



County of Los Angeles
INTERNAL SERVICES DEPARTMENT

1100 North Eastern Avenue
Los Angeles, California 90063

SELWYN HOLLINS
Director

"Trusted Partner and Provider of Choice"

Telephone: (323) 267-2101
FAX: (323) 264-7135

June 14, 2022

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, CA 90012

Dear Supervisors:

ADOPTED

BOARD OF SUPERVISORS
COUNTY OF LOS ANGELES

51 June 14, 2022

CELIA ZAVALA
EXECUTIVE OFFICER

**REQUEST TO AWARD AND EXECUTE A SOLE SOURCE CONTRACT FOR
MICROSOFT UNIFIED SUPPORT AND CONSULTING SERVICES
(ALL DISTRICTS – 3 VOTES)**

CIO RECOMMENDATION: APPROVE (X)

SUBJECT

Request delegated authority to Internal Services Department (ISD) to award and execute a Unified Support and Consulting Services sole source contract with Microsoft Corporation (Microsoft) to provide as-needed technical professional services and proactive/reactive proprietary services that support the County's Microsoft environment.

IT IS RECOMMENDED THAT THE BOARD:

1. Authorize the Director of ISD, or designee, to award and execute the recommended contract (Attachment 1), with Microsoft to provide Unified Support and Consulting Services for an initial contract term of two-years, commencing upon execution, with six one-year renewal options, and six additional month-to-month extensions. The total amount authorized for expenditure under this contract shall not exceed \$13 million per calendar year during the term of the contract.
2. Authorize the Director of ISD, or designee, to (i) exercise the renewal options and month-to-month extensions in accordance with the recommended contract; (ii) upon review and approval as to from by County Counsel, execute applicable amendments to the contract to make necessary changes which affects the

statements of work to add/delete services and/or features to existing Unified service packages, make changes to the pricing schedules, and/or revise the terms and conditions to align with Board policy changes and directives; (iii) execute applicable contract amendments should the original contracting entity merge, be acquired, or otherwise have a change of entity; (iv) execute individual Work Orders (WO) and/or Statements of Services (SOS) on behalf of County departments; and (v) to amend, delete, and/or replace any Exhibits to the contract to approve programmatic and/or administrative workflow changes needed to effectively manage the contract.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTIONS

The maintenance/support that comes with Microsoft commercial software licenses is limited to software updates, bug fixes, and software/security patches. As such, County departments have been acquiring Microsoft support services through support specific contracts since 2005.

On June 30, 2015, the Board of Supervisors (Board) approved the current Premier Support Services (PSS) contract with Microsoft which provides access to internal Microsoft resources and highly technical advisory and support services to County departments. The current PSS contract, which is administered by ISD, expires on June 29, 2022, and provides services such as technical planning and assessments, third-tier product support, direct high-end technical engineering resources and dedicated design and deployment services of Microsoft products and technologies.

Microsoft is the sole provider for certain proprietary Microsoft support and consulting services. The proprietary services are developed in conjunction with Microsoft product groups and contain intellectual property that can only be provided by Microsoft. The scope of services in the recommended contract will allow Microsoft to provide support services to the County to address emergent and time-sensitive consulting and performance management needs. Therefore, a sole source contract with Microsoft is necessary to ensure that essential support services continue to be available. Additionally, the recommended contract will allow the County to transition from PSS and take advantage of solutions provided under the new Microsoft Unified Support Services program.

Approval of recommendation number one will allow the County to continue contracting with Microsoft to provide Unified Support and Consulting Services for County departments under the new Unified Program. The recommended contract will also streamline the County's contracting and monitoring process, utilizing a single contract

to provide services with a single set of terms and conditions, instead of departments individually negotiating contracts or purchase orders for such services.

Recommendation number two requests delegated authority to the Director of ISD, or designee, to execute amendments to exercise renewal options and month-to-month extensions, make necessary changes that affect the statements of work to ensure that the County aligns with the ever-changing IT needs, make changes to the pricing schedules, execute individual WO and/or SOS on behalf of County departments, and execute administrative contract amendments to effectively manage the contract.

IMPLEMENTATION OF STRATEGIC PLAN GOALS

The recommended actions support the County Strategic Plan III.2.1 Enhance Information Technology Platforms to Securely Share and Exchange Data; Goal III.2.2 Leverage Technology to Increase Visibility of and Access to Services; and Goal III.2.3 Prioritize and Implement Technology Initiatives That Enhance Service Delivery and Increase Efficiency; Goal III.2, Embrace Digital Government for the Benefit of our Internal Customers and Communities to ensure that each department maximizes the use of technology to raise awareness of available programs and services; and Goal III.3 Operational Effectiveness, Fiscal Responsibility, and Accountability, by maximizing the effectiveness of the County's processes and operations and effectively managing County resources to provide efficient and responsive Microsoft support services in the County.

FISCAL IMPACT/FINANCING

The recommended contract shall not exceed \$13 million per calendar year during the term of the contract. The recommended contract does not guarantee any minimum amount of work to Microsoft. The County only incurs obligations as individual WOs/SOSs are awarded. Work will only be awarded where sufficient budgeted funds are available from the County departments requesting Microsoft support services.

The Microsoft compensation for work performed under the recommended contract is based on a percentage fee of the County's historical spend under three service categories, i) server products, ii) user products and iii) Azure, the County's cloud computing service operated by Microsoft through Microsoft-managed data centers, and fixed hourly rates for as-needed professional support and consulting services. Microsoft's hourly rates cannot exceed the maximum rates set forth in the recommended contract. Microsoft's percentage fee and hourly rates are fixed for the first year of the contract. Rates can be increased up to a maximum of three percent,

if requested and only if Microsoft has applied such rate increases to its published Public Sector Rates for the then-current fiscal year.

Expenditures under the recommended contract will vary from year-to-year based on the needs of County departments, and County departments are responsible for ensuring they have adequate funding prior to requesting services under the recommended contract. County departments with an executed WO and/or SOS shall be responsible for ensuring that services do not exceed the amount, scope of work, and period of performance specified in the executed WO and/or SOS.

Funding for these services is included in ISD's and other County departments' Fiscal Year 2021-22 Adopted Budgets, and sufficient appropriation will be requested in the future years. Expenditures over the term of the contract in any given year will remain within each departments' budgeted appropriation for such services.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The recommended contract has been approved as to form by County Counsel and it includes suitable terms and conditions to protect the County. ISD worked closely with County Counsel to negotiate the most advantageous and commercially responsible terms possible for the County, with the original 2015 contract terms and conditions remaining substantially unchanged.

The recommended contract contains the required Board policy provisions, including those pertaining to consideration of qualified County employees targeted for layoff as well as qualified GAIN/GROW participants for employment openings, compliance with the Jury Duty Ordinance, Safely Surrender Baby Law, Child Support Program, and Zero Tolerance Human Trafficking. The recommended contract also contains provisions for assignment and delegation, compliance with applicable law, force majeure, indemnification, Public Records Act compliance, termination for default, and compliance with the Health Insurance Portability and Accountability Act of 1996.

Given that this is also an IT contract, appropriate provisions were included for confidentiality, the handling of security incidents, and the required limits of applicable insurance for network security and privacy liability, and technology errors and omissions coverage are also included.

Due to the highly specialized and technical nature of the contracted services, these services cannot be provided by County personnel. Accordingly, the recommended contract is not a Proposition A contract and is not subject to the Living Wage Program (County Code Chapter 2.221). ISD has determined that the services under the

recommended contract do not impact Board Policy No. 5.030, "Low-Cost Labor Resource Program", due to the specialized nature of the services.

In compliance with Board Policy 6.020 "Chief Information Office Board Letter Approval", the Office of the Chief Information Officer (OCIO) reviewed the information technology (IT) components of this request and recommends approval. The OCIO determined this recommended action does not include any new IT items that would necessitate a formal CIO Analysis.

CONTRACTING PROCESS

On October 15, 2021, ISD released a Request for Information to survey the market for companies that can provide both support and consulting services for Microsoft products and technologies to determine the feasibility of releasing a competitive solicitation for the replacement services. Based on the responses received, it is ISD's intent to unbundle those services that are not proprietary to Microsoft and divide the contracted services into multiple smaller contracts as a viable procurement strategy to encourage small, local, and diverse business utilization. However, there will still be a need for the recommended sole source contract with Microsoft to provide technical engineering resources and support services for customized and proprietary software.

On November 3, 2021, in compliance with Board Policy 5.100, Sole Source Contracts, ISD provided notification to the Board (Attachment 2) of its intent to enter into sole source negotiations for a contract with Microsoft to replace the existing PSS contract, which provides highly technical advisory and support services for County departments. The notice was within the time frames required by the policy. During the contract development and negotiations process ISD worked closely with the CIO and County Counsel to ensure the contract best meets the needs of the County. In accordance with the Board's Policy, the Sole Source Justification, and corresponding Sole Source Checklist (Attachment 3) has been reviewed and approved by the Chief Executive Office.

A summary of the Community Business Enterprise Program information for the recommended Contractor is included (Attachment 4).

The provisions represent the best positions that could be reached by the parties involved and are similar to the provisions previously approved by the Board in the current 2015 contract. The recommended contract represents a minimal risk position for the County.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

To ensure that ISD best meets the needs of its customers and to improve Microsoft services for County departments, the recommended contract will transition the County from the current PSS contracting model to the new Unified Support contracting model where the County can access enhanced Microsoft services and solutions.

Approval of recommendations will allow the County to continue contracting with Microsoft to provide Unified Support and Consulting Services for County departments, and it will enable ISD to continue providing County departments with critical Microsoft support services without disruption.

CONCLUSION

Upon approval by the Board, it is requested that the Executive Office, Board of Supervisors return one stamped copy of the approved Board Letter to the Director of ISD.

Respectfully submitted,



SELWYN HOLLINS
Director

Reviewed by,



PETER LOO
Acting Chief Information Officer

SH:MO:LG:CC:ew

Attachments

c: Executive Office, Board of Supervisors
 Chief Executive Office
 Chief Information Office
 ISD Board Deputies
 County Counsel



CONTRACT BY AND BETWEEN
COUNTY OF LOS ANGELES
AND
MICROSOFT CORPORATION
FOR
MICROSOFT UNIFIED SUPPORT AND CONSULTING
SERVICES

TABLE OF CONTENTS		
PARAGRAPH	TITLE	PAGE
RECITALS		1
1	APPLICABLE DOCUMENTS	2
2	DEFINITIONS	3
	2.1 Standard Definitions	3
3	WORK	7
4	TERM OF CONTRACT	8
5	CONTRACT SUM	8
	5.1 Total Contract Sum	8
	5.2 Written Approval for Reimbursement	9
	5.3 Notification of 75% of Total Contract Sum	9
	5.4 No Payment for Services Provided Following Expiration-Termination of Contract	9
	5.5 Fee Schedule	9
	5.6 Invoices and Payments	10
	5.7 Work Approval and Acceptance	12
	5.8 Warranty	15
	5.9 County Approval of Invoices	16
	5.10 Default Method of Payment: Direct Deposit or Electronic Funds Transfer	16
6	ADMINISTRATION OF CONTRACT- COUNTY	17
	6.1 County Administration	17
	6.2 County's Program Director	17
	6.3 County's Program Manager	18
	6.4 County's Project Manager	19
7	ADMINISTRATION OF CONTRACT-CONTRACTOR	20
	7.1 Contractor Administration	20
	7.2 Contractor's Project Manager	21
	7.3 Contractor's Support Practice Manager	21
	7.4 Contractor's Services Account Executive	21
	7.5 Approval of Contractor's Staff	23
	7.6 Contractor's Staff Identification	23
	7.7 Background and Security Investigations	23
	7.8 Confidentiality	24
8	STANDARD TERMS AND CONDITIONS	27

8.1	Amendments.....	27
8.2	Assignment and Delegation/Mergers or Acquisitions.....	28
8.3	Authorization Warranty	29
8.4	Budget Reductions	29
8.5	Complaints.....	29
8.6	Compliance with Applicable Law	30
8.7	Compliance with Civil Rights Laws	31
8.8	Compliance with the County's Jury Service Program	32
8.9	Conflict of Interest.....	33
8.10	Consideration of Hiring County Employees Targeted for Layoffs or are on a County Re-Employment List	34
8.11	Consideration of Hiring GAIN-GROW Participants	34
8.12	Contractor Responsibility and Debarment	35
8.13	Contractor's Acknowledgement of County's Commitment to Safely Surrendered Baby Law	37
8.14	Contractor's Warranty of Adherence to County's Child Support Compliance Program	38
8.15	County's Quality Assurance Plan.....	38
8.16	Damage to County Facilities, Buildings or Grounds.....	39
8.17	Employment Eligibility Verification	39
8.18	Counterparts and Electronic Signatures and Representations	40
8.19	Fair Labor Standards	40
8.20	Force Majeure.....	40
8.21	Governing Law, Jurisdiction, and Venue.....	41
8.22	Independent Contractor Status	41
8.23	Indemnification.....	42
8.24	General Provisions for all Insurance Coverage.....	43
8.25	Insurance Coverage	46
8.26	Reserved	48
8.27	Reserved	48
8.28	Nondiscrimination and Affirmative Action.....	48
8.29	Non Exclusivity	49
8.30	Notice of Delays.....	50
8.31	Notice of Disputes.....	50

8.32	Notice to Employees Regarding the Federal Earned Income Credit.....	50
8.33	Notice to Employees Regarding the Safely Surrendered Baby Law	50
8.34	Notices	51
8.35	Prohibition Against Inducement or Persuasion	51
8.36	Public Records Act	51
8.37	Publicity	52
8.38	Record Retention and Inspection-Audit Settlement	52
8.39	Recycled Bond Paper	53
8.40	Subcontracting.....	54
8.41	Termination for Breach of Warranty to Maintain Compliance with County's Child Support Compliance Program.....	55
8.42	Termination for Convenience.....	56
8.43	Termination for Default	56
8.44	Termination for Improper Consideration	58
8.45	Termination for Insolvency.....	58
8.46	Termination for Non-Adherence of County Lobbyist Ordinance.....	59
8.47	Termination for Non-Appropriation of Funds.....	59
8.48	Validity	60
8.49	Waiver.....	60
8.50	Warranty Against Contingent Fees	60
8.51	Warranty of Compliance with County's Defaulted Property Tax Reduction Program	60
8.52	Termination for Breach of Warranty to Maintain Compliance with County's Defaulted Property Tax Reduction Program	61
8.53	Time off for Voting	61
8.54	Compliance with County's Zero Tolerance Policy on Human Trafficking .	61
8.55	Gratuitous Efforts	62
8.56	Compliance with Fair Chance Employment Practices	62
8.57	Compliance with the County Policy of Equity.....	62
8.58	Prohibition from Participation in Future Solicitation(s).....	63
8.59	COVID-19 Vaccinations of County Contractor Personnel.....	63

8.60	Limitation of Liability.....	65
8.61	Effect of Termination.....	67
8.62	Severability.....	67
8.63	Third Party Beneficiary.....	68
9	UNIQUE TERMS AND CONDITIONS.....	68
9.1	Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) ...	68
9.2	Ownership of Materials, Software and Copyright.....	69
9.3	Patent, Copyright and Trade Secret Indemnification	71
9.4	Data Destruction.....	73
9.5	Products and Services Data Protection Addendum.....	73
9.6	Reimbursement for County's Mitigation Costs.....	74
10	SURVIVAL.....	74
	SIGNATURES	76

STANDARD EXHIBITS

- A-1 Statement of Work-Microsoft Unified Product Support Description
- A-2 Statement of Work-Microsoft Consulting Support Description
- A-3 Additional Definitions and Terms and Conditions
- A-4 Customer Service Request for Services Process
- A-5 Acceptance Certificate Form
- A-6 Microsoft Unified Support Sample Work Order
- A-7 Microsoft Consulting Services Sample Statement of Services
- A-8 Microsoft Sample Customer Status Report
- B-1 Microsoft Unified Support Published Price List
- B-2 Microsoft Consulting Services Published Price List
- C County's Work Order/Statement of Services Process
- D Contractor's EEO Certification
- E County's Administration
- F Contractor's Administration
- G COVID-19 Vaccination Certification of Compliance
- G1-IT Contractor Acknowledgement and Confidentiality Agreement
- H Jury Service Ordinance
- I Safely Surrendered Baby Law

UNIQUE EXHIBITS

INFORMATION SECURITY AND PRIVACY REQUIREMENTS

- J Information Security and Privacy Requirements
- K Microsoft Products and Services Data Protection Addendum

**CONTRACT BETWEEN
COUNTY OF LOS ANGELES
AND
MICROSOFT CORPORATION
FOR
MICROSOFT UNIFIED SUPPORT AND CONSULTING SERVICES**

This Contract ("Contract") made and entered into this ____ day of _____, 2022 by and between the County of Los Angeles, hereinafter referred to as County and Microsoft Corporation, hereinafter referred to as "Contractor". Microsoft Corporation is located at 1 Microsoft Way, Redmond, WA 98052.

RECITALS

WHEREAS, the County may contract with private businesses for certain technology support services, referred to as Microsoft Unified Support and Consulting Services ("Services") for the purposes of this Contract, when certain requirements are met; and

WHEREAS, the Contractor is a private sector (though publicly traded) firm specializing in providing Microsoft Unified Support and Consulting Services; and

WHEREAS, the Services will be acquired by County Departments on an individual basis through Work Orders under the administration and with the approval of the Internal Services Department (ISD) Director, or his/her designee; and

WHEREAS, this Contract is for Services that are technical and highly specialized, are provided on an intermittent basis, cannot be performed by current County employees or by individuals who could be recruited; and

WHEREAS, this Contract is authorized under the California Government Code Section 31000, which authorizes the Board of Supervisors to contract for special services; and

NOW THEREFORE, in consideration of the mutual covenants contained herein, and for good and valuable consideration, the parties agree to the following:

1 APPLICABLE DOCUMENTS

Exhibits A, B, C, D, E, F, G, H, I, J and K are attached to and form a part of this Contract. In the event of any conflict or inconsistency in the definition or interpretation of any word, responsibility, schedule, or the contents or description of any task, deliverable, goods, service, or other work, or otherwise between the base Contract and the Exhibits, or between Exhibits, such conflict or inconsistency shall be resolved by giving precedence first to the terms and conditions of the Contract and then to the Exhibits according to the following priority.

Standard Exhibits:

- 1.1 A-1 Statement of Work-Microsoft Unified Product Support Description
- 1.2 A-2 Statement of Work-Microsoft Consulting Support Description
- 1.3 A-3 Additional Definitions and Terms and Conditions
- 1.4 A-4 Customer Service Request for Services Process
- 1.5 A-5 Acceptance Certificate Form
- 1.6 A-6 Microsoft Unified Support Sample Work Order
- 1.7 A-7 Microsoft Consulting Services Sample Statement of Services
- 1.8 A-8 Microsoft Customer Status Report
- 1.9 B-1 Microsoft Unified Support Published Price List
- 1.10 B-2 Microsoft Consulting Services Published Price List
- 1.11 C County's Work Order/SOS Request Process
- 1.12 D Contractor's EEO Certification
- 1.13 E County's Administration
- 1.14 F Contractor's Administration
- 1.15 G COVID-19 Vaccination Certification of Compliance
- 1.16 G1-IT Contractor Acknowledgement and Confidentiality Agreement
- 1.17 H Jury Service Ordinance
- 1.18 I Safely Surrendered Baby Law

Unique Exhibits:

Information Security and Privacy Requirements Exhibit

- 1.19 J Information Security and Privacy Requirements

1.20 K Microsoft Products and Services Data Protection Addendum

This Contract constitutes the complete and exclusive statement of understanding between the parties, and supersedes all previous contracts, written and oral, and all communications between the parties relating to the subject matter of this Contract. No change to this Contract shall be valid unless prepared pursuant to Paragraph 8.1 (Amendments) and signed by both parties.

