.

"**Locally Redundant Storage (LRS) Account**" is a storage account for which data is replicated synchronously only within a Primary Region.

"**Primary Region**" is a geographical region in which data within a storage account is located, as selected by you when creating the storage account. You may execute write requests only against data stored within the Primary Region associated with storage accounts.

"**Read Access Geographically Redundant Storage (RA-GRS) Account**" is a storage account for which data is replicated synchronously within a Primary Region and then replicated asynchronously to a Secondary Region. You can directly read data from, but cannot write data to, the Secondary Region associated with RA-GRS Accounts.

"**Secondary Region**" is a geographical region in which data within a GRS or RA-GRS Account is replicated and stored, as assigned by Microsoft Azure based on the Primary Region associated with the storage account. You cannot specify the Secondary Region associated with storage accounts.

"**Total Storage Transactions**" is the set of all storage transactions, other than Excluded Transactions, attempted within a one-hour interval across all storage accounts in the Storage Service in a given subscription.

"**Zone Redundant Storage (ZRS) Account**" is a storage account for which data is replicated across multiple facilities. These facilities may be within the same geographical region or across two geographical regions.

Monthly Uptime Percentage: Monthly Uptime Percentage is calculated using the following formula:

$$100\% - Average\ Error\ Rate$$

Service Credit – LRS, ZRS, GRS and RA-GRS (write requests) Accounts:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Credit – RA-GRS (read requests) Accounts:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

Service Credit – LRS, GRS and RA-GRS (write requests) Blob Storage Accounts (Cool Access Tier):

Monthly Uptime Percentage	Service Credit
< 99%	10%
< 98%	25%

Service Credit – RA-GRS (read requests) Blob Storage Accounts (Cool Access Tier):

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 98%	25%

Table of Contents / Definitions

StorSimple Service

Additional Definitions:

"**Backup**" is the process of backing up data stored on a registered StorSimple device to one or more associated cloud storage accounts within Microsoft Azure.

"**Cloud Tiering**" is the process of transferring data from a registered StorSimple device to one or more associated cloud storage accounts within Microsoft Azure.

"**Deployment Minutes**" is the total number of minutes during which a Managed Item has been configured for Backup or Cloud Tiering to a StorSimple storage account in Microsoft Azure.

"**Failure**" means the inability to fully complete a properly configured Backup, Tiering, or Restoring operation due to unavailability of the StorSimple Service.

"**Managed Item**" refers to a volume that has been configured to Backup to the cloud storage accounts using the StorSimple Service.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Managed Items for a given Microsoft Azure subscription during a billing month.

"**Restoring**" is the process of copying data to a registered StorSimple device from its associated cloud storage account(s).

Downtime: The total accumulated Deployment Minutes across all Managed Items configured for Backup or Cloud Tiering by you in a given Microsoft Azure subscription during which the StorSimple Service is unavailable for the Managed Item. The StorSimple Service is considered unavailable for a given Managed Item from the first Failure of a Backup, Cloud Tiering, or Restoring operation with respect to the Managed Item until the initiation of a successful Backup, Cloud Tiering, or Restoring operation of the Managed Item, provided that retries are continually attempted no less frequently than once every thirty minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Stream Analytics – API Calls

Additional Definitions:

"**Total Transaction Attempts**" is the total number of authenticated REST API requests to manage a streaming job within the Stream Analytics Service by Customer during a billing month for a given Microsoft Azure subscription.

"**Failed Transactions**" is the set of all requests within Total Transaction Attempts that return an Error Code or otherwise do not return a Success Code within five minutes from Microsoft's receipt of the request.

"**Monthly Uptime Percentage**" for API calls within the Stream Analytics Service is represented by the following formula:

$$\text{Monthly Uptime \%} = \frac{\text{Total Transaction Attempts} - \text{Failed Transactions}}{\text{Total Transaction Attempts}}$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Stream Analytics – Jobs

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given job has been deployed within the Stream Analytics Service during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all jobs deployed by Customer in a given Microsoft Azure subscription during a billing month.

Downtime is the total accumulated Deployment Minutes, across all jobs deployed by Customer in a given Microsoft Azure subscription, during which the job is unavailable. A minute is considered unavailable for a deployed job if the job is neither processing data nor available to process data throughout the minute.

Monthly Uptime Percentage for jobs within the Stream Analytics Service is represented by the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Traffic Manager Service

Additional Definitions:

"**Deployment Minutes**" is the total number of minutes that a given Traffic Manager Profile has been deployed in Microsoft Azure during a billing month.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all Traffic Manager Profiles deployed by you in a given Microsoft Azure subscription during a billing month.