2 DEFINITIONS

2.1 Standard Definitions:

2.1.1 The headings herein contained are for convenience and reference only and are not intended to define the scope of any provision thereof. The following words as used herein shall be construed to have the following meaning, unless otherwise apparent from the context in which they are used.

2.1.1.1 Acceptance: The County's issuance of a written Acceptance Certificate or the process by which County approves the Services, as more fully described in the applicable Work Order (WO) or Statement of Services (SOS).

2.1.1.2 Acceptance Certificate: The notice County shall issue to Contractor indicating that Contractor has resolved the subject problem or issues. A form of the Acceptance Certificate is attached as Exhibit A-5.

2.1.1.3 Acceptance Criteria: The mutually agreed upon standards set forth in each applicable WO and/or SOS.

2.1.1.4 Acceptance Test: The mutually agreed upon process and procedures by which the parties will determine the Services meet the acceptance criteria. Where no Acceptance Tests are included in a WO and/or SOS, the Services shall be deemed accepted upon completion and delivery to County, and County's review and issuance of an Acceptance Certificate.

2.1.1.5 Board of Supervisors (Board): The Board of

Supervisors of the County of Los Angeles acting as governing body.

- 2.1.1.6 **Confidential Information:** Information marked or otherwise identified in writing by a party as proprietary or confidential or that, under the circumstances surrounding the disclosure would be considered proprietary or confidential by a reasonable person acting in good faith. It includes, but is not limited to, non- public information regarding each party's business processes, products, features, marketing and promotions. Confidential Information does not include information which:(i) the recipient developed independently; (ii) the recipient knew before receiving it from the other party; or (iii) is, or subsequently becomes publicly available, or is received from another source, in both cases other than by a breach of an obligation of confidentiality under this Contract.
- 2.1.1.7 **Contract or Agreement:** This agreement executed between County and Contractor. Included are all supplemental agreements amending or extending the service to be performed. The Contract sets forth the terms and conditions for the issuance and performance of all tasks, deliverables, services and other work.
- 2.1.1.8 **Contractor:** The person or persons, sole proprietor, partnership, joint venture, corporation or other legal entity who has entered into an agreement with the County to perform or execute the work covered by this Contract.
- 2.1.1.9 **County Department:** A department or any other administrative body as defined in Los Angeles County Code Title 2 -"Administration", any named County department as well as related agencies and/or related districts who will acquire the Services pursuant to a Work Order and/or Statement of Services. County Department shall also include any governmental entity for which the Board of Supervisors is the governing board.

- 2.1.1.10 **County Program Director:** Person designated by County with authority for County on contractual or administrative matters relating to this Contract that cannot be resolved by the County's Project Manager. In the case of this Contract, the County Program Director shall mean the County of Los Angeles Internal Services Department Contracting Division Manager, or designee.
- 2.1.1.11 **County Program Manager:** Person designated by County's Program Director to manage the operations under this Contract.
- 2.1.1.12 **County Project Manager:** Person designated by each County Department with responsibility for day-to-day supervision of any and all Services provided by Contractor under each WO and/or SOS issued by such Department. The County Project Manager shall be designated by each County Department in each SOS or Work Order.
- 2.1.1.13 **Contractor Project Manager:** The person designated by the Contractor to administer the Contract operations under this Contract.
- 2.1.1.14 **Contractor's Support Practice Manager:** The individual designated by Contractor with responsibility for the day-to-day supervision of Contractor's satisfactory performance of its responsibilities under WOs issued under this Contract.
- 2.1.1.15 **Contractor Services Account Executive:** The individual designated by Contractor with overall responsibility of administration of the Contract.
- 2.1.1.16 **Day(s):** Calendar Day(s) unless otherwise specified.
- 2.1.1.17 **Decrement:** Debit against prepaid fees.
- 2.1.1.18 **Deficiency:** Any of the following: (i) nonconformance with the specifications and functional requirements in an applicable WO and/or SOS, (ii) defects(s) in Services relating to design, materials or workmanship, (iii) error(s), omission(s), failure(s) to meet any

standards set forth in any WO and/or SOS, or (iv) other problem(s) which result in the services not meeting the Acceptance Criteria established in the applicable WO and/or SOS.

2.1.1.19 **Effective Date:** The date of approval of this Contract by County's Board of Supervisors.

2.1.1.20 **ISD:** The term "ISD" shall mean County of Los Angeles Internal Services Department.

2.1.1.19 **Fiscal Year:** The twelve (12) month period beginning July 1st and ending the following June 30th.

2.1.1.20 **Services:** The Microsoft Unified Support Services as described in Exhibit A-1 and Microsoft Consulting Services as described in Exhibit A-2 shall include all associated tasks and deliverables (e.g, reports, fixes, etc.) and Service Deliverables (as defined in Exhibit A-3 (Additional Terms and Conditions), as applicable.

2.1.1.21 **Statement of Work:** The description of work, services offered, directions, provisions, and requirements provided herein and special provisions pertaining to the method, frequency, manner and place of performing the contract services.

2.1.1.22 **Subcontract:** An agreement by the Contractor to employ a Subcontractor to provide services to fulfill this Contract, if approved by the County.

2.2.1.23 **Subcontractor:** Any individual, person or persons, sole proprietor, firm, partnership, joint venture, corporation, or other legal entity furnishing supplies, services of any nature, equipment, and/or materials to contractor in furtherance of contractor's performance of this contract, at any tier, under oral or written agreement.

2.2.2.24 **Work Order (WO) and/or Statement of Services (SOS):** A subordinate agreement document issued by County to the Contractor executed wholly within and subject to the provisions of this Contract, for the performance of Services and associated tasks and deliverables. No work shall be performed by

Contractor except in accordance with an executed WO and/or SOS and in accordance with Paragraph 3 (Work) and Exhibits A-1 and A-2.

3 WORK

- 3.1 Pursuant to the provisions of this Contract, the Contractor shall fully perform, complete and deliver on time, all tasks, deliverables, services and other work as set forth in: (i) this Contract and as more fully set forth in Exhibit A-1, Microsoft Unified Product Support and each WO and, (i) Exhibit A-2, Microsoft Consulting Services and each SOS.
- 3.2 If the Contractor provides any tasks, deliverables, goods, services, or other work, other than as specified in this contract, the same shall be deemed to be a gratuitous effort on the part of the contractor, and the Contractor shall have no claim whatsoever against the County.
- 3.3 Services shall be acquired by ISD for individual County Departments and through issuance of a WO and/or SOS that has been approved and executed by County's Program Director and Contractor. Following approval and execution, each WO and/or SOS shall be issued to Contractor by County's Program Director in accordance with the procedures set forth in Sub-paragraph 3.4.
- 3.4 When a County Department has identified a need for Services it shall first consult with ISD County Program Manager to decide how best to fulfill that need under this Contract and then complete a draft ISD WO and/or SOS, which it shall submit to the County Program Manager for review. County will contact Contractor to review the required services and WO and/or SOS draft. Contractor shall not be authorized to begin work under an ISD WO and/or SOS and County shall not be obligated to pay Contractor for any work done under a WO and/or SOS unless and until County Program Director has approved the WO and/or SOS and it has been issued to and executed by Contractor's Contract Manager.
- 3.5 ISD will act as the central coordinate to administer and track all Services awarded under this Contract. County Departments acquiring Services under this Contract will monitor and manage the performance of such Services.
- 3.6 Changes to an executed WO and/or SOS by County Program Manager, must be made through a WO and/or SOS Amendment pursuant to Sub- paragraph 8.1.5.

4 TERM OF CONTRACT

- 4.1 The term of this Contract shall be two (2) years commencing after execution by County's Board of Supervisors, unless sooner terminated or extended, in whole or in part, as provided in this Contract.
- 4.2 The County shall have the sole option to extend this Contract term for up to six (6) additional one (1) year periods and six (6) month to month extensions, for a maximum total Contract term of eight (8) years and six (6) months. Each extension option may be exercised at the sole discretion of the ISD's Department Head or his/her designee as authorized by the Board of Supervisors.

The County maintains a database that track/monitor contractor performance history. Information entered into the database may be used for a variety of purposes, including determining whether the County will exercise a contract term extension option.

- 4.3 The Contractor shall notify ISD when this Contract is within six (6) months of the expiration of the term as provided for hereinabove. Upon occurrence of this event, the Contractor shall send written notification to ISD at the address herein provided in Exhibit E - County's Administration.
- 4.4 Notwithstanding any other provisions of this Paragraph 4 (Term of Contract), for any WO and/or SOS issued prior to this Contract's expiration date, with an expiration date subsequent to the Contract's termination date, then the terms and conditions of this Contract shall survive in full force and effect as to such particular WO and/or SOS up to the WO and/or SOS expiration date; provided, however, that such extended Contract expiration date shall apply to such WO and/or SOS only, shall not extend such date for any other purpose whatsoever, including issuing a new or amended WO and/or SOS or extending any other WO and/or SOS; and that such WO and/or SOS has not been terminated by County in accordance with this Contract.

5 CONTRACT SUM

5.1 Total Contract Sum

- 5.1.1 Contractor shall provide Services at the rates listed in Exhibit B-1 and B-2, Pricing Schedule for total maximum amount of this Contract for each calendar year. The Maximum Contract Sum shall not exceed \$13 million dollars per calendar year for the term of this Contract.

5.2 Written Approval for Reimbursement

5.2.1 The Contractor shall not be entitled to payment or reimbursement for any tasks or services performed, nor for any incidental or administrative expenses whatsoever incurred in or incidental to performance hereunder, except as specified herein. Assumption or takeover of any of the Contractor's duties, responsibilities, or obligations, or performance of same by any person or entity other than the Contractor, whether through assignment, subcontract, delegation, merger, buyout, or any other mechanism, with or without consideration for any reason whatsoever, shall not occur except with the County's express prior written approval.

5.3 Notification of 75% of Total Contract Sum

The Contractor shall maintain a system of record keeping that will allow the Contractor to determine when it has incurred seventy-five percent (75%) of the total contract sum under this Contract. Upon occurrence of this event, the Contractor shall send written notification to ISD at the address herein provided in Exhibit E, County's Administration.

5.4 No Payment for Services Provided Following Expiration-Termination of Contract

5.4.1 The Contractor shall have no claim against County for payment of any money or reimbursement, of any kind whatsoever, for any service provided by the Contractor after the expiration or other termination of this Contract. Should the Contractor receive any such payment it shall immediately notify County and shall immediately repay all such funds to County. Payment by County for services rendered after expiration-termination of this Contract shall not constitute a waiver of County's right to recover such payment from the Contractor. This provision shall survive the expiration or other termination of this Contract.

5.5 Fee Schedule

5.5.1 The fees for the Services provided hereunder are set forth on the Microsoft Unified Support Published Price list in Exhibit B-1 and Microsoft Consulting Services Published Price List in Exhibit B-2.

5.6 Invoices and Payments

- 5.6.1 The Contractor shall invoice the County only for providing the tasks, deliverables, goods, services, and other work specified in Exhibit A-1 and A-2, Statement of Work and elsewhere hereunder. The Contractor shall prepare invoices, which shall include the charges owed to the Contractor by the County under the terms of this Contract. The Contractor's payments shall be as provided in Exhibit B-1 and B-2 (Published Pricing Lists) and the Contractor shall be paid only for the tasks, deliverables, goods, services, and other work approved in writing by the County. Contractor shall invoice the County after issuance of each WO and/or SOS pursuant to Paragraph 3 (Work). Each invoice shall state the costs of the Services specified in the County Department WO and/or SOS. If the County does not approve work in writing no payment shall be due to the Contractor for that work.
- 5.6.2 The Contractor's invoices shall be priced in accordance with Exhibit B-1 and B-2 (Published Pricing Lists).
- 5.6.3 The Contractor's invoices shall contain the information set forth in Exhibit A-1 and A-2 (Statement of Work) describing the tasks, deliverables, goods, services, work hours, and facility and/or other work for which payment is claimed.
- 5.6.4 The Contractor shall submit the monthly invoices to the County by the 15th calendar day of the month following the month of service.
- 5.6.5 All invoices under this Contract shall be submitted in two (2) copies to the following address:
- Internal Services Department
9150 Imperial Hwy., MS:46
Downey, CA 90242
Email: bcuellar@isd.lacounty.gov
Attention: Brianna Cuellar
- 5.6.7 Submission of invoices

In order for Contractor to invoice the County for the County Department's WO and/or SOS payment, the WO and/or SOS must have been reviewed and approved by the County Project Manager and County Program Manager and issued to Contractor as is provided in Exhibit C ("County's Work

Order Process"). Contractor shall submit its invoice for approval and payment to the County Project Manager for each WO and/or SOS along with a copy of the approved WO and/or SOS. Contractor shall also provide copies of these documents to the County Program Manager. Each invoice shall contain, to the extent not already set forth in the WO and/or SOS accompanying the invoice, the information required in Sub-paragraph 5.6.3.

5.6.8 Customer Status Report

For each WO and/or SOS, Contractor shall, on a monthly basis, submit its Reporting Form ("Report") in the format shown in Exhibit A-8 ("Microsoft Customer Status Report") to the applicable County Project Manager with a copy to the County Program Manager. Each Report shall include at least:

- 5.6.8.1 The identifying County number of this Contract;
- 5.6.8.2 The identifying number or other designation of the WO and/or SOS as mutually agreed to by County and Contractor;
- 5.6.8.3 A description of the Services provided for which Decrement is claimed;
- 5.6.8.4 The name(s) and titles of the individuals(s) who performed the work;
- 5.6.8.5 The total amount of the invoiced services;
- 5.6.8.6 The amount of the "Total Maximum Amount" remaining on the WO and/or SOS after subtracting previously billed and current charges;
- 5.6.8.7 Any other relevant information requested by County.

5.6.9 Invoice Related Disputes.

If disputes arise between the parties regarding invoices or Decrements and are not resolved within thirty (30) calendar days, the parties shall follow the procedures set forth in Sub-Paragraph 8.31 (Notice of Disputes).

- 5.6.10 All invoices submitted by the Contractor for payment must have the written approval of the County Project Manager prior to any payment thereof. In no event shall the County be

liable or responsible for any payment prior to such written approval. Approval for payment will not be unreasonably withheld.

5.6.11 County shall not pay Contractor for any amounts not specified in each applicable WO and/or SOS. County shall not, under any circumstances, pay Contractor separately for any travel time, vacation, sick leave, per diem, expenses, and/or any other costs and/or out-of-pocket expenses for any services rendered under this Contract or any WO and/or SOS issued hereunder.

5.6.12 County shall not pay Contractor for any sales taxes, duties, tariffs, levies or other governmental charges or expenses (including, without limitation, any value added taxes) to which such fees are subject. Contractor is responsible for taxes based on its personal property ownership and/or net income.

5.6.13 Commencing on the Effective Date of this Contract, County shall pay fees to Contractor in accordance with the rates set forth in Exhibits B-1 and B-2. On the first and each following anniversary Effective Date, and for the remaining term of this Contract, the fees set forth in Exhibit B-1 and B-2 can be increased by the percentage increase, if any, up to a maximum of three percent (3%), if requested and Contractor has provided County with documentation that Contractor has applied the same rate increase to its published Public Sector Rates for the then-current Contractor fiscal year. Upon request by the County Project Manager or County Program Manager, the parties will cooperate and timely execute a written amendment to this Contract before any increase takes effect and becomes part of this Contract. Any such fee increases shall be applied only to WOs or SOSs executed after the applicable anniversary. In no event shall Contractor invoice County separately for any out-of-pocket expenses being paid under any WO or SOS. Should Contractor's published Public Sector Rates decrease, such lower rates shall be immediately extended to County for all existing and subsequent WOs or SOSs.

5.7 Work Approval Testing and Acceptance

5.7.1 Acceptance Criteria

Contractor will consult with each County Project Manager to establish a mutually agreed to Acceptance Test Plan, a mutually agreed to process and procedure by which the parties will verify that the Services meet the Acceptance Criteria, the agreed upon objective standards by which the parties will verify that the Services Deliverables meet the specifications and/or requirements set forth in the WO and/or SOS. Conformity to the Acceptance Criteria, as judged by the County Project Manager in his/her sole discretion, shall determine whether County will accept or reject the Services.

5.7.2 Process for Acceptance Test

Each County Project Manager shall appoint personnel who shall attend, participate in, and verify the results of the Acceptance Testing. Contractor shall demonstrate that all work being tested either meets or exceeds the Acceptance Criteria. Testing shall include or be performed in the presence of County representatives.

5.7.3 Acceptance Tests

The parties shall, in each instance, mutually agree upon the Acceptance Criteria and testing which will apply to the Services Contractor delivers when a County Department orders Services from the SOS it has in place with Contractor. When the County Department is satisfied that the Services at least meet the Acceptance Criteria the parties previously agreed upon, the applicable County Project Manager shall issue Contractor an Acceptance Certificate, copy the County Program Manager, and close the matter. Contractor shall not under any circumstances Decrement a County Department's WO and/or SOS for any Service Contractor has provided until the County Department has accepted those Services and issued an Acceptance Certificate.

5.7.4 Decrements

For each WO and/or SOS, Contractor, on a monthly basis shall submit to the County Program Manager and the applicable County Project Manager a copy of the Report. Along with cumulative information that is required by Exhibit C ("Work Order Process"), the Report shall separately state

all Decrements for which Contractor is charging the County for the reporting period. The County shall use the report to verify that all Decrements for which Contractor has charged the Decrement for the reporting period are supported by an Acceptance Certificate or Accepted in accordance with the applicable WO and/or SOS. Where Contractor has not provided an Acceptance Certificate for a Decrement and the applicable County Project Manager is not otherwise able to verify that the Decrement is supported by an Acceptance Certificate, the County shall challenge the Decrement and Contractor shall reverse the Decrement until the matter is resolved through Sub-Paragraph 8.31 (Notice of Disputes).

5.7.5 Notice of Deficiencies

If the applicable County Project Manager makes a good faith determination that Contractor's work as a whole, or a component thereof, has failed to successfully complete an Acceptance Test, he/she shall promptly notify Contractor's Support Practice Manager in writing of the Deficiencies identified at that time, specifying with as much detail as possible, the manner in which the work failed to pass the applicable Acceptance Test ("Notice").

5.7.6 Correction of Deficiencies

Upon receipt of Notice from County, Contractor shall promptly commence all reasonable efforts to correct the Deficiencies County identifies. Contractor shall notify the applicable County Project Manager when it has corrected the Deficiencies and the Acceptance Test shall resume. For each WO and/or SOS, Contractor shall, at no additional cost to County, be required to continue its efforts to correct any remaining Deficiencies until Contractor succeeds.

5.7.7 Time for Correction of Deficiencies

Contractor shall correct to the satisfaction of County, at no additional cost to County, all Deficiencies in the Services. Contractor shall initiate repairs on Deficiencies which have a critical or significant impact on County's operations within two (2) business days following notice from County and shall use all reasonable efforts to resolve the Deficiencies in the time

frame set forth in the applicable WO and/or SOS. Contractor shall be solely liable for any direct costs incurred by County associated with any Deficiencies.

5.7.8 Remedy

In the event Contractor fails the Acceptance Test, County may pursue any and all remedies set forth in this Contract or as otherwise provided at law and/or inequity.

5.8 Warranty

5.8.1 Warranty

Contractor warrants and represents that: (1) all work and Services shall be performed in a professional and workmanlike manner, with all necessary care, skill and diligence, and in accordance with the applicable WO and/or SOS and other requirements set forth herein; (2) all work and Services shall conform to the requirements and specifications of the respective WO and/or SOS throughout the term of this Contract, including any and all extensions thereof; and, (3) all work and Services shall be free of Deficiencies.

5.8.2 Legal Proceedings

Contractor represents, warrants, and agrees that there are no existing or threatened legal proceedings against Contractor that would have an adverse effect upon its ability to perform its obligations under this Contract or its financial condition or operations and shall notify County promptly in writing of any change in this circumstance.

5.8.3 Disabling Devices

Contractor represents, warrants, and agrees that Contractor will not knowingly cause any interruption of the operations of, or vulnerability to, the work, or County's computer and network systems through any device, method or means including, without limitation, the use of any "virus," "worm," "lockup," "time bomb," "key lock," device or program, or disabling or defective code, which has the potential or capability of causing any interruption of the operations of, or accessibility to, the work, or County's computer and network systems or which could alter, destroy, or inhibit the use of

the work or County's computer and network systems, or the data contained therein which could block access to or prevent the use of the work or County's computer and network system.

5.8.4 Disclaimer

EXCEPT FOR THE EXPRESS WARRANTIES AND REPRESENTATIONS PROVIDED IN THIS CONTRACT, ANY SOS EXECUTED HEREUNDER AND ANY UNDERLYING PRODUCT PURCHASE AGREEMENTS AND/OR PURCHASE ORDERS, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CONTRACTOR DISCLAIMS AND EXCLUDES ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS WHETHER EXPRESS, IMPLIED OR STATUTORY INCLUDING, BUT NOT LIMITED TO, REPRESENTATIONS, WARRANTIES, OR CONDITIONS OF TITLE, NON-INFRINGEMENT, SATISFACTORY CONDITION, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO ANY SERVICES, SERVICE DELIVERABLES, FXES, PRODUCTS, OR ANY OTHER MATERIALS OR INFORMATION.

5.9 **County Approval of Invoices**

All invoices submitted by the Contractor for payment must have the written approval of the County's Project Manager prior to any payment thereof. In no event shall the County be liable or responsible for any payment prior to such written approval. Approval for payment will not be unreasonably withheld.

5.10 **Default Method of Payment: Direct Deposit or Electronic Funds Transfer**

5.10.1 The County, at its sole discretion, has determined that the most efficient and secure default form of payment for goods and/or services provided under an agreement/ contract with the County shall be Electronic Funds Transfer (EFT) or direct deposit, unless an alternative method of payment is deemed appropriate by the Auditor-Controller (A-C).

5.10.2 The Contractor shall submit a direct deposit authorization request via the website <https://directdeposit.lacounty.gov> with banking and vendor information, and any other information that the A-C determines is reasonably necessary

to process the payment and comply with all accounting, record keeping, and tax reporting requirements.

5.10.3 Any provision of law, grant, or funding agreement requiring a specific form or method of payment other than EFT or direct deposit shall supersede this requirement with respect to those payments.

5.10.4 At any time during the duration of the agreement/contract, a Contractor may submit a written request for an exemption to this requirement. Such request must be based on specific legal, business or operational needs and explain why the payment method designated by the A-C is not feasible and an alternative is necessary. The A-C, in consultation with the contracting department(s), shall decide whether to approve exemption requests.

6 ADMINISTRATION OF CONTRACT - COUNTY

6.1 County Administration

6.1.1 A listing of all County Administration referenced in the following subparagraphs are designated in Exhibit E - County's Administration. The County will notify the Contractor in writing of any change in the names or addresses shown.

6.2 County's Program Director

6.2.1 Program Director shall, on behalf of County, have the authority to negotiate and recommend all changes to this Contract; execute WOs and SOSs, Work Orders, and Work Order Amendments, and responsibility to confirm by administrative oversight and monitoring of Contractor's services provided hereunder, to assure that:

- a) County Departments utilize the Contract to acquire Services only as is provided herein;
- b) Each WO and/or SOS is duly approved by the Program Manager, or at his/her direction, by the Program Manager and, once approved, executed by County's Program Director, is issued to Contractor's Contracts Manager for Contractor's implementation;
- c) All directives of County's Board of Supervisors are implemented;

- d) All issues, problems, or disputes which cannot be resolved by the County Program Manager under Sub-Paragraph 8.31 (Notice of Disputes) are addressed, and;

6.3 County Program Manager

The County Program Manager, on behalf of County, has the administrative responsibility to assist the County Program Director and each County Project Manager as they may require in fulfilling their respective duties by:

- a) Jointly, with County's Project Managers, reviewing each WO and/or SOS to ensure compliance in accordance with requirements set forth in Exhibit C ("WO/SOS Issuance Process");
- b) Forwarding the WO and/or SOS to the County Program Director for approval, if applicable;
- c) Jointly, with County's Project Managers, reviewing, and approving or rejecting all Contractor personnel proposed to provide Services under each SOS, and once approved, each change of Contractor personnel that Contractor proposes or County requests;
- d) Assuring that each proposed WO and/or SOS conforms to the guidelines which are set forth in this Contract for Services;
- e) Negotiating and recommending changes to any approved WO and/or SOS by use of the Amendment process provided in Subparagraph 8.1.5 and, when assured that the proposed changes meet County's requirements under this Contract, forwarding any proposed change to the County Program Director for approval;
- f) Reviewing all Contractor produced usage reports under the WO and/or SOS to (i) verify that each County Project Manager authorized each Decrement to that WO and/or SOS by issuing an Acceptance Certificate, and (ii) follow-up as necessary upon such review;
- g) Meeting with Contractor's Support Practice Manager, as required, to assure the orderly and satisfactory progress of Contractor's work on each outstanding WO and/or SOS; and,
- h) Taking action to resolve any issues, problems, or disputes that were not resolved by each County Project Manager.

6.4 County's Project Manager

Each County Project Manager shall be identified by name in each WO and/or SOS. Each County Project Manager or his/her designee shall, in accordance with the provisions of this Paragraph 6 ("Administration of Contract - County") and Exhibit C ("WO/SOS Issuance Process"), approve each proposed WO and/or SOS for the subject County Department and shall be authorized to delegate, as necessary and appropriate, WO/SOS-related operational responsibilities to appropriate managers within the County Department. County Project Managers and their delegates shall:

- a) Prepare a draft WO and/or SOS which identifies the County Department's technical and functional requirements and forward the draft WO and/or SOS to the County Project Manager for review and final approval and execution by the County Program Director;
- b) Review, approve or reject, with the concurrence of County's Program Manager, all Contractor personnel proposed to provide Services under each WO and/or SOS and, once approved, review, approve or reject each change of Contractor personnel that is proposed by Contractor or requested by County;
- c) Carry out the day-to-day operational and administrative responsibilities of the Contract by assuring that County has the appropriate representation at all meetings and keeping and updating records of program activity;
- d) Recommend and negotiate changes to each executed WO and/or SOS by use of process set forth in Sub-paragraph 8.1.5 and, when assured that the proposed changes meet County's requirements under this Contract, forward the proposed change to County's Program Manager for review and, thereafter, approval and execution by County's Program Director;
- e) Participate in all Acceptance Testing or other review for compliance by Contractor with the terms and conditions of Service delivery under the WO and/or SOS to which County's Project Manager is assigned;
- f) Identify Deficiencies and assure that those Deficiencies are corrected by Contractor as provided in this Contract and, where not corrected, notify the County Program Manager so that

County may pursue its rights and remedies as provided under this Contract regarding the Deficiencies Contractor does not correct;

- g) Issue Acceptance Certificates to Contractor when appropriate and as required by this Contract
- h) Monitor and report on Contractor's WO and/or SOS performance and provide regular status reports as required by the County Program Manager;
- i) Approve or disapprove all Contractor WO and/or SOS invoices for which he/she is County Project Manager;
- j) Inspect any and all equipment, services, and/or other work provided by or on behalf of Contractor; and,
- k) Coordinate, meet, and/or confer with Contractor's Support Practice Manager on a regular basis with respect to all work being performed on active tasks and deliverables and provide direction to Contractor regarding County policy, information and procedural requirements.

7 ADMINISTRATION OF CONTRACT - CONTRACTOR

7.1 Contractor Administration

A listing of all of Contractor's Administration referenced in the following paragraphs is designated in Exhibit F (Contractor's Administration). The Contractor will notify the County in writing of any change in the names or addresses shown.

7.2 Contractor's Project Manager

7.2.1 The Contractor's Project Manager is designated in Exhibit F (Contractor's Administration). The Contractor shall notify the County in writing of any change in the name or address of the Contractor's Project Manager.

7.2.2 The Contractor's Project Manager shall be responsible for the Contractor's day-to-day activities as related to this Contract and shall meet and coordinate with County's Project Manager and County's Contract Project Monitor on a regular basis.

7.2.3 Contractor's Contracts Manager shall have the responsibility for all contractual and legal aspects of Contractor's performance of its obligation under this Contract. Contractor's Contract Manager shall carry out the following tasks:

- 7.2.3.1 Reviewing and approving all WO and/or SOS documents on behalf of Contractor, and specifically, as to each Contractor proposal to provide Services, Contractor's Contracts Manager shall assure that the Contractor proposal is fully responsive to the WO and/or SOS which County's Program Director submitted to Contractor's Contract Manager.
- 7.2.3.2 Approving each Contractor proposal, submitting it to County's Program Manager, and meeting and conferring with County's Program Manager as required to resolve any issues County has regarding the responsiveness of Contractor's proposal;
- 7.2.3.3 Resolving Contractor business, contractual and administrative matters relating to this Contract that cannot be resolved by Contractor's Support Practice Manager;
- 7.2.3.4 Resolving all issues, problems, or disputes which may arise which cannot be resolved by Contractor's Support Practice Managers under Sub-Paragraph 8.31 (Notice of Disputes); and,
- 7.2.3.5 Receiving all notices pursuant to this Contract and taking such other steps as may be necessary to fulfill Contractor's responsibilities hereunder.

7.3 Contractor's Support Practice Manager

- 7.3.1 Contractor's Support Practice Manager shall be responsible for the overall administration of this Contract with the County. Contractor's Support Practice Manager shall carry out such responsibilities through the following activities:
 - 7.3.1.1 Assuring that Contractor responds fully and completely to County's needs for Services by developing the scope of and then drafting and finalizing the WO and/or SOS to meet the County's needs as stated in the proposal County submits to Contractor, obtaining County's Acceptance of the Services Contractor proposes to provide, and providing oversight of Contractor's provision of those Services;
 - 7.3.1.2 Assuring that Contractor personnel perform their assigned work as required;
 - 7.3.1.3 Taking such corrective action as is necessary when Deficiencies in Services are identified by either Contractor or County;

- 7.3.1.4 Meeting and conferring on a regular basis with the County Project Managers assigned to the WOs and/or SOSs;
- 7.3.1.5 Providing regular status reports to County's Program Manager;
- 7.3.1.6 Keeping and updating all records relating to this Contract Contractor provides to County;
- 7.3.1.7 Meeting and/or conferring with County's Program Manager on a regular basis with respect to all work being performed on WO and/or SOS tasks and Services.
- 7.3.1.8 Resolving any issues, problems or disputes which may arise which cannot be resolved by Contractor's Services Account Executive through Paragraph 8.31 (Notice of Disputes); and,
- 7.3.1.9 Representing Contractor in the Dispute Resolution procedure as required in Paragraph 8.31 (Notice of Disputes);
- 7.3.1.10 Assuring that Contractor fulfills its reporting responsibilities in every respect regarding project activity;

7.4 Contractor's Services Account Executive

- 7.4.1 Contractor's Services Account Executive shall be responsible for drafting, finalizing, delivering and processing all WOs and/or SOSs, including change orders. Contractor's Services Account Executive shall provide prompt responses to all issues and questions regarding WOs and/or SOSs.

7.5 Approval of Contractor's Staff

- 7.5.1 County has the right to approve or disapprove all of the Contractor's staff performing work hereunder and any proposed changes in the Contractor's staff, including, but not limited to, the Contractor's Project Manager. Should Contractor wish to make a material change to its Staff performing work hereunder, Contractor shall seek County's prior consent, which consent shall not be unreasonably withheld.

7.6 Contractor's Staff Identification

7.6.1 Contract shall provide, at Contractor's expense, all staff providing services under this Contract with a photo identification badge.

7.7 Background and Security Investigations

7.7.1 Each of Contractor's staff performing services under this Contract, who is in a designated sensitive position, as determined by County in County's sole discretion, shall undergo and pass a background investigation to the satisfaction of County as a condition of beginning and continuing to perform services under this Contract. A Contractor employee shall have the right to refuse to submit to the background and security investigation. In such event, the Contractor employee shall be withdrawn and replaced by Contractor. Such background investigation must be obtained through fingerprints submitted to the California Department of Justice to include State, local, and federal-level review, which may include, but shall not be limited to, criminal conviction information. The fees associated with the background investigation shall be at the expense of the Contractor, regardless of whether the member of Contractor's staff passes or fails the background investigation.

If a member of Contractor's staff does not pass the background investigation or refuses to submit to the background investigation, County may request that the member of Contractor's staff be removed immediately from performing services under the Contract. Contractor shall comply with County's request at any time during the term of the Contract. County will not provide to Contractor or to Contractor's staff any information obtained through the County's background investigation.

7.7.2 County, in its sole discretion, may immediately deny or terminate facility access to any member of Contractor's staff that does not pass such investigation to the satisfaction of the County or whose background or conduct is incompatible with County facility access.

7.7.3 Disqualification of any member of Contractor's staff pursuant to this Paragraph 7.5 shall not relieve Contractor of its obligation to complete all work in accordance with the terms and conditions of this Contract.

7.8 Confidentiality

- 7.8.1 Except as expressly provided for in Subparagraph [7.8.4] or as disclosure may be required by any applicable law including, but not limited to, the California Public Records Act, for a period of five (5) years after initial disclosure, neither party shall use the other's Confidential Information without the other's written consent except in furtherance of this business relationship or disclose the other's Confidential Information except (i) to obtain advice from legal or financial consultants, or (ii) if compelled by law, in which case the party compelled to make the disclosure will use its best efforts to give the other party notice of the requirement so that the disclosure can be contested.
- 7.8.2 County and Contractor shall take reasonable precautions to safeguard each other's Confidential Information. Such precautions will be at least as great as those each party takes to protect its own Confidential Information. Each party may disclose the other's Confidential Information to its personnel only on a need-to-know basis. When Confidential Information is no longer necessary to perform any obligation under any SOS, the receiving party will, at the other's request, either return it or destroy it.
- 7.8.3 Contractor shall maintain the confidentiality of all records and information received, obtained and/or produced under the provisions of this Contract in accordance with all applicable Federal, State and local laws, rules, regulations, ordinances, directives, guidelines, policies and procedures relating to confidentiality, including, without limitation, County policies concerning information technology security and the protection of confidential records and information.
- 7.8.4 Each party is free to develop its respective products independently without the use of the other's Confidential Information. Neither County nor Contractor is obligated to restrict the future work assignments of people who have had access to Confidential Information. In addition, County, Contractor and the people who have had access to Confidential Information are free to use the information that the people retain in their unaided memories related to information technology, including ideas, concepts, know-how or techniques, so long as such use does not disclose Confidential Information of the other party in violation of this Sub-Paragraph [7.8]. This use will not grant either party any rights under the

other's copyrights or patents and does not require payment of royalties or separate license.

- 7.8.5 Either party may provide suggestions, comments or other feedback to the other with respect to the other's Confidential Information. Feedback is voluntary and the party receiving feedback is not required to hold it in confidence, as long as feedback does not constitute Confidential Information. The party receiving feedback will not disclose the source of feedback without the providing party's consent. Feedback may be used for any purpose without obligation of any kind, as long as feedback does not constitute any Confidential Information.
- 7.8.6 Contractor may use any technical information it derives from providing services related to Contractor's products for problem resolution, troubleshooting, and product functionality enhancements and fixes for Contractor's knowledge base. Contractor agrees not to identify County or disclose any County Confidential Information in any item in the knowledge base.
- 7.8.7 In recognizing Contractor's need to identify its services and related clients to sustain itself, County shall not inhibit Contractor from publishing its role under this Contract within the following conditions: (a) Contractor shall develop all publicity material in a professional manner. (b) During the term of this Contract, Contractor shall not publish or disseminate any commercial advertisements, press releases, feature articles, or other materials using the name of County without the prior written consent of County's Program Manager. County shall not unreasonably withhold or delay such written consent. (c) Contractor may, without the prior written consent of County, indicate in its proposals and sales materials that it has been awarded this Contract with County, provided that the requirements of this Sub-Paragraph [7.8] shall apply.
- 7.8.8 In lieu of Contractor's providing to County an executed Contractor Acknowledgement and Confidentiality Agreement in the forms show in Exhibit J for each of its employees and agents performing Services under this Contract, Contractor may provide such acknowledgements on behalf of its personnel, and in that event, Contractor shall as set forth in this Paragraph 7.8 indemnify, defend, and hold harmless County, its officers, employees, and agents, from and against any and all third party claims, demands, damages, liabilities, losses,

costs and expenses, including, without limitation, reasonable defense costs and legal, accounting and other expert, consulting, or professional fees, to the extent caused by any failure by Contractor, its officers, employees, agents, or Subcontractors, to comply with this Paragraph 7.8, as determined by a court of competent jurisdiction or as mutually agreed to by the parties. Any legal defense pursuant to Contractor's indemnification obligations under this Paragraph 7.8. shall be conducted by Contractor and performed by counsel selected by Contractor and approved by County. Notwithstanding the preceding sentence, County shall have the right to participate in any such defense at its sole cost and expense, except that in the event Contractor fails to provide County with a full and adequate defense, as determined by County in its sole judgment, County shall be entitled to retain its own counsel, including, without limitation, County Counsel, and to reimbursement from Contractor for all such costs and expenses incurred by County in doing so. Contractor shall not have the right to enter into any settlement, agree to any injunction, or make any admission, in each case, on behalf of County without County's prior written approval. To the extent the indemnity, defense, and hold harmless obligations relate to Contractor's failure to maintain confidentiality of Professional Services Data Professional Services Data, it shall be subject to the limitations set forth in Paragraph 8.60 (Limitation of Liability). "Professional Services Data" means all data, including all text, sound, video, image files or software, that are provided to Contractor, by or on behalf of County (or that County authorizes Microsoft to obtain from a Product) or otherwise obtained or processed by or on behalf of Contractors through an engagement with Contractor to obtain Services.

- 7.8.9 Contractor shall inform all of its officers, employees, agents and subcontractors providing services hereunder of the confidentiality provisions of this Contract.
- 7.8.10 Contractor shall sign and adhere to the provisions of the "Contractor Acknowledgement and Confidentiality Agreement", Exhibit G1-IT.

8 STANDARD TERMS AND CONDITIONS

8.1 Amendments

- 8.1.1 For any change which affects the scope of work, term, contract sum, payments, or any term or condition included under this Contract, an amendment to the Contract shall be prepared and executed by the Contractor and by the ISD Director, or his/her designee.
- 8.1.2 The County's Board of Supervisors or Chief Executive Officer or designee may require the addition and/or change of certain terms and conditions in the Contract during the term of this Contract. The County reserves the right to add and/or change such provisions as required by the County's Board of Supervisors or Chief Executive Officer. To implement such changes, an Amendment to the Contract shall be prepared and executed by the Contractor and by ISD Director, or his/her designee.
- 8.1.3 The ISD Director, or his/her designee, may at his/her sole discretion, authorize extensions of time as defined in Paragraph 4 - Term of Contract. The Contractor agrees that such extensions of time shall not change any other term or condition of this Contract during the period of such extensions. To implement an extension of time, an Amendment to the Contract shall be prepared and executed by the contractor and by ISD Director, or his/her designee.
- 8.1.4 For any changes to any of the transactional Exhibits (i.e. Exhibits A, inclusive, B, C, E and F) to the Contract, an Amendment shall be prepared and executed by the ISD Director, or his/her designee, and in writing by Contractor.
- 8.1.5 For any change which affects the scope of work, period of performance, payments, or any other aspect of a WO and/or SOS, without affecting any term or condition of this Contract, a WO and/or SOS Amendment shall be prepared and executed by the Director of ISD, or his/her designee, and executed by the Contractor.

8.2 Assignment and Delegation/Mergers or Acquisitions

- 8.2.1 The contractor shall notify the County of any pending acquisitions/mergers of its company unless otherwise legally

prohibited from doing so. If the contractor is restricted from legally notifying the County of pending acquisitions/mergers, then it should notify the County of the actual acquisitions/mergers as soon as the law allows and provide to the County the legal framework that restricted it from notifying the County prior to the actual acquisitions/mergers.