"**Traffic Manager Profile**" or "**Profile**" refers to a deployment of the Traffic Manager Service created by you containing a domain name, endpoints, and other configuration settings, as represented in the Management Portal.

"**Valid DNS Response**" means a DNS response, received from at least one of the Traffic Manager Service name server clusters, to a DNS request for the domain name specified for a given Traffic Manager Profile.

Downtime: The total accumulated Deployment Minutes, across all Profiles deployed by you in a given Microsoft Azure subscription, during which the Profile is unavailable. A minute is considered unavailable for a given Profile if all continual DNS queries for the DNS name specified in the Profile that are made throughout the minute do not result in a Valid DNS Response within two seconds.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

Table of Contents / Definitions

Virtual Machines

Additional Definitions:

“**Availability Set**” refers to two or more Virtual Machines deployed across different Fault Domains to avoid a single point of failure.

“**Fault Domain**” is a collection of servers that share common resources such as power and network connectivity.

“**Maximum Available Minutes**” is the total accumulated minutes during a billing month for all Internet facing Virtual Machines that have two or more instances deployed in the same Availability Set. Maximum Available Minutes is measured from when at least two Virtual Machines in the same Availability Set have both been started resultant from action initiated by you to the time you have initiated an action that would result in stopping or deleting the Virtual Machines.

“**Virtual Machine**” refers to persistent instance types that can be deployed individually or as part of an Availability Set.

Downtime: The total accumulated minutes that are part of Maximum Available Minutes that have no External Connectivity.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Table of Contents / Definitions

VPN Gateway

Additional Definitions:

“**Maximum Available Minutes**” is the total accumulated minutes during a billing month which a given VPN Gateway has been deployed in a Microsoft Azure subscription.

“**Virtual Network**” refers to a virtual private network that includes a collection of user-defined IP addresses and subnets that form a network boundary within Microsoft Azure.

“**VPN Gateway**” refers to a gateway that facilitates cross-premises connectivity between a Virtual Network and a customer on-premises network.

Downtime: Is the total accumulated Maximum Available Minutes during which a VPN Gateway is unavailable. A minute is considered unavailable if all attempts to connect to the VPN Gateway within a thirty-second window within the minute are unsuccessful.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Basic Gateway for VPN or ExpressRoute Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Standard Gateway for VPN or ExpressRoute / High Performance Gateway for VPN or ExpressRoute Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.95%	10%
< 99%	25%

Table of Contents / Definitions

Visual Studio Online – Build Service

Additional Definitions:

"**Build Service**" is a feature that allows customers to build their applications in Visual Studio Online.

"**Maximum Available Minutes**" is the total number of minutes for which the paid Build Service has been enabled for a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated minutes for a given Microsoft Azure subscription during which the Build Service is unavailable. A minute is considered unavailable if all continuous HTTP requests to the Build Service to perform operations initiated by you throughout the minute either result in an Error Code or do not return a response.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Visual Studio Online – Load Testing Service

Additional Definitions:

"**Load Testing Service**" is a feature that allows customers to generate automated tasks to test the performance and scalability of applications.

"**Maximum Available Minutes**" is the total number of minutes for which the paid Load Testing Service has been enabled for a given Microsoft Azure subscription during a billing month.

Downtime: The total accumulated minutes for a given Microsoft Azure subscription during which the Load Testing Service is unavailable. A minute is considered unavailable if all continuous HTTP requests to the Load Testing Service to perform operations initiated by you throughout the minute either result in an Error Code or do not return a response.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Visual Studio Online – User Plans Service

Additional Definitions:

"**Build Service**" is a feature that allows customers to build their applications in Visual Studio Online.

"**Deployment Minutes**" is the total number of minutes for which a User Plan has been purchased during a billing month.

"**Load Testing Service**" is a feature that allows customers to generate automated tasks to test the performance and scalability of applications.

"**Maximum Available Minutes**" is the sum of all Deployment Minutes across all User Plans for a given Microsoft Azure subscription during a billing month.

"**User Plan**" refers to the set of features and capabilities selected for a user within a Visual Studio Online account in a Customer subscription. User Plan options and the features and capabilities per User Plan are described on the http://www.visualstudio.com website.