8.2.2 The contractor shall not assign, exchange, transfer, or delegate its rights or duties under this Contract, whether in whole or in part, without the prior written consent of County, in its discretion, and any attempted assignment, delegation, or otherwise transfer of its rights or duties, without such consent shall be null and void. For purposes of this paragraph, County consent shall require a written Amendment to the Contract, which is formally approved and executed by the parties. Any payments by the County to any approved delegate or assignee on any claim under this Contract shall be deductible, at County's sole discretion, against the claims, which the contractor may have against the County.

8.2.3 Any assumption, assignment, delegation, or takeover of any of the contractor's duties, responsibilities, obligations, or performance of same by any person or entity other than the contractor, whether through assignment, subcontract, delegation, merger, buyout, or any other mechanism, with or without consideration for any reason whatsoever without County's express prior written approval, shall be a material breach of the Contract which may result in the termination of this Contract. In the event of such termination, County shall be entitled to pursue the same remedies against contractor as it could pursue in the event of default by contractor.

8.2.3. Shareholders, partners, members, or other equity holders of Contractor may transfer, sell, exchange, assign, or divest themselves of any interest they may have therein. However, in the event any such sale, transfer, exchange, assignment, or divestment is effected in such a way as to give majority control of Contractor to any person(s), corporation, partnership, or legal entity other than the majority controlling interest therein at the time of execution of the Contract, such disposition is an assignment, and such assignment of this Contract requires the prior written consent of County in accordance with applicable provisions of this Contract.

8.3 Authorization Warranty

- 8.3.1 The contractor represents and warrants that the person executing this Contract for the contractor is an authorized agent who has actual authority to bind the contractor to each and every term, condition, and obligation of this Contract and that all requirements of the contractor have been fulfilled to provide such actual authority.

8.4 Budget Reductions

- 8.4.1 In the event that the County's Board of Supervisors adopts, in any fiscal year, a County Budget which provides for reductions in the salaries and benefits paid to the majority of County employees and imposes similar reductions with respect to County contracts, the County reserves the right to reduce its payment obligation under this Contract correspondingly for that fiscal year and any subsequent fiscal year during the term of this Contract (including any extensions), and the services to be provided by the contractor under this Contract shall also be reduced correspondingly. The County's notice to the contractor regarding said reduction in payment obligation shall be provided within thirty (30) calendar days of the Board's approval of such actions. Except as set forth in the preceding sentence, the contractor shall continue to provide all of the services set forth in this Contract.

8.5 Complaints

- 8.5.1 The Contractor shall develop, maintain and operate procedures for receiving, investigating and responding to complaints.
- 8.5.2 Complaint Procedures
- 8.5.2.1 Within ten (10) business days after the Contract effective date, the contractor shall provide the County with the Contractor's policy for receiving, investigating and responding to user complaints.
- 8.5.2.2 The County will review the contractor's policy and provide the contractor with approval of said plan or with requested changes.
- 8.5.2.3 If the County requests changes in the contractor's policy, the contractor shall make such changes and

resubmit the plan within five (5) business days for County approval.

- 8.5.2.4 If, at any time, the Contractor wishes to change the contractor's policy, the contractor shall submit proposed changes to the County for approval before implementation.
- 8.5.2.5 The Contractor shall preliminarily investigate all complaints and notify the County's Project Manager of the status of the investigation within one (1) business days of receiving the complaint.
- 8.5.2.6 When complaints cannot be resolved informally, a system of follow-through shall be instituted which adheres to formal plans for specific actions and strict time deadlines.
- 8.5.2.7 Copies of all written responses shall be sent to the County's Project Manager within two (2) business days of mailing to the complainant.

8.6 Compliance with Applicable Law

- 8.6.1 In the performance of this Contract, contractor shall comply with all applicable Federal, State and local laws, rules, regulations, ordinances, directives, and County Board policies applicable to the provision of the Services by Contractor, and all provisions required thereby to be included in this Contract are hereby incorporated herein by reference. Contractor shall have up to fifteen (15) Days to correct any noncompliance with County rules, regulations, ordinances, guidelines and directives following written notice from County to Contractor, including written copies of such applicable rules, regulations, ordinances, guidelines and/or directives.
- 8.6.2 As set forth in this Paragraph 8.6, Contractor shall indemnify, defend and hold harmless County, its officers, employees, and agents, from and against any and all third party claims, demands, damages, liabilities, losses, costs, and expenses, including, without limitation, reasonable defense costs and legal, accounting and other expert, consulting or professional fees, to the extent caused by any failure by Contractor, its officers, employees, agents, or Subcontractors, to comply with any such laws, rules, regulations, ordinances, directives, and County Board policies applicable to the provision of the

Services by Contractor (collectively, the "Laws") or otherwise resulted in a third party claim against County arising directly from Contractor's failure to comply with the Laws, as determined by a court of competent jurisdiction or as mutually agreed to by the parties. Any legal defense pursuant to Contractor's indemnification obligations under Paragraph 8.6 (Compliance with Applicable Law) shall be conducted by Contractor and performed by counsel selected by contractor and approved by County. Notwithstanding the preceding sentence, County shall have the right to participate in any such defense at its sole cost and expense, except that in the event contractor fails to provide County with a full and adequate defense, as determined by County in its sole judgment, County shall be entitled to retain its own counsel, including, without limitation, County Counsel, and to reimbursement from contractor for all such costs and expenses incurred by County in doing so. Contractor shall not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of County without County's prior written approval. To the extent the indemnity, defense, and hold harmless obligations relate to Contractor's failure to maintain confidentiality of Professional Services Data or any failure to comply with the Laws applicable to the provision of the Services by Contractor or otherwise resulted in a third party claim against County arising directly from Contractor's failure to comply with the Laws, it shall be subject to the limitations set forth in Paragraph 8.60 (Limitation of Liability).

8.7 Compliance with Civil Rights Laws

8.7.1 The contractor hereby assures that it will comply with Subchapter VI of the Civil Rights Act of 1964, 42 USC Sections 2000 (e) (1) through 2000 (e) (17), to the end that no person shall, on the grounds of race, creed, color, sex, religion, ancestry, age, condition of physical handicap, marital status, political affiliation, or national origin, be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under this Contract or under any project, program, or activity supported by this Contract. The contractor shall comply with Exhibit D - Contractor's EEO Certification.

8.8 Compliance with the County's Jury Service Program

8.8.1 Jury Service Program:

This Contract is subject to the provisions of the County's ordinance entitled Contractor Employee Jury Service ("Jury Service Program") as codified in Sections 2.203.010 through 2.203.090 of the Los Angeles County Code, a copy of which is attached as Exhibit H and incorporated by reference into and made a part of this Contract.

8.8.2 Written Employee Jury Service Policy.

1. Unless the contractor has demonstrated to the County's satisfaction either that the contractor is not a "contractor" as defined under the Jury Service Program (Section 2.203.020 of the County Code) or that the contractor qualifies for an exception to the Jury Service Program (Section 2.203.070 of the County Code), the contractor shall have and adhere to a written policy that provides that its Employees shall receive from the contractor, on an annual basis, no less than five days of regular pay for actual jury service. The policy may provide that Employees deposit any fees received for such jury service with the contractor or that the contractor deduct from the Employee's regular pay the fees received for jury service.
2. For purposes of this paragraph, "contractor" means a person, partnership, corporation or other entity which has a contract with the County or a subcontract with a County contractor and has received or will receive an aggregate sum of fifty thousand dollars (\$50,000) or more in any twelve (12) month period under one or more County contracts or subcontracts. "Employee" means any California resident who is a full-time employee of the contractor. "Full-time" means forty (40) hours or more worked per week, or a lesser number of hours if: 1) the lesser number is a recognized industry standard as determined by the County, or 2) contractor has a long-standing practice that defines the lesser number of hours as full-time. Full-time employees providing short-term, temporary services of ninety (90) days or less within a twelve (12) month period are not considered full-time for purposes of the Jury Service Program. If the contractor uses any subcontractor to perform services for the County

under the Contract, the subcontractor shall also be subject to the provisions of this paragraph. The provisions of this paragraph shall be inserted into any such subcontract agreement and a copy of the Jury Service Program shall be attached to the agreement.

3. If the contractor is not required to comply with the Jury Service Program when the Contract commences, the contractor shall have a continuing obligation to review the applicability of its "exception status" from the Jury Service Program, and the contractor shall immediately notify the County if the contractor at any time either comes within the Jury Service Program's definition of "contractor" or if the contractor no longer qualifies for an exception to the Jury Service Program. In either event, the contractor shall immediately implement a written policy consistent with the Jury Service Program. The County may also require, at any time during the Contract and at its sole discretion, that the contractor demonstrate, to the County's satisfaction that the contractor either continues to remain outside of the Jury Service Program's definition of "contractor" and/or that the contractor continues to qualify for an exception to the Program.
4. Contractor's violation of this paragraph of the Contract may constitute a material breach of the Contract. In the event of such material breach, County may, in its sole discretion, terminate the Contract and/or bar the contractor from the award of future County contracts for a period of time consistent with the seriousness of the breach.

8.9 Conflict of Interest

- 8.9.1 No County employee whose position with the County enables such employee to influence the award of this Contract or any competing Contract, and no spouse or economic dependent of such employee, shall be employed in any capacity by the contractor or have any other direct or indirect financial interest in this Contract. No officer or employee of the contractor who may financially benefit from the performance of work hereunder shall in any way participate in the County's approval, or ongoing evaluation, of such work, or in any way attempt to unlawfully influence the County's approval or ongoing evaluation of such work.

8.9.2 The contractor shall comply with all conflict of interest laws, ordinances, and regulations now in effect or hereafter to be enacted during the term of this Contract. The contractor warrants that it is not now aware of any facts that create a conflict of interest. If the contractor hereafter becomes aware of any facts that might reasonably be expected to create a conflict of interest, it shall immediately make full written disclosure of such facts to the County. Full written disclosure shall include, but is not limited to, identification of all persons implicated and a complete description of all relevant circumstances. Failure to comply with the provisions of this paragraph shall be a material breach of this Contract.

8.10 Consideration of Hiring County Employees Targeted for Layoffs or are on a County Re-Employment List

8.10.1 Should the contractor require additional or replacement personnel after the effective date of this Contract to perform the services set forth herein, the contractor shall give first consideration for such employment openings to qualified, permanent County employees who are targeted for layoff or qualified, former County employees who are on a re-employment list during the life of this Contract.

8.11 Consideration of Hiring GAIN-GROW Participants

8.11.1 Should the contractor require additional or replacement personnel after the effective date of this Contract, the contractor shall give consideration for any such employment openings to participants in the County's Department of Public Social Services Greater Avenues for Independence (GAIN) Program or General Relief Opportunity for Work (GROW) Program who meet the contractor's minimum qualifications for the open position. For this purpose, consideration shall mean that the contractor will interview qualified candidates. The County will refer GAIN-GROW participants by job category to the contractor. Contractors shall report links of available job openings with job requirements to: GAINGROW@DPSS.LACOUNTY.GOV and BSERVICES@WDACS.LACOUNTY.GOV and DPSS will refer qualified GAIN/GROW job candidates.

8.11.2 In the event that both laid-off County employees and GAIN/GROW participants are available for hiring, County employees shall be given first priority.

8.12 Contractor Responsibility and Debarment

8.12.1 Responsible Contractor

A responsible contractor is a contractor who has demonstrated the attribute of trustworthiness, as well as quality, fitness, capacity and experience to satisfactorily perform the contract. It is the County's policy to conduct business only with responsible contractors.

8.12.2 Chapter 2.202 of the County Code

The contractor is hereby notified that, in accordance with Chapter 2.202 of the County Code, if the County acquires information concerning the performance of the contractor on this or other contracts which indicates that the contractor is not responsible, the County may, in addition to other remedies provided in the Contract, debar the contractor from bidding or proposing on, or being awarded, and/or performing work on County contracts for a specified period of time, which generally will not exceed five (5) years but may exceed five (5) years or be permanent if warranted by the circumstances, and terminate any or all existing contracts the contractor may have with the County.

8.12.3 Non-responsible contractor

The County may debar a contractor if the Board of Supervisors finds, in its discretion, that the contractor has done any of the following: 1) violated a term of a contract with the County or a nonprofit corporation created by the County, 2) committed an act or omission which negatively reflects on the contractor's quality, fitness or capacity to perform a contract with the County, any other public entity, or a nonprofit corporation created by the County, or engaged in a pattern or practice which negatively reflects on same, 3) committed an act or offense which indicates a lack of business integrity or business honesty, or 4) made or submitted a false claim against the County or any other public entity.

8.12.4 Contractor Hearing Board

8.12.4.1 If there is evidence that the contractor may be subject to debarment, the Department will notify the contractor in writing of the evidence which is

the basis for the proposed debarment and will advise the contractor of the scheduled date for a debarment hearing before the Contractor Hearing Board.

- 8.12.4.2 The Contractor Hearing Board will conduct a hearing where evidence on the proposed debarment is presented. The contractor and/or the contractor's representative shall be given an opportunity to submit evidence at that hearing. After the hearing, the Contractor Hearing Board shall prepare a tentative proposed decision, which shall contain a recommendation regarding whether the contractor should be debarred, and, if so, the appropriate length of time of the debarment. The contractor and the Department shall be provided an opportunity to object to the tentative proposed decision prior to its presentation to the Board of Supervisors.
- 8.12.4.3 After consideration of any objections, or if no objections are submitted, a record of the hearing, the proposed decision, and any other recommendation of the Contractor Hearing Board shall be presented to the Board of Supervisors. The Board of Supervisors shall have the right to modify, deny, or adopt the proposed decision and recommendation of the Contractor Hearing Board.
- 8.12.4.4 If a contractor has been debarred for a period longer than five (5) years, that contractor may after the debarment has been in effect for at least five (5) years, submit a written request for review of the debarment determination to reduce the period of debarment or terminate the debarment. The County may, in its discretion, reduce the period of debarment or terminate the debarment if it finds that the contractor has adequately demonstrated one or more of the following: 1) elimination of the grounds for which the debarment was imposed; 2) a bona fide change in ownership or management; 3) material evidence discovered after debarment was imposed; or 4) any other reason that is in the best interests of the County.

- 8.12.4.5 The Contractor Hearing Board will consider a request for review of a debarment determination only where 1) the contractor has been debarred for a period longer than five (5) years; 2) the debarment has been in effect for at least five (5) years; and 3) the request is in writing, states one or more of the grounds for reduction of the debarment period or termination of the debarment, and includes supporting documentation. Upon receiving an appropriate request, the Contractor Hearing Board will provide notice of the hearing on the request. At the hearing, the Contractor Hearing Board shall conduct a hearing where evidence on the proposed reduction of debarment period or termination of debarment is presented. This hearing shall be conducted and the request for review decided by the Contractor Hearing Board pursuant to the same procedures as for a debarment hearing.
- 8.12.4.6 The Contractor Hearing Board's proposed decision shall contain a recommendation on the request to reduce the period of debarment or terminate the debarment. The Contractor Hearing Board shall present its proposed decision and recommendation to the Board of Supervisors. The Board of Supervisors shall have the right to modify, deny, or adopt the proposed decision and recommendation of the Contractor Hearing Board.

8.12.5 Subcontractors of Contractor

These terms shall also apply to subcontractors of County contractors.

8.13 Contractor's Acknowledgement of County's Commitment to Safely Surrendered Baby Law

- 8.13.1 The contractor acknowledges that the County places a high priority on the implementation of the Safely Surrendered Baby Law. The contractor understands that it is the County's policy to encourage all County contractors to voluntarily post the County's "Safely Surrendered Baby Law" poster, in Exhibit I, in a prominent position at the contractor's place of business.

The contractor will also encourage its subcontractors, if any, to post this poster in a prominent position in the subcontractor's place of business. Information and posters for printing are available at:

<https://lacounty.gov/residents/family-services/child-safety/safe-surrender/>

8.14 Contractor's Warranty of Adherence to County's Child Support Compliance Program

8.14.1 The contractor acknowledges that the County has established a goal of ensuring that all individuals who benefit financially from the County through contracts are in compliance with their court-ordered child, family and spousal support obligations in order to mitigate the economic burden otherwise imposed upon the County and its taxpayers.

8.14.2 As required by the County's Child Support Compliance Program (County Code Chapter 2.200) and without limiting the contractor's duty under this Contract to comply with all applicable provisions of law, the contractor warrants that it is now in compliance and shall during the term of this Contract maintain in compliance with employment and wage reporting requirements as required by the Federal Social Security Act (42 USC Section 653a) and California Unemployment Insurance Code Section 1088.5, and shall implement all lawfully served Wage and Earnings Withholding Orders or Child Support Services Department Notices of Wage and Earnings Assignment for Child, Family or Spousal Support, pursuant to Code of Civil Procedure Section 706.031 and Family Code Section 5246(b).

8.15 County's Quality Assurance Plan

The County or its agent(s) will monitor the contractor's performance under this Contract on not less than an annual basis. Such monitoring will include assessing the contractor's compliance with all Contract terms and conditions and performance standards. Contractor deficiencies which the County determines are significant or continuing and that may place performance of the Contract in jeopardy if not corrected will be reported to the Board of Supervisors and listed in the appropriate contractor performance database. The report to the Board will include improvement/corrective action measures taken by the County and the contractor. If improvement does not occur consistent with the corrective action measures, the County may terminate this

Contract or impose other penalties as specified in this Contract.

8.16 Damage to County Facilities, Buildings or Grounds

- 8.16.1 The contractor shall repair, or cause to be repaired, at its own cost, any and all damage to County facilities, buildings, or grounds caused by the contractor or employees or agents of the contractor. Such repairs shall be made immediately after the contractor has become aware of such damage, but in no event later than thirty (30) days after the occurrence.
- 8.16.2 If the contractor fails to make timely repairs, County may make any necessary repairs. All costs incurred by County, as determined by County, for such repairs shall be repaid by the contractor by cash payment upon demand.

8.17 Employment Eligibility Verification

- 8.17.1 The contractor warrants that it fully complies with all Federal and State statutes and regulations regarding the employment of aliens and others and that all its employees performing work under this Contract meet the citizenship or alien status requirements set forth in Federal and State statutes and regulations. The contractor shall obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by Federal and State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, (P.L. 99-603), or as they currently exist and as they may be hereafter amended. The contractor shall retain all such documentation for all covered employees for the period prescribed by law.
- 8.17.2 As provided for in this Paragraph, the Contractor shall indemnify, defend, and hold harmless, the County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against the contractor or the County or both to the extent caused by failure by Contractor, its officers, employees, agents, or Subcontractors, to comply with any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing work under this Contract, as determined by a court of competent jurisdiction or as mutually agreed to by the parties.

8.18 Counterparts and Electronic Signatures and Representations

This Contract may be executed in two or more counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same Contract. The facsimile, email or electronic signature of the Parties shall be deemed to constitute original signatures, and facsimile or electronic copies hereof shall be deemed to constitute duplicate originals.

The County and the Contractor hereby agree to regard electronic representations of original signatures of authorized officers of each party, when appearing in appropriate places on the Amendments prepared pursuant to Paragraph 8.1 (Amendments) and received via communications facilities (facsimile, email or electronic signature), as legally sufficient evidence that such legally binding signatures have been affixed to Amendments to this Contract.

8.19 Fair Labor Standards

8.19.1 As set forth in this Paragraph, the contractor shall comply with all applicable provisions of the Federal Fair Labor Standards Act and shall indemnify, defend, and hold harmless the County and its agents, officers, and employees from any and all liability, including, but not limited to, wages, overtime pay, liquidated damages, penalties, court costs, and reasonable attorneys' fees to the extent caused by any failure by Contractor, its officers, employees, agents, or subcontractors to comply with any wage and hour law, including, but not limited to, the Federal Fair Labor Standards Act, for work performed by the contractor's employees for which the County may be found jointly or solely liable, as determined by a court of competent jurisdiction or as mutually agreed to by the parties.