Downtime: The total accumulated Deployment Minutes, across all User Plans for a given Microsoft Azure subscription, during which the User Plan is unavailable. A minute is considered unavailable for a given User Plan if all continuous HTTP requests to perform operations, other than operations pertaining to the Build Service or the Load Testing Service, throughout the minute either result in an Error Code or do not return a response.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}}\ x\ 100$$

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Other Online Services

Bing Maps Enterprise Platform

Downtime: Any period of time when the Service is not available as measured in Microsoft's data centers, provided that you access the Service using the methods of access, authentication and tracking methods documented in the Bing Maps Platform SDKs.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ number\ of\ minutes\ in\ a\ month\ -Downtime}{Total\ number\ of\ minutes\ in\ a\ month}\ x\ 100$$

where Downtime is measured as the total number of minutes during the month when the aspects of the Service set forth above are unavailable.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to Bing Maps Enterprise Platform purchased through Open Value and Open Value Subscription volume licensing agreements.

Service Credits will not apply if: (i) you fail to implement any Services updates within the time specified in the Bing Maps Platform API's Terms of Use; and (ii) you do not provide Microsoft with at least ninety (90) days' advance notice of any known significant usage volume increase, with significant usage volume increase defined as 50% or more of the previous month's usage.

Table of Contents / Definitions

Bing Maps Mobile Asset Management

Downtime: Any period of time when the Service is not available as measured in Microsoft's data centers, provided that you access the Service using the methods of access, authentication and tracking methods documented in the Bing Maps Platform SDKs.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ number\ of\ minutes\ in\ a\ month\ -Downtime}{Total\ number\ of\ minutes\ in\ a\ month}\ x\ 100$$

where Downtime is measured as the total number of minutes during the month when the aspects of the Service set forth above are unavailable.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Service Level Exceptions: This SLA does not apply to Bing Maps Enterprise Platform purchased through Open Value and Open Value Subscription volume licensing agreements.

Service Credits will not apply if: (i) you fail to implement any Services updates within the time specified in the Bing Maps Platform API's Terms of Use; and (ii) you do not provide Microsoft with at least ninety (90) days' advance notice of any known significant usage volume increase, with significant usage volume increase defined as 50% or more of the previous month's usage.

Table of Contents / Definitions

Minecraft: Education Edition

Downtime: Any period of time when users are unable to access Minecraft: Education Edition.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ number\ of\ minutes\ in\ a\ month\ -Downtime}{Total\ number\ of\ minutes\ in\ a\ month}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Power BI Embedded

Deployment Minutes: is the total number of minutes for which a given workspace collection has been provisioned during a billing month.

Maximum Available Minutes: is the sum of all Deployment Minutes across all workspace collections provisioned by a customer in a given Microsoft Azure subscription during a billing month.

Downtime: is the total accumulated Deployment Minutes, during which the workspace collection is unavailable. A minute is considered unavailable for a given workspace collection if all continuous attempts within the minute to read or write any portion of Power BI Embedded data result in an Error Code or do not return a response within five minutes.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\ -Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Table of Contents / Definitions

Power BI Pro

Downtime: Any period of time when users are unable to read or write any portion of Power BI data to which they have appropriate permissions.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ number\ of\ minutes\ in\ a\ month\ -Downtime}{Total\ number\ of\ minutes\ in\ a\ month}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Translator API

Downtime: Any period of time when users are not able to perform translations.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Total\ number\ of\ minutes\ in\ a\ month\ - Downtime}{Total\ number\ of\ minutes\ in\ a\ month}\ x\ 100$$

where Downtime is measured as the total number of minutes during the month when the aspects of the Service set forth above are unavailable.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	25%
< 99%	50%
< 95%	100%

Table of Contents / Definitions

Windows Desktop Operating System

Additional Definitions:
"**Maximum Available Minutes**" is the total accumulated minutes during a billing month for Windows ATP portal. Maximum Available Minutes is measured from when the Tenant has been created resultant from successful completion of the on-boarding process.

"**Tenant**" represents Windows ATP customer specific cloud environment.

Downtime: The total accumulated minutes that are part of Maximum Available Minutes in which the Customer unable to access any portion of a Windows ATP portal site collections for which they have appropriate permissions and customer has a valid, active, license.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{Maximum\ Available\ Minutes\ - Downtime}{Maximum\ Available\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Service Credit:

Monthly Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

Service Level Exceptions: This SLA does not apply to any trial/preview version Tenants.

Table of Contents / Definitions

Appendix A – Service Level Commitment for Virus Detection and Blocking, Spam Effectiveness, or False Positive

With respect to Exchange Online and EOP licensed as a standalone Service or via ECAL suite, or Exchange Enterprise CAL with Services, you may be eligible for Service Credits if we do not meet the Service Level described below for: (1) Virus Detection and Blocking, (2) Spam Effectiveness, or (3) False Positive. If any one of these individual Service Levels is not met, you may submit a claim for a Service Credit. If one Incident causes us to fail more than one SLA metric for Exchange Online or EOP, you may only make one Service Credit claim for that incident per Service.