8.20 Force Majeure

8.20.1 Neither party shall be liable for such party's failure to perform its obligations under and in accordance with this Contract, if such failure arises out of fires, floods, epidemics, quarantine restrictions, other natural occurrences, strikes, lockouts (other than a lockout by such party or any of such party's subcontractors), freight embargoes, or other similar events to those described above, but in every such case the failure to perform must be totally beyond the reasonable control and without any fault or negligence of such party (such events are referred to in this paragraph as "force majeure events").

- 8.20.2 Notwithstanding the foregoing, a default by a subcontractor of contractor shall not constitute a force majeure event, unless such default arises out of causes beyond the reasonable control of both contractor and such subcontractor, and without any fault or negligence of either of them. In such case, contractor shall not be liable for failure to perform, unless the goods or services to be furnished by the subcontractor were obtainable from other sources in sufficient time to permit contractor to meet the required performance schedule. As used in this subparagraph, the term “subcontractor” and “subcontractors” mean subcontractors at any tier.
- 8.20.3 In the event contractor's failure to perform arises out of a force majeure event, contractor agrees to use commercially reasonable best efforts to obtain goods or services from other sources, if applicable, and to otherwise mitigate the damages and reduce the delay caused by such force majeure event.

8.21 Governing Law, Jurisdiction, and Venue

This Contract shall be governed by, and construed in accordance with, the laws of the State of California. The contractor agrees and consents to the exclusive jurisdiction of the courts of the State of California (except with respect to claims that are subject to the exclusive federal subject matter jurisdiction, as to which Contractor agrees and consents to the exclusive jurisdiction of the Federal District Court of the Central District of California) for all purposes regarding this Contract and further agrees and consents that venue of any action brought hereunder shall be exclusively in the County of Los Angeles.

8.22 Independent Contractor Status

- 8.22.1 This Contract is by and between the County and the contractor and is not intended, and shall not be construed, to create the relationship of agent, servant, employee, partnership, joint venture, or association, as between the County and the contractor. The employees and agents of one party shall not be, or be construed to be, the employees or agents of the other party for any purpose whatsoever.
- 8.22.2 The contractor shall be solely liable and responsible for providing to, or on behalf of, all persons performing work pursuant to this Contract all compensation and benefits. The County shall have no liability or responsibility for the payment of any salaries, wages, unemployment benefits, disability

benefits, Federal, State, or local taxes, or other compensation, benefits, or taxes for any personnel provided by or on behalf of the contractor.

8.22.3 The contractor understands and agrees that all persons performing work pursuant to this Contract are, for purposes of Workers' Compensation liability, solely employees of the contractor and not employees of the County. The contractor shall be solely liable and responsible for furnishing any and all Workers' Compensation benefits to any person as a result of any injuries arising from or connected with any work performed by or on behalf of the contractor pursuant to this Contract.

8.22.4 The contractor shall adhere to the provisions stated in Paragraph 7.8 (Confidentiality).

8.23 Indemnification

8.23.1 As set forth in this Paragraph, Contractor agrees to indemnify, defend and hold harmless County and County special districts and their elected and appointed officers, employees and agents from and against any third party claims for damages for bodily injury (including death) and damage to real property or tangible personal property for which it is legally liable to that third party and pay all cost, damages and attorney fees that a court finally awards or that are in a settlement approved by Contractor. Upon being served with any action or claim, County shall promptly notify Contractor in writing of same. County shall permit Contractor to control the defense of any action or claim to the extent permitted by law, and shall cooperate with Contractor in the defense.

8.24 General Provisions for all Insurance Coverage

8.24.1 Without limiting Contractor's indemnification of County, and in the performance of this Contract and until all of its obligations pursuant to this Contract have been met, Contractor shall provide and maintain at its own expense insurance coverage satisfying the requirements specified in Paragraphs 8.24 and 8.25 of this Contract. These minimum insurance coverage terms, types and limits (the "Required Insurance") also are in addition to and separate from any other contractual obligation imposed upon Contractor pursuant to this Contract. The County in no way warrants

that the Required Insurance is sufficient to protect the Contractor for liabilities which may arise from or relate to this Contract. The Contractor will satisfy all insurance requirements through a program of self-insurance, commercial insurance, a combination of the two, or any similar risk financing alternative.

8.24.2 Evidence of Coverage and Notice to County

- 8.24.2.1 Certificate(s) of insurance coverage (Certificate) satisfactory to County, and a copy of an Additional Insured endorsement confirming County and its Agents (defined below) has been given Insured status under the Contractor's General Liability policy, shall be delivered to County at the address shown below and provided prior to commencing services under this Contract.
- 8.24.2.2 Renewal Certificates shall be provided to County not less than ten (10) days prior to contractor's policy expiration dates. The County reserves the right to obtain complete, insurance certificates of any required contractor and/or sub-contractor at any time.
- 8.24.2.3 Certificates shall identify all Required Insurance coverage types and limits specified herein, reference this Contract by name or number, and be signed by an authorized representative of the insurer(s). The Insured party named on the Certificate shall match the name of the contractor identified as the contracting party in this Contract. Certificates shall provide the full name of each insurer providing coverage, its NAIC (National Association of Insurance Commissioners) identification number.
- 8.24.2.4 Neither the County's failure to obtain, nor the County's receipt of, or failure to object to a non-complying insurance certificate or endorsement, or any other insurance documentation or information provided by the contractor, its insurance broker(s) and/or insurer(s), shall be construed as a waiver of any of the Required Insurance provisions.

- 8.24.2.5 Certificates and copies of any required endorsements shall be sent to:

County of Los Angeles
Internal Services Department
Information Technology Contracts – PCS
Microsoft Unified Support Services
9150 E. Imperial Hwy., MS:46
Downey, CA 90242
Attention: Brianna Cuellar

- 8.24.2.6 Contractor also shall promptly report to County any injury or property damage accident or incident, including any injury to a Contractor employee occurring on County property, and any loss, disappearance, destruction, misuse, or theft of County property, monies or securities entrusted to contractor. Contractor also shall promptly notify County of any third party claim or suit filed against Contractor or any of its subcontractors which arises from or relates to this Contract and could result in the filing of a claim or lawsuit against contractor and/or County.

8.24.3 Additional Insured Status and Scope of Coverage

The County of Los Angeles, its Special Districts, Elected Officials, Officers, Agents, employees and volunteers (collectively County and its Agents) shall be provided additional insured status under contractor's General Liability policy with respect to liability arising out of Contractor's ongoing and completed operations performed on behalf of the County.

8.24.4 Cancellation of or Changes in Insurance

Contractor shall provide County with, or contractor's insurance policies shall contain a provision that County shall receive, written notice of cancellation or any change in Required Insurance, including insurer, limits of coverage, term of coverage or policy period. The written notice shall be provided to County at least ten (10) days in advance of cancellation for non-payment of premium and thirty (30) days in advance for any other cancellation or policy change. Failure to provide written notice of cancellation or any change in Required Insurance may constitute a material breach of

the Contract, in the sole discretion of the County, upon which the County may suspend or terminate this Contract.

8.24.5 Failure to Maintain Insurance

Contractor's failure to maintain or to provide acceptable evidence that it maintains the Required Insurance shall constitute a material breach of the Contract, upon which County immediately may withhold payments due to contractor, and/or suspend or terminate this Contract. County, at its sole discretion, may obtain damages from contractor resulting from said breach.

8.24.6 Insurer Financial Ratings

Coverage shall be placed with insurers acceptable to the County with A.M. Best ratings of not less than A:VII unless otherwise approved by County.

8.24.7 Contractor's Insurance Shall Be Primary

Contractor's insurance policies, with respect to any claims related to this Contract, shall be primary with respect to all other sources of coverage available to Contractor. Any County maintained insurance or self-insurance coverage shall be in excess of and not contribute to any contractor coverage.

8.24.8 Reserved.

8.24.9 Deductibles and Self-Insured Retentions (SIRs)

Contractor's policies shall not obligate the County to pay any portion of any contractor deductible or SIR.

8.24.10 Reserved.

8.24.11 Application of Excess Liability Coverage

Contractors may use a combination of primary, and excess insurance policies which provide coverage as broad as ("follow form" over) the underlying primary policies, to satisfy the Required Insurance provisions.

8.24.13 Alternative Risk Financing Programs

The County reserves the right to review, Contractor use of self-insurance, risk retention groups, risk purchasing groups, pooling arrangements and captive insurance to satisfy the Required Insurance provisions. The County and its Agents shall be designated as an Additional Covered Party under any approved program to the extent of the contractual liabilities assumed in this Agreement under any approved program.

8.24.14 **County Review and Approval of Insurance Requirements**

The County reserves the right to review and adjust the Required Insurance provisions, conditioned upon County's determination of changes in risk exposures.

8.25 **Insurance Coverage**

8.25.1 **Commercial General Liability** insurance (providing scope of coverage equivalent to ISO policy form CG 00 01), naming County and its Agents as an additional insured, with limits of not less than:

General Aggregate: \$4 million

Products/Completed Operations Aggregate: \$2 million

Personal and Advertising Injury: \$2 million

Each Occurrence: \$2 million

8.25.2 **Automobile Liability** insurance (providing scope of coverage equivalent to ISO policy form CA 00 01) with limits of not less than \$1 million for bodily injury and property damage, in combined or equivalent split limits, for each single accident. Insurance shall cover liability arising out of Contractor's use of autos pursuant to this Contract, including owned, leased, hired, and/or non-owned autos, as each may be applicable.

8.25.3 **Workers Compensation and Employers' Liability** insurance or qualified self- insurance satisfying statutory requirements for Contractor is responsible, which includes Employers' Liability coverage with limits of not less than \$1 million per accident. If applicable to Contractor's operations, coverage also shall be arranged to satisfy the requirements of any federal workers or workmen's compensation law or any federal occupational disease law.

8.25.4 Unique Insurance Coverage

8.25.4.1 Professional Liability-Errors and Omissions

Insurance covering Contractor's liability arising from or related to this Contract, with limits of not less than \$5 million per claim and \$5 million aggregate. Further, Contractor understands and agrees it shall maintain such coverage for a period of not less than two (2) years following this Agreement's expiration, termination or cancellation.

8.25.4.2 Network Security & Privacy Coverage Insurance

The Contractor shall secure and maintain network security and privacy coverage insurance coverage with limits of \$10 million per occurrence and in the aggregate during the term of the Contract, including coverage for: network security liability; privacy liability; privacy regulatory proceeding, defense, response, expenses and fines; technology professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption. The Contractor shall provide to the County certificates of insurance evidencing the foregoing upon the County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, shall not be construed as a limitation upon the Contractor's liability or as full performance of its indemnification obligations hereunder. No exclusion/restriction for unencrypted portable devices/media may be on the policy.

8.26 Reserved.

8.27 Reserved.

8.28 Nondiscrimination and Affirmative Action

- 8.28.1 The contractor certifies and agrees that all persons employed by it, its affiliates, subsidiaries, or holding companies are and shall be treated equally without regard to or because of race, color, religion, ancestry, national origin, sex, age, physical or mental disability, marital status, or political affiliation, in compliance with all applicable Federal and State anti-discrimination laws and regulations.
- 8.28.2 The contractor shall certify to, and comply with, the provisions of Exhibit D (Contractor's EEO Certification).
- 8.28.3 The contractor shall take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to race, color, religion, ancestry, national origin, sex, age, physical or mental disability, marital status, or political affiliation, in compliance with all applicable Federal and State anti-discrimination laws and regulations. Such action shall include, but is not limited to: employment, upgrading, demotion, transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training, including apprenticeship.
- 8.28.4 The contractor certifies and agrees that it will deal with its subcontractors, bidders, or vendors without regard to or because of race, color, religion, ancestry, national origin, sex, age, physical or mental disability, marital status, or political affiliation.
- 8.28.5 The contractor certifies and agrees that it, its affiliates, subsidiaries, or holding companies shall comply with all applicable Federal and State laws and regulations to the end that no person shall, on the grounds of race, color, religion, ancestry, national origin, sex, age, physical or mental disability, marital status, or political affiliation, be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under this Contract or under any project, program, or activity supported by this Contract.

- 8.28.6 The contractor shall allow County representatives access to the contractor's employment records during regular business hours to verify compliance with the provisions of this Paragraph 8.28 (Nondiscrimination and Affirmative Action) when so requested by the County.
- 8.28.7 If the County finds that any provisions of this Paragraph 8.28 (Nondiscrimination and Affirmative Action) have been violated, such violation shall constitute a material breach of this Contract upon which the County may terminate or suspend this Contract. While the County reserves the right to determine independently that the anti-discrimination provisions of this Contract have been violated, in addition, a determination by the California Fair Employment and Housing Commission or the Federal Equal Employment Opportunity Commission that the contractor has violated Federal or State anti-discrimination laws or regulations shall constitute a finding by the County that the contractor has violated the anti-discrimination provisions of this Contract.
- 8.28.8 The parties agree that in the event the contractor violates any of the anti-discrimination provisions of this Contract, the County shall, at its sole option, be entitled to the sum of five hundred dollars (\$500) for each such violation pursuant to California Civil Code Section 1671 as liquidated damages in lieu of terminating or suspending this Contract.

8.24.9 Subcontractor Insurance Coverage Requirements

Contractor shall include all subcontractors as insureds under Contractor's own policies, or shall provide County with each subcontractor's separate evidence of insurance coverage. Contractor shall be responsible for verifying each subcontractor complies with the Required Insurance provisions herein, and shall require that each subcontractor name the County and contractor as additional insureds on the subcontractor's General Liability policy. Contractor shall obtain County's prior review and approval of any subcontractor request for modification of the Required Insurance.

8.29 Non Exclusivity

- 8.29.1 Nothing herein is intended nor shall be construed as creating any exclusive arrangement with the contractor. This Contract

shall not restrict County from acquiring similar, equal or like goods and/or services from other entities or sources.

8.30 Notice of Delays

- 8.30.1 Except as otherwise provided under this Contract, when either party has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this Contract, that party shall, within one (1) business day, give notice thereof, including all relevant information with respect thereto, to the other party.

8.31 Notice of Disputes

- 8.31.1 The contractor shall bring to the attention of the County's Project Manager and/or County's Project Director any dispute between the County and the contractor regarding the performance of services as stated in this Contract. If the County's Project Manager or County's Project Director is not able to resolve the dispute, the ISD Director, or designee, shall resolve it.

8.32 Notice to Employees Regarding the Federal Earned Income Credit

- 8.32.1 The contractor shall notify its employees, and shall require each subcontractor to notify its employees, that they may be eligible for the Federal Earned Income Credit under the federal income tax laws. Such notice shall be provided in accordance with the requirements set forth in Internal Revenue Service Notice No. 1015.

8.33 Notice to Employees Regarding the Safely Surrendered Baby Law

- 8.33.1 The contractor shall notify and provide to its employees, and shall require each subcontractor to notify and provide to its employees, information regarding the Safely Surrendered Baby Law, its implementation in Los Angeles County, and where and how to safely surrender a baby. The information is set forth in Exhibit I, Safely Surrendered Baby Law of this Contract. Additional information is available at:

<https://lacounty.gov/residents/family-services/child-safety/safe-surrender/>

8.34 Notices

- 8.34.1 All notices or demands required or permitted to be given or made under this Contract shall be in writing and shall be hand delivered with signed receipt or mailed by first-class registered or certified mail, postage prepaid, addressed to the parties as identified in Exhibits E - County's Administration and F - Contractor's Administration. Addresses may be changed by either party giving ten (10) days prior written notice thereof to the other party. The ISD Director, or designee, shall have the authority to issue all notices or demands required or permitted by the County under this Contract.

8.35 Prohibition Against Inducement or Persuasion

- 8.35.1 Notwithstanding the above, the contractor and the County agree that, during the term of this Contract and for a period of one year thereafter, neither party shall in any way intentionally induce or persuade any employee of one party to become an employee or agent of the other party. No bar exists against any hiring action initiated through a public announcement.

8.36 Public Records Act

- 8.36.1 Any documents submitted by the contractor; all information obtained in connection with the County's right to audit and inspect the contractor's documents, books, and accounting records pursuant to Paragraph 8.38 (Record Retention and Inspection-Audit Settlement) of this Contract; as well as those documents which were required to be submitted in response to the Request for Proposals (RFP) used in the solicitation process for this Contract shall become a matter of public record and shall be regarded as public records. Exceptions will be those elements in the California Government Code Section 6250 et seq. (Public Records Act) and which are marked "trade secret", "confidential", or "proprietary". The County shall not in any way be liable or responsible for the disclosure of any such records including, without limitation, those so marked, if disclosure is required by law, or by an order issued by a court of competent jurisdiction.
- 8.36.2 In the event the County is required to defend an action on a Public Records Act request for any of the aforementioned documents, information, books, records, and/or contents of a

proposal marked “trade secret”, “confidential”, or “proprietary”, the Contractor agrees to defend and indemnify the County from all reasonable costs and expenses, including reasonable attorney’s fees, in action or liability arising under the Public Records Act. For purposes of clarity, Contractor’s obligations under this Paragraph 8.36.2. apply to actions taken by County to protect Contractor’s “trade secret”, “confidential”, or “proprietary” under the Public Records Act at the request of Contractor.

8.37 Publicity

8.37.1 The contractor shall not disclose any details in connection with this Contract to any person or entity except as may be otherwise provided hereunder or required by law. However, in recognizing the contractor’s need to identify its services and related clients to sustain itself, the County shall not inhibit the contractor from publishing its role under this Contract within the following conditions:

8.37.1.1 The Contractor shall develop all publicity material in a professional manner; and

8.37.1.2 During the term of this Contract, the contractor shall not, and shall not authorize another to, publish or disseminate any commercial advertisements, press releases, feature articles, or other materials using the name of the County without the prior written consent of the County’s Project Director. The County shall not unreasonably withhold written consent.

8.37.2 The Contractor may, without the prior written consent of County, indicate in its proposals and sales materials that it has been awarded this Contract with the County of Los Angeles, provided that the requirements of this Paragraph 8.37 (Publicity) shall apply.

8.38 Record Retention and Inspection-Audit Settlement

8.38.1 The Contractor shall maintain accurate and complete financial records of its activities and operations relating to this Contract in accordance with generally accepted accounting principles. The Contractor shall also maintain accurate and complete employment and other records relating to its performance of this Contract. The Contractor agrees that the County, or its

authorized representatives, shall have access to and the right to examine, audit, excerpt, copy, or transcribe any pertinent transaction, activity, or record relating to this Contract. All such material, including, but not limited to, all financial records, bank statements, cancelled checks or other proof of payment, timecards, sign-in/sign-out sheets and other time and employment records, and proprietary data and information, shall be kept and maintained by the Contractor and shall be made available to the County during the term of this Contract and for a period of five (5) years thereafter unless the County's written permission is given to dispose of any such material prior to such time. All such material shall be maintained by the contractor at a location in Los Angeles County, provided that if any such material is located outside Los Angeles County, then, at the County's option, the contractor shall pay the County for travel, per diem, and other costs incurred by the County to examine, audit, excerpt, copy, or transcribe such material at such other location.

- 8.38.2 Failure on the part of the Contractor to comply with any of the provisions of this Subparagraph 8.38 shall constitute a material breach of this Contract upon which the County may terminate or suspend this Contract.
- 8.38.3 If, at any time during the term of this Contract or within five (5) years after the expiration or termination of this Contract, representatives of the County conduct an audit of the Contractor regarding the work performed under this Contract, and if such audit finds that the County's dollar liability for any such work is less than payments made by the County to the Contractor, then the difference shall be either: a) repaid by the Contractor to the County by cash payment upon demand or b) at the sole option of the County's Auditor-Controller, deducted from any amounts due to the Contractor from the County, whether under this Contract or otherwise. If such audit finds that the County's dollar liability for such work is more than the payments made by the County to the contractor, then the difference shall be paid to the Contractor by the County by cash payment, provided that in no event shall the County's maximum obligation for this Contract exceed the funds appropriated by the County for the purpose of this Contract.

8.39 Recycled Bond Paper

- 8.39.1 Consistent with the Board of Supervisors' policy to reduce the amount of solid waste deposited at the County landfills, the

contractor agrees to use recycled-content paper to the maximum extent possible on this Contract.

8.40 Subcontracting

- 8.40.1 Subcontracting is strictly prohibited, and the Contractor must not subcontract any of its obligations under the Contract without the County's prior consent. If Contractor deems it necessary to subcontract, a written request must be submitted to the County and Contractor must receive prior written consent of the County to subcontract. Any subcontracting without prior approval of the County is in violation of this provision shall be deemed a material breach of this Contract. For purposes of clarity, Microsoft does use subprocessors as defined and provided for in the Microsoft Products and Services Data Protection Addendum.
- 8.40.2 If the Contractor desires to subcontract, the Contractor shall provide the following information promptly at the County's request:
- 8.40.2.1 A description of the work to be performed by the Subcontractor;
 - 8.40.2.2 A draft copy of the proposed Subcontract; and
 - 8.40.2.3 Other pertinent information and/or certifications requested by the County.
- 8.40.3 The Contractor shall indemnify, defend, and hold the County harmless with respect to the activities of each and every Subcontractor in the same manner and to the same degree as if such Subcontractor(s) were the Contractor employees. To the extent the indemnity, defense, and hold harmless obligations relate to Contractor's failure to maintain confidentiality of Professional Services Data or any failure to comply with the Laws applicable to the provision of the Services by Contractor or otherwise resulted in a third party claim against County arising directly from Contractor's failure to comply with the Laws, it shall be subject to the limitations set forth in Paragraph 8.60 (Limitation of Liability).
- 8.40.4 The Contractor shall remain fully responsible for all performances required of it under this Contract, including those that the contractor has determined to subcontract,

notwithstanding the County's approval of the Contractor's proposed subcontract.

- 8.40.5 The County's consent to subcontract shall not waive the County's right to prior and continuing approval of any and all personnel, including Subcontractor employees, providing services under this Contract. The Contractor is responsible to notify its Subcontractors of this County right.
- 8.40.6 The County's Project Director is authorized to act for and on behalf of the County with respect to approval of any subcontract and subcontractor employees. After approval of the subcontract by the County, Contractor shall forward a fully executed subcontract to the County for their files.
- 8.40.7 The Contractor shall be solely liable and responsible for all payments or other compensation to all Subcontractors and their officers, employees, agents, and successors in interest arising through services performed hereunder, notwithstanding the County's consent to subcontract.
- 8.40.8 The Contractor shall obtain certificates of insurance, which establish that the subcontractor maintains all the programs of insurance required by the County from each approved subcontractor. Before any Subcontractor employee may perform any work hereunder, Contractor shall ensure delivery of all such documents to:

Internal Services Department
9150 E. Imperia Hwy., MS:46
Downey, CA 90242
Attention: Brianna Cuellar

8.41 Termination for Breach of Warranty to Maintain Compliance with County's Child Support Compliance Program

- 8.41.1 Failure of the Contractor to maintain compliance with the requirements set forth in Paragraph 8.14 (Contractor's Warranty of Adherence to County's Child Support Compliance Program) shall constitute default under this Contract. Without limiting the rights and remedies available to the County under any other provision of this Contract, failure of the contractor to cure such default within ninety (90) calendar days of written notice shall be grounds upon which

the County may terminate this Contract pursuant to Paragraph 8.43 (Termination for Default) and pursue debarment of the Contractor, pursuant to County Code Chapter 2.202.

8.42 Termination for Convenience

8.42.1 This Contract may be terminated, in whole or in part, from time to time, when such action is deemed by the County, in its sole discretion, to be in its best interest. Termination of work hereunder shall be effected by notice of termination to the contractor specifying the extent to which performance of work is terminated and the date upon which such termination becomes effective. The date upon which such termination becomes effective shall be no less than thirty (30) days after the notice is sent.

8.42.2 After receipt of a notice of termination and except as otherwise directed by the County, the contractor shall:

8.42.2.1 Stop work under this Contract on the date and to the extent specified in such notice, and

8.42.2.2 Transfer to County, to the extent not previously transferred to County, all work in progress and all other completed work. County shall pay for such completed work pursuant to a fee and invoice schedule that has been mutually agreed to by the parties, and

8.42.2.2 Complete performance of such part of the work as shall not have been terminated by such notice.

8.42.3 All material including books, records, documents, or other evidence bearing on the costs and expenses of the contractor under this Contract shall be maintained by the contractor in accordance with Paragraph 8.38 (Record Retention and Inspection-Audit Settlement).

8.43 Termination for Default

8.43.1 Either party may, by written notice to the other party has materially breached this Contract. County may, by written notice to Contractor terminate the whole or any part of this Contract, if, in the judgment of County's Project Director:

- 8.43.1.1 Contractor has materially breached this Contract and does not cure within the time frame provided for in 8.43.1.3. below; or
 - 8.43.1.2 Contractor fails to timely provide and/or satisfactorily perform any task, deliverable, service, or other work required either under this Contract and does not cure within the time frame provided for in Section 8.43.1.3 below; or
 - 8.43.1.3 Contractor fails to demonstrate a high probability of timely fulfillment of performance requirements under this Contract, or of any obligations of this Contract and in either case, fails to demonstrate convincing progress toward a cure within fifteen (15) working days (or such longer period as the County may authorize in writing) after receipt of written notice from the County specifying such failure.
- 8.43.2 Except with respect to defaults of any Subcontractor, the Contractor shall not be liable for any such excess costs of the type identified in Paragraph 8.43.1 if its failure to perform this Contract arises out of causes beyond the control and without the fault or negligence of the contractor. Such causes may include, but are not limited to: acts of God or of the public enemy, acts of the County in either its sovereign or contractual capacity, acts of Federal or State governments in their sovereign capacities, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather; but in every case, the failure to perform must be beyond the control and without the fault or negligence of the contractor. If the failure to perform is caused by the default of a subcontractor, and if such default arises out of causes beyond the control of both the contractor and subcontractor, and without the fault or negligence of either of them, the contractor shall not be liable for any such excess costs for failure to perform, unless the goods or services to be furnished by the subcontractor were obtainable from other sources in sufficient time to permit the contractor to meet the required performance schedule. As used in this paragraph, the term "subcontractor(s)" means subcontractor(s) at any tier.
- 8.43.4 If, after the County has given notice of termination under the provisions of Paragraph 8.43 (Termination for Default) it is determined by the County that the Contractor was not in default (or the default was cured) under the provisions of

Paragraph 8.43 (Termination for Default) or that the default was excusable under the provisions of Subparagraph 8.43.3, the rights and obligations of the parties shall be the same as if the notice of termination had been issued pursuant to Paragraph 8.42 (Termination for Convenience).

- 8.43.5 The rights and remedies of the County provided in this Paragraph 8.43 (Termination for Default) shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

8.44 Termination for Improper Consideration

- 8.44.1 The County may, by written notice to the Contractor, immediately terminate the right of the contractor to proceed under this Contract if it is found that consideration, in any form, was offered or given by the contractor, either directly or through an intermediary, to any County officer, employee, or agent with the intent of securing this Contract or securing favorable treatment with respect to the award, amendment, or extension of this Contract or the making of any determinations with respect to the contractor's performance pursuant to this Contract. In the event of such termination, the County shall be entitled to pursue the same remedies against the Contractor as it could pursue in the event of default by the Contractor.
- 8.44.2 The Contractor shall immediately report any attempt by a County officer or employee to solicit such improper consideration. The report shall be made either to the County manager charged with the supervision of the employee or to the County Auditor-Controller's Employee Fraud Hotline at (800) 544-6861.
- 8.44.3 Among other items, such improper consideration may take the form of cash, discounts, services, the provision of travel or entertainment, or tangible gifts.

8.45 Termination for Insolvency

- 8.45.1 The County may terminate this Contract forthwith in the event of the occurrence of any of the following:
 - 8.45.1.1 Insolvency of the Contractor. The Contractor shall be deemed to be insolvent if it cannot pay its debts as they become due, whether or not a petition has

been filed under the Federal Bankruptcy Code and whether or not the contractor is insolvent within the meaning of the Federal Bankruptcy Code;

8.45.1.2 The filing of a voluntary or involuntary petition regarding the Contractor under the Federal Bankruptcy Code;

8.45.1.3 The appointment of a Receiver or Trustee for the contractor; or

8.45.1.4 The execution by the Contractor of a general assignment for the benefit of creditors.

8.45.2 The rights and remedies of the County provided in this Paragraph 8.45 (Termination for Insolvency) shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

8.46 Termination for Non-Adherence of County Lobbyist Ordinance

8.46.1 The Contractor, and each County Lobbyist or County Lobbying firm as defined in County Code Section 2.160.010 retained by the contractor, shall fully comply with the County's Lobbyist Ordinance, County Code Chapter 2.160. Failure on the part of the contractor or any County Lobbyist or County Lobbying firm retained by the contractor to fully comply with the County's Lobbyist Ordinance shall constitute a material breach of this Contract, upon which the County may in its sole discretion, immediately terminate or suspend this Contract.

8.47 Termination for Non-Appropriation of Funds

8.47.1 Notwithstanding any other provision of this Contract, the County shall not be obligated for the Contractor's performance hereunder or by any provision of this Contract during any of the County's future fiscal years unless and until the County's Board of Supervisors appropriates funds for this Contract in the County's Budget for each such future fiscal year. In the event that funds are not appropriated for this Contract, then this Contract shall terminate as of June 30 of the last fiscal year for which funds were appropriated. The County shall notify the contractor in writing of any such non-allocation of funds at the earliest possible date.

8.48 Validity

- 8.48.1 If any provision of this Contract or the application thereof to any person or circumstance is held invalid, the remainder of this Contract and the application of such provision to other persons or circumstances shall not be affected thereby.

8.49 Waiver

- 8.49.1 No waiver by the County of any breach of any provision of this Contract shall constitute a waiver of any other breach or of such provision. Failure of the County to enforce at any time, or from time to time, any provision of this Contract shall not be construed as a waiver thereof. The rights and remedies set forth in this Paragraph 8.49 shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

8.50 Warranty Against Contingent Fees

- 8.50.1 The contractor warrants that no person or selling agency has been employed or retained to solicit or secure this Contract upon any Contract or understanding for a commission, percentage, brokerage, or contingent fee, excepting bona fide employees or bona fide established commercial or selling agencies maintained by the contractor for the purpose of securing business.
- 8.50.2 For breach of this warranty, the County shall have the right to terminate this Contract and, at its sole discretion, deduct from the Contract price or consideration, or otherwise recover, the full amount of such commission, percentage, brokerage, or contingent fee.

8.51 Warranty of Compliance with County's Defaulted Property Tax Reduction Program

- 8.51.1 Contractor acknowledges that County has established a goal of ensuring that all individuals and businesses that benefit financially from County through contract are current in paying their property tax obligations (secured and unsecured roll) in order to mitigate the economic burden otherwise imposed upon County and its taxpayers.

Unless Contractor qualifies for an exemption or exclusion, contractor warrants and certifies that to the best of its

knowledge it is now in compliance, and during the term of this Contract will maintain compliance, with Los Angeles County Code Chapter 2.206.

8.52 Termination for Breach of Warranty to Maintain Compliance with County's Defaulted Property Tax Reduction Program

8.52.1 Failure of contractor to maintain compliance with the requirements set forth in Paragraph 8.51 "Warranty of Compliance with County's Defaulted Property Tax Reduction Program" shall constitute default under this contract. Without limiting the rights and remedies available to County under any other provision of this contract, failure of contractor to cure such default within ten (10) days of notice shall be grounds upon which County may terminate this contract and/or pursue debarment of contractor, pursuant to County Code Chapter 2.206.

8.53 Time Off for Voting

8.53.1 The contractor shall notify its employees, and shall require each subcontractor to notify and provide to its employees, information regarding the time off for voting law (Elections Code Section 14000). Not less than ten (10) days before every statewide election, every contractor and subcontractors shall keep posted conspicuously at the place of work, if practicable, or elsewhere where it can be seen as employees come or go to their place of work, a notice setting forth the provisions of Section 14000.

8.54 Compliance with County's Zero Tolerance Policy on Human Trafficking

Contractor acknowledges that the County has established a Zero Tolerance Policy on Human Trafficking prohibiting contractors from engaging in human trafficking.

If a Contractor or member of Contractor's staff is convicted of a human trafficking offense, the County shall require that the Contractor or member of Contractor's staff be removed immediately from performing services under the Contract. County will not be under any obligation to disclose confidential information regarding the offenses other than those required by law.

Disqualification of any member of Contractor's staff pursuant to this paragraph shall not relieve Contractor of its obligation to complete all work in accordance with the terms and conditions of this Contract.

8.55 Gratuitous Efforts

If Contractor provides any task, deliverable, Service, or other work to County that utilizes other than approved Contractor personnel, and/or that goes beyond the applicable WO and/or SOS expiration date, and/or that exceeds the total sum as specified in an WO and/or SOS, as originally written or modified, in accordance with Sub-paragraph 8.1 (AMENDMENTS), or is other than as specified in an approved WO and/or SOS, these shall be gratuitous efforts on the part of Contractor for which Contractor shall have no claim whatsoever against County.

8.55.1 Pro Bono Services

Contractor may, from time to time, provide Pro Bono Services for County through this Contract and an accompanying No-Cost WO and/or SOS which does not create a legal obligation for County to pay Contractor for such Services. It is Contractor's intent, under this Contract and accompanying No-Cost WO and/or SOS, to be in compliance with applicable laws and regulations. It is specifically understood that all Pro Bono Services provided under this Contract and accompanying No-Cost WO and/or SOS are for the sole benefit and use of County.

8.56 Compliance with Fair Chance Employment Practices

Contractor shall comply with fair chance employment hiring practices set forth in California Government Code Section 12952, Employment Discrimination: Conviction History. Contractor's violation of this paragraph of the Contract may constitute a material breach of the Contract. In the event of such material breach, County may, in its sole discretion, terminate the Contract.

8.57 Compliance with the County Policy of Equity

The contractor acknowledges that the County takes its commitment to preserving the dignity and professionalism of the workplace very seriously, as set forth in the County Policy of Equity (CPOE) (<https://ceop.lacounty.gov/>). The contractor further acknowledges that the County strives to provide a workplace free from discrimination, harassment, retaliation and inappropriate conduct

based on a protected characteristic, and which may violate the CPOE. The contractor, its employees and subcontractors who are assigned to work with County acknowledge and certify receipt and understanding of the CPOE. Failure of the contractor, its employees or its subcontractors to uphold the County's expectations of a workplace free from harassment and discrimination, including inappropriate conduct based on a protected characteristic, may subject the contractor to termination of contractual agreements as well as civil liability.

8.58 Prohibition from Participation in Future Solicitation(s)

A Proposer, or a Contractor or its subsidiary or Subcontractor ("Proposer/Contractor"), is prohibited from submitting a bid or proposal in a County solicitation if the Proposer/Contractor has provided advice or consultation for the solicitation. A Proposer/Contractor is also prohibited from submitting a bid or proposal in a County solicitation if the Proposer/Contractor has developed or prepared any of the solicitation materials on behalf of the County. A violation of this provision shall result in the disqualification of the Contractor/Proposer from participation in the County solicitation or the termination or cancellation of any resultant County contract. This provision shall survive the expiration, or other termination of this Agreement.

8.59 COVID-19 Vaccinations of County Contractor Personnel

1. At Contractor's sole cost, Contractor shall comply with Chapter 2.212 (COVID-19 Vaccinations of County Contractor Personnel) of County Code Title 2 - Administration, Division 4. All employees of Contractor and persons working on its behalf, including but not limited to, Subcontractors of any tier (collectively, "Contractor Personnel"), must be fully vaccinated against the novel coronavirus 2019 ("COVID-19") prior to (1) interacting in person with County employees, interns, volunteers, and commissioners ("County workforce members"), (2) working on County owned or controlled property while performing services under this Contract, and/or (3) coming into contact with the public while performing services under this Contract (collectively, "In-Person Services").
2. Contractor Personnel are considered "fully vaccinated" against COVID-19 two (2) weeks or more after they have received (1) the second dose in a 2-dose COVID-19 vaccine series (e.g.,

Pfizer-BioNTech or Moderna), (2) a single-dose COVID-19 vaccine (e.g., Johnson and Johnson [J&J]/Janssen), or (3) the final dose of any COVID-19 vaccine authorized by the World Health Organization ("WHO").

3. Prior to assigning Contractor Personnel to perform In-Person Services, Contractor shall obtain proof that such Contractor Personnel have been fully vaccinated by confirming Contractor Personnel is vaccinated through any of the following documentation: (1) official COVID-19 Vaccination Record Card (issued by the Department of Health and Human Services, CDC or WHO Yellow Card), which includes the name of the person vaccinated, type of vaccine provided, and date of the last dose administered ("Vaccination Record Card"); (2) copy (including a photographic copy) of a Vaccination Record Card; (3) Documentation of vaccination from a licensed medical provider; (4) a digital record that includes a quick response ("QR") code that when scanned by a SMART HealthCard reader displays to the reader client name, date of birth, vaccine dates, and vaccine type, and the QR code confirms the vaccine record as an official record of the State of California; or (5) documentation of vaccination from Contractors who follow the CDPH vaccination records guidelines and standards. Contractor shall also provide written notice to County before the start of work under this Contract that its Contractor Personnel are in compliance with the requirements of this section. Contractor shall retain such proof of vaccination for the document retention period set forth in this Contract, and must provide such records to the County for audit purposes, when required by County.
4. Contractor shall evaluate any medical or sincerely held religious exemption request of its Contractor Personnel, as required by law. If Contractor has determined that Contractor Personnel is exempt pursuant to a medical or sincerely held religious reason, the Contractor must also maintain records of the Contractor Personnel's testing results. The Contractor must provide such records to the County for audit purposes, when required by County. The unvaccinated exempt Contractor Personnel must meet the following requirements prior to (1) interacting in person with County workforce members, (2) working on County owned or controlled property while performing services under this Contract, and/or (3) coming into contact with the public while performing services under this Contract:

- a. Test for COVID-19 with either a polymerase chain reaction (PCR) or antigen test has an Emergency Use Authorization (EUA) by the FDA or is operating per the Laboratory Developed Test requirements by the U.S. Centers for Medicare and Medicaid Services. Testing must occur at least weekly, or more frequently as required by County or other applicable law, regulation or order.
 - b. Wear a mask that is consistent with CDC recommendations at all times while on County controlled or owned property, and while engaging with members of the public and County workforce members.
 - c. Engage in proper physical distancing, as determined by the applicable County department that the Contract is with.
5. In addition to complying with the requirements of this section, Contractor shall also comply with all other applicable local, departmental, State, and federal laws, regulations and requirements for COVID-19. A completed Exhibit G (COVID-19 Vaccination Certification of Compliance) is a required part of any agreement with the County.

8.60 Limitation of Liability

8.60.1 Contractor's maximum, aggregate liability to County in connection with each WO and/or SOS issued under this Contract for direct damages, regardless of the theory of liability, shall not exceed five (5) times the total amount of the applicable WO and/or SOS giving rise to the claims, or one million six hundred thousand dollars (\$1,600,000), whichever is greater. In addition, Contractor's maximum, aggregate liability under this Contract, including any and all SOSs, is limited to direct damages finally awarded or as agreed to by the parties, in an amount not to exceed Thirty Million Dollars (\$30,000,000) for the initial two (2) year term of the Contract. This amount will be increased by Fifteen Million Dollars (\$15,000,000) for each year the County extends the Contract term, up to a maximum of Seventy-Five Million Dollars (\$75,000,000) as follows:

First one-year extension: Forty-Five Million Dollars
(\$45,000,000)

Second one-year extension: Sixty Million Dollars
(\$60,000,000)

Third one-year extension: Seventy-Five Million Dollars
(\$75,000,000)

Thereafter, for each year extended beyond the fifth anniversary of this Contract, it will be adjusted in good faith as mutually agreed upon for each additional year the County exercises an additional option year based on the expected purchase commitments for Services for that year. In the event that Contractor provides services under a Pro Bono WO and/or SOS, however, then its liability to the County under this Sub-paragraph 8.60 shall not exceed five thousand dollars (\$5,000) for each such WO and/or SOS.