1. Virus Detection and Blocking Service Level

a. "Virus Detection and Blocking" is defined as the detection and blocking of Viruses by the filters to prevent infection. "Viruses" is broadly defined as known malware, which includes viruses, worms, and Trojan horses.
b. A Virus is considered known when widely used commercial virus scanning engines can detect the virus and the detection capability is available throughout the EOP network.
c. Must result from a non-purposeful infection.
d. The Virus must have been scanned by the EOP virus filter.
e. If EOP delivers an email that is infected with a known virus to you, EOP will notify you and work with you to identify and remove it. If this results in the prevention of an infection, you won't be eligible for a Service Credit under the Virus Detection and Blocking Service Level.
f. The Virus Detection and Blocking Service Level shall not apply to:
   i. Forms of email abuse not classified as malware, such as spam, phishing and other scams, adware, and forms of spyware, which due to its targeted nature or limited use is not known to the anti-virus community and thus not tracked by anti-virus products as a virus.
   ii. Corrupt, defective, truncated, or inactive viruses contained in NDRs, notifications, or bounced emails.
g. The Service Credit available for the Virus Detection and Blocking Service is: 25% Service Credit of Applicable Monthly Service Fee if an infection occurs in a calendar month, with a maximum of one claim allowed per calendar month.

2. Spam Effectiveness Service Level

a. "Spam Effectiveness" is defined as the percentage of inbound spam detected by the filtering system, measured on a daily basis.
b. Spam effectiveness estimates exclude false negatives to invalid mailboxes.
c. The spam message must be processed by our service and not be corrupt, malformed, or truncated.
d. The Spam Effectiveness Service Level does not apply to email containing a majority of non-English content.
e. You acknowledge that classification of spam is subjective and accept that we will make a good faith estimation of the spam capture rate based on evidence timely supplied by you.
f. The Service Credit available for the Spam Effectiveness Service is:

% of Calendar Month that Spam Effectiveness is below 99%	Service Credit
>25%	25%
> 50%	50%
100%	100%

3. False Positive Service Level

a. "False Positive" is defined as the ratio of legitimate business email incorrectly identified as spam by the filtering system to all email processed by the service in a calendar month.
b. Complete, original messages, including all headers, must be reported to the abuse team.
c. Applies to email sent to valid mailboxes only.
d. You acknowledge that classification of false positives is subjective and understand that we will make a good faith estimation of the false positive ratio based on evidence timely supplied by you.
e. This False Positive Service Level shall not apply to:
   i. bulk, personal, or pornographic email
   ii. email containing a majority of non-English content
   iii. email blocked by a policy rule, reputation filtering, or SMTP connection filtering

iv. email delivered to the junk folder

f. The Service Credit available for the False Positive Service is:

False Positive Ratio in a Calendar Month	Service Credit
> 1:250,000	25%
> 1:10,000	50%
> 1:100	100%

Appendix B - Service Level Commitment for Uptime and Email Delivery

With respect to EOP licensed as a standalone Service, ECAL suite, or Exchange Enterprise CAL with Services, you may be eligible for Service Credits if we do not meet the Service Level described below for (1) Uptime and (2) Email Delivery.

1. **Monthly Uptime Percentage**:
   If the Monthly Uptime Percentage for EOP falls below 99.999% for any given month, you may be eligible for the following Service Credit:

Monthly Uptime Percentage	Service Credit
<99.999%	25%
<99.0%	50%
<98.0%	100%

2. **Email Delivery Service Level**:
   a. "Email Delivery Time" is defined as the average of email delivery times, measured in minutes over a calendar month, where email delivery is defined as the elapsed time from when a business email enters the EOP network to when the first delivery attempt is made.
   b. Email Delivery Time is measured and recorded every 5 minutes, then sorted by elapsed time. The fastest 95% of measurements are used to create the average for the calendar month.
   c. We use simulated or test emails to measure delivery time.
   d. The Email Delivery Service Level applies only to legitimate business email (non-bulk email) delivered to valid email accounts.
   e. This Email Delivery Service Level does not apply to:
      1. Delivery of email to quarantine or archive
      2. Email in deferral queues
      3. Denial of service attacks (DoS)
      4. Email loops
   f. The Service Credit available for the Email Delivery Service is:

Average Email Delivery Time (as defined above)	Service Credit
> 1	25%
> 4	50%
> 10	100%