8.60.2 Notwithstanding any provision of this Contract to the contrary, whether expressly or by implication, the Limitation of Liability set forth in Subparagraph 8.60.1 does not apply to the following, which are hereby expressly excluded from and not affected by such limitation: (a) Contractor's obligations under Sub-paragraphs 8.17 (Employment Eligibility Verification), 8.19 (Fair Labor Standards), 8.23 (Indemnification), 8.24 (General Provisions for All Insurance Coverage), 8.25 (Insurance Coverage), and 8.36 (Public Records Act); (b) Contractor's liability to County for damages caused by gross negligence or willful misconduct to the extent caused by Contractor and/or its agent(s), as determined by a court of competent jurisdiction or as mutually agreed to by the parties ; (c) Contractor's obligations under Sub-paragraph 7.8 (Confidentiality) except for all liability related to Professional Services Data, which will remain subject to the limitations above in Sub-paragraph 8.60.1 and exclusions below in Sub-paragraph 8.60.3; and (d) the parties' obligations to each other arising from a breach of the other party's intellectual property rights.

8.60.3 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER CONTRACTOR NOR THE COUNTY SHALL BE LIABLE TO THE OTHER FOR ANY: (i) INDIRECT DAMAGES, (ii) CONSEQUENTIAL DAMAGES (INCLUDING,

WITHOUT LIMITATION, DAMAGES FOR BUSINESS INTERRUPTION OR LOSS OF BUSINESS INFORMATION), (iii) SPECIAL, OR (iv) INCIDENTAL DAMAGES, OR (v) DAMAGES FOR LOSS OF PROFITS OR REVENUES ARISING IN CONNECTION WITH THIS CONTRACT, ANY SOS, SERVICES, SERVICE DELIVERABLES, FIXES, PRODUCTS, OR ANY OTHER MATERIALS OR INFORMATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF SUCH POSSIBILITY WAS REASONABLY FORESEEABLE. THIS EXCLUSION OF LIABILITY DOES NOT APPLY TO EITHER PARTY'S LIABILITY TO THE OTHER FOR VIOLATION OF ANY CONFIDENTIALITY (EXCEPT AS NOTED IN SUB-PARAGRAPH 8.60.2 ABOVE) OR INTELLECTUAL PROPERTY OBLIGATIONS.

8.61 Effect of Termination

8.61.1 In the event County terminates this Contract in whole or in part as provided hereunder or upon the expiration of the Contract, as applicable, then, unless otherwise specified by County in writing:

1. Contractor shall continue the performance of this Contract to the extent not terminated.
2. Contractor shall cease to perform the Services being terminated on the date and to the extent specified in such notice and provide to County all completed Services and Services in progress, in a media reasonably requested by County, if applicable.
3. County will pay to Contractor all sums due and payable to Contractor for Services properly performed through the effective date of such expiration or termination (prorated as appropriate).
4. At County's option, Contractor shall provide a credit for, or return to County, all monies paid in advance by County, yet unearned by Contractor, including any prepaid fees, no later than thirty (30) days after the date of County's termination of any (or all) of the Statements of Services under this Contract and/or the Contract, whether such termination is for convenience or any default or breach hereunder.
5. Contractor shall promptly return to County any and all of the County's Confidential Information that relates to

the portion of the Contract or Services terminated by County in a media reasonably requested by County.

8.62 Severability

If any provision of this Contract is adjudged void or invalid for any reason whatsoever, but would be valid if part of the wording thereof were deleted or changed, then such provision shall apply with such modifications as may be necessary to make it valid and effective. In the event that one or more of the provisions of this Contract is found to be invalid, illegal or unenforceable in any respect, such provision shall be deemed deleted here from and the validity, legality, and enforceability of the remaining provisions contained herein shall not in any way be affected or impaired thereby.

8.63 Third Party Beneficiary

Notwithstanding any other provision of this Contract, the Contractor and County do not in any way intend that any person or entity shall acquire any rights as a third party beneficiary of this Contract, except that this provision shall not be construed to diminish the Contractor's indemnification obligations hereunder.

9 UNIQUE TERMS AND CONDITIONS

9.1 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

9.1.1 Contractor expressly acknowledges and agrees that the provision of services under this Agreement does not require or permit access by Contractor or any of its officers, employees, or agents, to any patient medical records/patient information. Accordingly, Contractor shall instruct its officers, employees, and agents that they are not to pursue, or gain access to, patient medical records/patient information for any reason whatsoever.

9.1.2 Notwithstanding the forgoing, the parties acknowledge that in the course of the provision of services hereunder, Contractor or its officers, employees, and agents, may have inadvertent access to patient medical records/patient information. Contractor understands and agrees that neither it nor its officers, employees, or agents, are to take advantage of such access for any purpose whatsoever.

Additionally, in the event of such inadvertent access, Contractor

and its officers, employees, and agents, shall maintain the confidentiality of any information obtained and shall notify Director that such access has been gained immediately, or upon the first reasonable opportunity to do so. In the event of a breach by Contractor of any of its obligations set forth in this Paragraph 9.1 that results in the unauthorized disclosure of patient medical records/patient information, Contractor agrees to pay direct costs incurred by County as provided for in Paragraph 9.6 (Reimbursement for County's Mitigation Costs), to the extent such breach was caused by Contractor.

- 9.1.3 Contractor also agrees to provide appropriate training to its employees regarding their obligations as described hereinabove.

9.2 Ownership of Materials, Software and Copyright

- 9.2.1 The following will apply:

- a. *Products and fixes.*** All products, related solutions and fixes provided under this Agreement will be licensed according to the terms of the license agreement packaged with or otherwise applicable to such product. County is responsible for paying any licensing fees associated with products.
- b. *Pre-existing work.*** All pre-existing work will remain the sole property of the party providing the pre-existing work. During the performance of services, each party grants to the other (and their contractors as necessary) a temporary, non-exclusive license to use, reproduce and modify any of its pre-existing work provided to the other party solely for the performance of such services.

Except as may be otherwise explicitly agreed to in a WOs or SOSs, upon payment in full, Contractor grants County a non-exclusive, perpetual, fully paid-up license to use, reproduce and modify (if applicable) Contractor's pre-existing work in the form delivered to County as part of the Service Deliverables only for County's internal business operations.

The perpetual license to Contractor's pre-existing work that Contractor leaves to County at the conclusion of Contractor's performance of the services is conditioned upon County's compliance with the terms of this Agreement and the applicable WOs or SOS.

- c. *Developments.*** Except as may be otherwise explicitly agreed to in a WO or SOS, upon payment in full Contractor grants County joint ownership in the developments of all non-preexisting work, and the Service Deliverables, under this Agreement and the associated WOs or SOS. County agrees to exercise its rights for its internal business operations only and County will not resell or distribute the developments to any third party. Each party shall be the sole owner of any modifications that it makes based upon the developments.
- d. *Affiliates rights and sublicensing to affiliates.*** Except as may be otherwise explicitly agreed to in a WO or SOS, County may sublicense the rights to the Service Deliverables granted hereunder to other governmental agencies that the County Board of Supervisors is the governing body for ("affiliates"), but County or its affiliates may not further sublicense these rights.

Any sublicensing of the Service Deliverables to County's affiliates, if permitted, must be consistent with the license terms in this Agreement or in any WOs or SOS.

- e. *Open source license restrictions.*** Because certain third party software is subject to open source license terms, the license rights that each party has granted to any computer code (or any intellectual property associated therewith) do not include any license, right, power or authority to incorporate, modify, combine and/or distribute that computer code with any other computer code in a manner which would subject the other's computer code to open source license terms. Furthermore, each party warrants that it will not provide or give to the other party computer code that is governed by open source license terms.

f. *Reservation of Rights.* All rights not expressly granted in this section are reserved.

- 9.2.2 During the term of this Contract and for five (5) years thereafter, the Contractor shall maintain and provide security for all of the Contractor's working papers prepared under this Contract. County shall have the right to inspect, copy and use at any time during and subsequent to the term of this Contract, any and all such working papers and all information contained therein.
- 9.2.3 Any and all materials, software and tools which are developed or were originally acquired by the Contractor outside the scope of this Contract, which the Contractor desires to use hereunder, and which the Contractor considers to be proprietary or confidential, must be specifically identified by the Contractor to the County's Project Manager as proprietary or confidential, and shall be plainly and prominently marked by the Contractor as "Proprietary" or "Confidential" on each appropriate page of any document containing such material.
- 9.2.4 The County will use reasonable means to ensure that the Contractor's proprietary and/or confidential items are safeguarded and held in confidence. The County agrees not to reproduce, distribute or disclose to non-County entities any such proprietary and/or confidential items without the prior written consent of the Contractor.
- 9.2.5 Notwithstanding any other provision of this Contract, the County will not be obligated to the Contractor in any way under Subparagraph 9.3.4 for any of the Contractor's proprietary and/or confidential items which are not plainly and prominently marked with restrictive legends as required by Subparagraph 9.2.3 or for any disclosure which the County is required to make under any state or federal law or order of court.
- 9.2.6 All the rights and obligations of this Paragraph 9.2 shall survive the expiration or termination of this Contract.

9.3 Patent, Copyright and Trade Secret Indemnification

- 9.3.1 Contractor shall indemnify, defend, and hold harmless County against any and all liability its trade secret and will pay the amount of any resulting adverse final judgment (or

settlement to which Contractor consents). County shall endeavor to notify Contractor promptly in writing of the claim and shall give Contractor sole control over its defense or settlement subject to County's approval of Contractor's counsel, which approval shall not be unreasonably withheld. County agrees to provide Contractor with reasonable assistance in defending the claim, and Contractor will reimburse County for expenses that County incurs in providing that assistance.

- 9.3.2 Contractor's obligations will not apply to the extent that liability is based on: (i) specifications, code, or materials County provides; (ii) County's running of the product, fix, or Service Deliverables after Contractor notifies County to discontinue running because of such a claim and after the County has a reasonable period of time to decess; (iii) County's combining or altering the product, fix or Service Deliverables with a non-Contractor product, data or business process unless Contractor required that County use that non-Contractor product, data or business process; (iv) damages attributable to the value of the use of a non-Contractor product, data or business process unless Contractor required that County use that product, data or business process; (v) County's altering the product, fix or Service Deliverables other than at the direction of Contractor; (vi) use of, or access to, products, fixes or Service Deliverables by any person or entity other than County or County's affiliates as permitted by Contractor; (vii) County's use of Contractor's trademark(s) without express written consent to do so; or (viii) for any trade secret claim, County's acquiring a trade secret (a) through improper means; (b) under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (c) from a person (other than Contractor or Contractor's affiliates) who owed to the party asserting the claim a duty to maintain the secrecy or limit the use of the trade secret.
- 9.3.3. If Contractor receives information concerning an infringement claim related to a product, fix, or Service Deliverable, Contractor may, at its expense and without obligation to do so, either (i) procure for County the right to continue to run the allegedly infringing Service Deliverable, or (ii) modify the Service Deliverable or replace it with a functional equivalent to make it non-infringing, in which case County will stop running the allegedly infringing product, fix, or Service Deliverable immediately thereafter. If, as a result

of an infringement claim, County's use of a product, fix, or Service Deliverable is enjoined by a court of competent jurisdiction, Contractor will, at Contractor's option, either procure the right to continue its use, replace it with a functional equivalent, modify it to make it non-infringing, or refund the amount paid and terminate the license for and, as applicable to certain Service Deliverables, County's ownership rights in, the infringing Service Deliverable. The foregoing is not intended to be the County's sole and exclusive remedy.

- a. To the extent permitted by applicable law, Customer will be responsible for any third-party claim to the extent it alleges that Customer's use of any Fix or Services Deliverable alone or in combination with anything else, violates the law or damages a third party.

9.4 Data Destruction

As provided for in the Microsoft Products and Services Data Protection Addendum (the "DPA"), Contractor(s) and Vendor(s) that have maintained, processed, or stored the County of Los Angeles' ("County") data and/or information, implied or expressed, have the sole responsibility to certify that the data and information have been appropriately destroyed consistent with the National Institute of Standards and Technology (NIST) Special Publication SP 800-88 titled *Guidelines for Media Sanitization*. Available at:

<http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-88>
[Rev.%201](#)

The data and/or information may be stored on purchased, leased, or rented electronic storage equipment (e.g., printers, hard drives) and electronic devices (e.g., servers, workstations) that are geographically located within the County, or external to the County's boundaries. As provided for in the DPA, the County must receive within ten (10) business days, a signed document from Contractor(s) and Vendor(s) that certifies and validates the data and information were placed in one or more of the following stored states: unusable, unreadable, and indecipherable.

As provided for in the DPA, any County data stored on purchased, leased, or rented electronic storage equipment and electronic

devices, including, but not limited to printers, hard drives, servers, and/or workstations are destroyed consistent with the current National Institute of Standard and Technology (NIST) Special Publication SP-800-88, *Guidelines for Media Sanitization*. As provided for in the DPA, Vendor shall provide County with written certification, within ten (10) business days of removal of any electronic storage equipment and devices that validates that any and all County data was destroyed and is unusable, unreadable, and/or undecipherable.

9.5 Products and Services Data Protection Addendum

Microsoft Products and Services Data Protection Addendum terms apply to Services as of the Effective Date of this Contract, and are incorporated into the Work Order or Statement of Services by this reference, as attached in Exhibit K.

9.6 Reimbursement for County's Mitigation Costs

In addition to the contractual obligations set forth in this Contract, to the extent that a Security Incident (as defined in the Microsoft Products and Services Data Protection Addendum) results from Contractor's failure to comply with its obligations under an applicable Statement of Work for Unified Support Services or Microsoft Consulting Services, and subject to the limitations of liability applicable to the applicable Unified Support Services or Microsoft Consulting Services in this Contract, Contractor will reimburse County for reasonable out-of-pocket remediation costs incurred by County in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" are costs that (a) are customary, reasonable and expected to be paid by similar entities like County, based on the nature and scope of the Security Incident (e.g., costs arising from required notification of individuals whose information was the subject of a breach, and costs associated with procuring credit monitoring protection for individuals who are put at risk of identity theft as a result of a breach), and (b) do not arise from or relate to County's violation of (i) laws applicable to County or (ii) County's obligations to third parties, and (c) in no event include costs arising related to compliance with laws applicable to County that are not generally applicable to information technology services providers. County must document all such expenditures and, upon Contractor's request, those expenditures must be validated by an independent third party industry expert chosen by both parties, with Contractor reimbursing County for

County's share of use of such expert. For avoidance of doubt, the costs reimbursed by Contractor under this paragraph will be characterized as direct damages subject to the limitation on liability in this Contract, and not as special damages excluded under the Limitation on Liability [Paragraph 8.60] in this Contract.

10 SURVIVAL

In addition to any terms and conditions of this Agreement that expressly survive expiration or termination of this Agreement by their terms, the following provisions shall survive the expiration or termination of this Agreement for any reason:

Paragraph 1 (Applicable Documents)

Paragraph 2 (Definitions)

Paragraph 3 (Work)

Paragraph 5.4 (No Payment for Services Provided Following
Expiration/Termination of Agreement)

Paragraph 7.8 (Confidentiality)

Paragraph 8.1 (Amendments)

Paragraph 8.2 (Assignment and Delegation/Mergers or Acquisitions)

Paragraph 8.6.2

Paragraph 8.19 (Fair Labor Standards)

Paragraph 8.20 (Force Majeure)

Paragraph 8.21 (Governing Law, Jurisdiction, and Venue)

Paragraph 8.23 (Indemnification)

Paragraph 8.24 (General Provisions for all Insurance Coverage)

Paragraph 8.25 (Insurance Coverage)

Paragraph 8.34 (Notices)

Paragraph 8.36 (Public Records Act)

Paragraph 8.38 (Record Retention and Inspection/Audit Settlement)

Paragraph 8.42 (Termination for Convenience)

Paragraph 8.43 (Termination for Default)

Paragraph 8.48 (Validity)

Paragraph 8.49 (Waiver)

Paragraph 8.58 (Prohibition from Participation in Future Solicitation(s))

Paragraph 8.60 (Limitation of Liability)

Paragraph 8.61 (Effect of Termination)

Paragraph 8.62 (Severability)

Paragraph 8.63 (Third Party Beneficiaries)

Paragraph 9.2 (Ownership of Materials, Software and Copyright)

Paragraph 9.3 (Patent, Copyright and Trade Secret Indemnification)

Paragraph 10 (Survival)

IN WITNESS WHEREOF, Contractor has executed this Contract, and the Board of Supervisors of the County of Los Angeles has caused this Contract to be executed by the Director of the Internal Services Department, or designee, and approved by County Counsel, and Contractor has caused this Contract to be executed in its behalf by its duly authorized officer, this _____ day of _____, 20____.

IN WITNESS WHEREOF,

COUNTY OF LOS ANGELES

By _____
Director

_____ Department

By _____
Contractor

Signed: _____

Printed: _____

Title: _____

APPROVED AS TO FORM:

DAWYN R. HARRISON
Acting County Counsel

By _____
Deputy County Counsel

CONTRACT PROVISIONS TABLE OF CONTENTS

STANDARD EXHIBITS

A-1	Statement of Work-Microsoft Unified Product Support Description
A-2	Statement of Work-Microsoft Consulting Support Description
A-3	Additional Definitions and Terms and Conditions
A-4	Customer Service Request for Services Process
A-5	Acceptance Certificate Form
A-6	Microsoft Unified Support Sample Work Order
A-7	Microsoft Consulting Services Sample Statement of Services
A-8	Microsoft Sample Customer Status Report
B-1	Microsoft Unified Support Published Price List
B-2	Microsoft Consulting Services Published Price List
C	County's Work Order/Statement of Services Process
D	Contractor's EEO Certification
E	County's Administration
F	Contractor's Administration
G	COVID-19 Vaccination Certification of Compliance
G1-IT	Contractor Acknowledgement and Confidentiality Agreement
H	Jury Service Ordinance
I	Safely Surrendered Baby Law

UNIQUE EXHIBITS

INFORMATION SECURITY AND PRIVACY REQUIREMENTS

J	Information Security and Privacy Requirements
K	Microsoft Products and Services Data Protection Addendum

- A-1 Statement of Work-Microsoft Unified Product Support Description
- A-2 Statement of Work-Microsoft Consulting Support Description
- A-3 Additional Definitions and Terms and Conditions
- A-4 Customer Service Request for Services Process
- A-5 Acceptance Certificate Form
- A-6 Microsoft Unified Support Sample Work Order
- A-7 Microsoft Consulting Services Statement of Services
- A-8 Microsoft Sample Customer Status Report

EXHIBIT A-1

Statement of Work

Microsoft Unified Products Support Description

Table of content

1	About this document.....	3
2	Support Services.....	4
	2.1 How to purchase	4
	2.2 Description of services.....	5
	2.2.1 Proactive services	5
	2.2.2 Reactive services	9
	2.2.3 Service delivery management	13
	2.3 Enhanced services and solutions	15
	2.3.1 Designated Support Engineering.....	15
	2.3.2 Rapid Response	16
	2.3.3 Azure Event Management	17
	2.3.4 Office 365 Engineering Direct	18
	2.3.5 Developer Support	18
	2.3.6 Support for Mission Critical	19
	2.4 Multi-country Support	19
	Multi-country Support Services Overview	19
	How to Purchase	19
	Multi-Country Support Additional Terms and Conditions	20
	2.5 Additional Terms and Conditions.....	21
	2.6 Your responsibilities.....	23

1 About this document

The Microsoft Unified Enterprise Support and Consulting Services Description provides you with information on the support services that are available to purchase from Microsoft.

Please familiarize yourself with the descriptions of the services that you purchase, including any prerequisites, disclaimers, limitations and your responsibilities. The services that you purchase will be listed in your Work Order (Work Order) or another applicable Statement of Services that references and incorporates this document.

Not all services listed in this document are available globally. For details on which services are available for purchase in your location, contact your Microsoft Services representative. Available services are subject to change.

2 Support services

Microsoft Unified Support Services (support services) is a comprehensive enterprise support set of services that helps accelerate your journey to the cloud, optimize your IT solutions, and use technology to realize new business opportunities for any stage of the IT lifecycle. Support services include:

- Proactive services help improve health of your IT infrastructure and operations
- Service Delivery Management to facilitate planning and implementation
- Prioritized 24x7 problem resolution services to provide rapid response to minimize downtime

2.1 How to purchase

Support services are available as a Base Package, with additional services, and enhanced services and solutions available to purchase under an existing Base Package agreement listed in the Enterprise Services Work Order, as described below.

Item	Description
Base Package	A combination of proactive, reactive and delivery management services that support Microsoft products and/or Online Services in use within your organization. Part of your Base Package includes a Flex Allowance* to use to add proactive services (marked with "+"), enhanced services and solutions services and/or Custom Proactive services to your Base Package. Base Package included services are represented with a "✓" throughout this section.
Additional services	Additional support services, including Proactive services are available to add to your Base Package during the term of your Work Order and are represented with a "+" throughout this section.
Enhanced services and solutions	Support services, which cover a specific Microsoft product or customer IT system, are available to add to your support Base Package during the term of your Work Order and are also represented with a "+" throughout this section.
Multi-country support	Multi-country Support provides support to you in multiple Support Locations, as described in your Work Order (or Work Orders).

*Flex Allowance is a flexible portion of your base package list price that may be applied towards the purchase of Proactive services, enhanced services and solutions, Proactive credits or Custom Proactive Services at the time of the services purchase. Your Microsoft representative will provide the portion of your Base Package list price available for use as Flex Allowance. The following conditions for allocation of your Flex Allowance apply:

- Up to 20% or \$50,000, whichever is higher, of your allotted Flex Allowance may be applied to the purchase of Proactive Credits or Custom Proactive services.
- Flex Allowance is allocated on an annual basis and any services to which Flex Allowance has been applied must be utilized during the applicable annual term.
- Flex Allowance may not be used for Service Delivery Management services, as defined herein.
- All available Flex Allowance must be allocated by time of contract execution or it will be forfeited.

2.2 Description of services

The items which are combined to form your support services package are described in this section. Also, listed are services that may be added to your Base Package or added during the Term of the agreement.

Proactive services

Proactive services help prevent issues in your Microsoft environment and will be scheduled to help ensure resource availability and delivery during the term of the applicable Work Order. The Proactive services that follow are available as identified below or detailed on your Work Order.

Planning services

Planning services provide assessments and reviews of your current infrastructure, data, application and security environment to help plan your remediation, upgrade, migration, deployment or solution implementation based on your desired outcomes.

Planning service types	Plan
Proof of Concept	+

+ - Additional service that may be purchased

Proof of Concept: An engagement to provide evidence that enables the customer to evaluate the feasibility of a proposed technical solution. The evidence can be in the form of working prototypes, documents, and designs, but are not usually production-ready deliverables.

Implementation services

Implementation services provide technical and project management expertise to accelerate design, deployment, migration, upgrade, and implementation of Microsoft technology solutions.

Implementation service types	Plan
Onboarding Services	+

+ - Additional service that may be purchased.

Onboarding Services: A direct engagement with a Microsoft resource to provide deployment, migration, upgrade or feature development assistance. This can include assistance with planning and validation of a proof-of-concept or production workload using Microsoft products.

Maintenance services

Maintenance services help prevent issues in your Microsoft environment and are typically scheduled in advance of the service delivery to help ensure resource availability.

Maintenance service types	Plan
On-demand Assessment	✓
Assessment Program	+
Offline Assessment	+
Proactive Monitoring	+
Proactive Operations Programs (POP)	+
Risk and Health Assessment Program as a Service (RAP as a Service)	+

✓ - Included as part of your Base Package.

⊕ - Additional service that may be purchased.

On-demand Assessment: Access to a self-service, online automated assessment platform that uses log analyses to analyze and assess your Microsoft technology implementation. On-demand Assessments cover limited technologies. Use of this assessment service requires an active Azure service with adequate data limits to enable use of the on-demand assessment service. Microsoft may provide assistance to enable initial setup of the service. In conjunction with the On-demand Assessment, and for an additional fee, an onsite Microsoft resource (for up to two days) or remote Microsoft resource (for up to one day) are available to assist with analyzing the data and prioritizing remediation recommendations per your services agreement. Onsite assessments may not be available in all geographies.

Assessment Program: An assessment on the design, technical implementation, operations or change management of your Microsoft technologies against Microsoft recommended practices. At the conclusion of the assessment, the Microsoft resource will work directly with you to remediate possible issues and provide a report containing the technical assessment of your environment, which may include a remediation plan.

Offline Assessment: An automated assessment of your Microsoft technology implementation with data collected remotely, or by a Microsoft resource at your location. The data gathered is analyzed by Microsoft using on-premises tools, and we provide you with a report of our findings and remediation recommendations.

Proactive Monitoring: Delivery of technical operations monitoring tools and recommendations for tuning your server incident management processes. This service helps you create incident matrices, conduct major incident reviews, and create the design for a sustained engineering team.

Proactive Operations Programs (POP): A review with your staff of your planning, design, implementation or operational processes against Microsoft recommended practices. This review is done either onsite or remotely by a Microsoft resource.

Risk and Health Assessment Program as a Service (RAP as a Service): An automated assessment of your Microsoft technology implementation, with data collected remotely. The gathered data is analyzed by Microsoft to create a findings report containing remediation recommendations. This service is available for on-site or remote delivery.

Optimization services

Optimization services focus on the goals of optimal utilization of the customer's technology investment. These services may include remote administration of cloud services, optimizing the adoption of Microsoft product capabilities by end users and ensuring a robust security and identity posture.

Optimization service types	Plan
Adoption Services	+
Development Focused Services	+
IT Services Management	+
Security Services	+

+ - Additional service that may be purchased.

Adoption Services: Adoption support services provide a suite of services that help you assess your organization's ability to modify, monitor and optimize changes linked to your Microsoft technology purchase. This includes support in the development and execution of your adoption strategy around the people side of change. Customers have access to resources with the expertise, knowledge and associated Microsoft recommended practices in support of their adoption program.

Development Focused Services: Services available to assist your staff build, deploy, and support applications built with Microsoft technologies.

- **Services Insights for Developers:** An annual assessment of your application development practices to help customers with recommended practice guidance for developing applications and solutions on Microsoft platforms.
- **Development Support Assistance:** Provides help in creating and developing applications that integrate Microsoft technologies on the Microsoft platform, specializing in Microsoft development tools and technologies, and is sold as a quantity of hours listed on your Work Order.

IT Services Management: A suite of services designed to help you evolve your legacy IT environment using modern service management approaches that enable innovation, flexibility, quality and operational cost improvements. Modern IT Service Management services may be delivered through remote or onsite advisory sessions or workshops to help ensure your monitoring, incident management or service desk processes are optimized to manage the dynamics of cloud-based services when moving an application or service to the cloud. IT Services Management services may be an element of a customized program of support services, available for an additional fee and may be defined in an exhibit and referenced in your Work Order.

Security Services: The Microsoft security solutions portfolio includes four focus areas: cloud security and identity, mobility, enhanced information protection and secure infrastructure.

Security services help customers understand how to protect and innovate their IT infrastructure, applications and data against internal and external threats. Security services may be an element of a customized program of support services, available for an additional fee and may be defined in an exhibit and referenced in your Work Order.

Education services

Education services provide training that help to enhance your support staff's technical and operational skills through either onsite, online or on-demand instruction.

Education service types	Plan
On-demand Education	✓
Webcasts	✓
Chalk Talks	+
Workshops	+

✓ - Included as part of your Base Package.

⊕ - Additional service that may be purchased.

On-demand Education: Access to a collection of online training materials and online labs from a workshop library digital platform developed by Microsoft.

Webcasts: Access to live Microsoft-hosted educational sessions, available on a wide selection of support and Microsoft technology topics, delivered remotely online.

Chalk Talks: Short interactive services, typically one-day sessions, that cover product and support topics provided in a lecture and demonstration format and are delivered by a Microsoft resource either in person or online.

Workshops: Advanced level technical training sessions, available on a wide selection of support and Microsoft technology topics, delivered by a Microsoft resource in person or online.

Workshops are purchased on a per-attendee basis or as a dedicated delivery to your organization, as specified on your Work Order. Workshops cannot be recorded without express written permission from Microsoft.

Additional Proactive services

Additional Proactive service types	Plan
Custom Proactive Services (Maintenance, Optimization and Education services)	⊕
Support Technology Advisor	⊕
Proactive Accelerator	⊕

+ - Additional service that may be purchased.

Custom Proactive services: A scoped engagement with Microsoft resources to deliver services at the customer's direction, in person or online, which are not otherwise described in this document. These engagements include Maintenance, Optimization and Education service types.

Support Technology Advisor (STA): A customized service that provides a technology assessment supporting customer business goals including, but not limited to, workload optimization, adoption or supportability, delivered by a Microsoft resource. This service may include a plan and technical guidance tailored to customer environment and business goals.

Proactive Accelerator: A Microsoft resource-led service comprised of a scoped set of activities to help you accomplish a technical or business outcome based on goals to eliminate deployment risks, increase availability, or optimize solution performance. Using a programmatic approach, the Microsoft resource will determine the set of activities needed for engagement, which may include, but are not limited to, fit gap analysis, onboarding, optimization, knowledge transfer, design validation, and implementation plan.

Other Proactive	Plan
Proactive Credits	+

Proactive Credits: The value of exchangeable services represented in credits on your Work Order. Proactive Credits can then be exchanged for, or applied to, one or more defined additional services, as described within this document, and at current rates provided by your Microsoft Services representative. After selecting the available additional service, we will deduct the value of that service from your credit balance, rounded up to the nearest unit.

Reactive services

Reactive services help resolve issues in your Microsoft environment and are typically consumed on demand. The following reactive services are included as-needed for currently supported Microsoft products and online services, unless otherwise noted on your Work Order.

Reactive service types	
Advisory Support	✓
Problem Resolution Support	✓
Reactive Support Management	✓
Extended Hotfix Support	✓
Onsite support	+
Root Cause Analysis	+
Reactive Support Management Add-on	+

Reactive service types	
Cybersecurity Support Services	+

✓ - Included as part of the Base Package.

+ - Additional service that may be purchased.

Advisory Support: Phone-based support on short-term (limited to six hours or less) and unplanned issues for IT Professionals. Advisory Support may include advice, guidance, and knowledge transfer intended to help you deploy and implement Microsoft technologies in ways that avoid common support issues and that can decrease the likelihood of system outages.

Architecture, solution development and customization scenarios are outside of the scope of these Advisory Services.

Problem Resolution Support: This assistance for problems with specific symptoms encountered while using Microsoft products includes troubleshooting a specific problem, error message or functionality that is not working as intended for Microsoft products. Incidents may be initiated either by phone or submitted via the web. Support requests for services and products, not covered by the applicable online service support portal, are managed from within the Microsoft Services online portal.

Severity definitions and the Microsoft estimated initial response times are detailed in the incident response tables below.

Upon your request, we may collaborate with third-party technology suppliers to help resolve complex multi-vendor product interoperability issues, however, it is the responsibility of the third party to support its product.

The incident severity determines the response levels within Microsoft, initial estimated response times and your responsibilities. You are responsible for outlining the business impact to your organization, in consultation with us, and Microsoft will assign the appropriate severity level. You can request a change in severity level during the term of an incident should the business impact require it.

Severity and situation	Our expected response	Your expected response
Severity 1 Critical business system down: Business at risk. Complete loss of a critical application or solution. Needs immediate attention	Azure components ¹ First call response in 15 minutes or less All other products and services - First call response in one hour or less Critical situation resource ² assigned Resources at your site, after 24 hours, with customer agreement Continuous effort on a 24/7 basis ³ Rapid escalation within Microsoft to product teams Notification of our senior executives, as required	- Notification of your senior executives, as requested by us Allocation of appropriate resources to sustain continuous effort on a 24/7 basis ³ Rapid access and response Submission via phone or web
Severity A Critical business system degraded: Significant loss or degradation of services Needs attention within one hour	First call response in one hour or less Critical situation resource ² assigned Continuous effort on a 24/7 basis ²	Allocation of appropriate resources to sustain continuous effort on a 24/7 basis ³ Rapid access and response Submission via phone or web
Severity B Moderate business impact: Moderate loss or degradation of services, but work can reasonably continue in an impaired manner Needs attention within two business hours ⁶	First call response in two hours or less Effort during business hours only ⁴	Allocation of appropriate resources to align to Microsoft effort Access and response from change control authority within four business hours Submission via phone or web
Severity C Minor business impact:	First call response in four hours or less Effort during business hours only ⁴	Accurate contact information on case owner Responsive within 24 hours Submission via phone or web

Severity and situation	Our expected response	Your expected response
Substantially functioning with minor or no impediments of services		
Needs attention within four business hours ⁶		

¹ The listed response time for your Azure components does not cover Azure China Cloud, Azure StorSimple, GitHub AE, Azure Communication Services or Billing & Subscription Management.

² Critical situation resources help drive for prompt issue resolution through case engagement, escalation, resourcing, and coordination.

³ We may need to downgrade the severity level if you are not able to provide adequate resources or responses to enable us to continue with problem resolution efforts.

⁴ Business hours are generally defined as 09:00 to 17:30 Local Standard Time, excluding holidays and weekends. Business hours may differ slightly in your country.

Reactive Support Management: Reactive Support Management provides oversight of support incidents to drive timely resolution and a high quality of support delivery. Service Delivery Management will be utilized for the Reactive Support Management of all support requests.

Per the Incident Response tables above, for Severity B and C incidents, the service is available by customer request during business hours to the Microsoft resource who can also provide escalation updates when requested. For Severity 1 and A incidents, an enhanced escalation process is initiated and automatically executed. The assigned Microsoft resource is then responsible for ensuring continued technical progress by providing you with status updates and an action plan.

For non-business hours extended coverage, you may purchase Additional Reactive Support Management Hours.

Extended Hotfix Support: Extended Hotfix Support allows you to request non-security hotfixes for select Microsoft software that has entered the Extended Support Phase of the Fixed Lifecycle, as defined by the Policy at <http://support.microsoft.com/lifecycle>. Service-specific prerequisites and limitations:

- Extended Hotfix Support availability is limited to the following products/product families:
 - Applications: Office
 - Dynamics: AX, CRM
 - Server: Exchange Server, SQL Server, System Center (excluding Configuration Manager), Windows Server
 - Systems: Windows client, Windows Embedded operating systems
- For the most current information about non-security hotfix availability for specific product versions, check the product lifecycle notes here.
- Although we use commercially reasonable efforts to respond to your requests for non-security hotfixes, you acknowledge that there may be cases in which a hotfix cannot be created or provided.
- Hotfixes are designed to address your specific problem and are not regression tested.
- Hotfixes may not be distributed to unaffiliated third parties without our written consent.

- Hotfix delivery times for non-English versions may vary, and localization fees may apply.
- We will not provide added features, functionality, updates, or design changes. We will only address problems for a selected product which cause it to crash, lose data, or otherwise materially deviate from the product's documented functionality.

Onsite Support: Onsite reactive support provides assistance at your location. This service is subject to Microsoft resource availability and requires an additional charge per onsite visit.

Root Cause Analysis: When explicitly requested prior to incident close, we will perform a structured analysis of potential causes of a single incident, or a series of related problems. You will be responsible for working with the Microsoft team to provide materials such as log files, network traces, or other diagnostic output. Root Cause Analysis is only available for certain Microsoft technologies and may incur an additional charge.

Reactive Support Management Add-on: You may elect to purchase additional hours to provide Reactive Support Management. These resources will operate remotely and deliver the service during the business hours in the time zone that is agreed upon in writing. This service is delivered in English and, where available, may be provided in your spoken language. This service is subject to Microsoft resource availability.

Cybersecurity Support Services: Provides specialized cybersecurity-related assistance under both reactive and proactive scenarios ("Cybersecurity Services"). These services help to reduce the risk of targeted cyber attacks, better prepare for security crisis situations or investigate and contain an active security compromise. Cybersecurity Services provides a customized program of support services, and maybe available for an additional fee defined in an Exhibit referenced in your Work Order.

Service delivery management

Service Delivery Management (SDM) is included with your support services, unless otherwise noted herein or in your Work Order. Additional delivery management services may be added when purchasing additional services or enhanced services and solutions.

SDM services are provided digitally and by a designated customer success account manager. This named resource may operate either remotely or onsite at your location.

Service Delivery Management scope

The following SDM services are available:

Service delivery management service types	Plan
Customer Organization Enablement	✓
Microsoft Product, Service, and Security Updates Guidance	✓
Program Development & Management	✓
Unified Enterprise Support Onboarding	✓
Cloud Success Program	+

Service delivery management service types	Plan
Customer Success Account Manager Developer	✓ ¹
Executive Relationship Management	✓
Service Delivery Management Add-on	+
Onsite Service Delivery Management	+

✓ - Included as part of the Base Package.

+ - Additional service that may be purchased.

✓¹ - Additional services that may be provided by Microsoft.

Customer Organization Enablement: Guidance and information provided to your named Support Service Administrator about how to manage utilization of your Unified Support services, and prepare you to use Unified Support digital and reactive services.

Microsoft Product, Service and Security Updates Guidance: Information shared with you about important upcoming product and service features and changes, as well as security bulletins for Microsoft technologies.

Program Development & Management: Activities designed to plan, propose, and manage your support program's services, across your organization to help you realize greater value from your investments in Microsoft technology and services. Microsoft may recommend a variety of services intended to help you achieve key business and technology outcomes, making use of the capabilities included in your Base Package support, as well as additional services you may purchase.

Unified Support Onboarding: Activities to support your initiation into Unified Support, including the introduction and promotion of self-service capabilities in the online support portal, with a goal of ensuring timely utilization of your Unified Support services.

Cloud Success Program: Planning and delivery services are included to help you achieve specific cloud outcomes, empowering you to accelerate the implementation, adoption and realized value of Microsoft cloud technologies.

Customer Success Account Manager Developer: A development focused Microsoft support resource who will deliver strategic advice and guidance to accelerate innovation and drive efficiency throughout the software development lifecycle. These limited resources may be assigned by Microsoft as conditions allow.

Executive Relationship Management: A set of activities to ensure the Microsoft Support team is aligned to your organization's strategic priorities and engaged with key business and technology decision makers.

Service Delivery Management Add-on: You may elect to purchase additional custom SDM resources to provide service delivery management services as part of a pre-determined scope of work, which are not explicitly detailed in this document. These resources will operate either remotely or onsite at your location. This service is also subject to Microsoft resource availability.

Onsite Service Delivery Management: You may request onsite visits from your customer success account manager that may require an additional charge per visit. This service is subject to Microsoft resource availability.

2.3 Enhanced services and solutions

In addition to the services provided as part of the Base Package or as additional services, the following optional enhanced services and solutions may be purchased. Enhanced services and solutions are available for an additional fee and may be defined in an Exhibit referenced in your Work Order.

Service	Plan
Designated Support Engineering	+
Rapid Response	+
Azure Event Management	+
O365 Engineering Direct	+
Developer Support	+ ¹
Support for Mission Critical	+

+ - Additional service that may be purchased.

+¹ - Additional service that may be purchased up to a limited maximum quantity.

Designated Support Engineering

Designated Support Engineering (DSE): DSE services may be purchased as pre-defined offerings or as a block of custom hours that can be used to deliver scoped proactive services.

When purchased as hours, DSE service hours are then deducted from your total purchased hours as they are utilized and delivered.

Pre-defined DSE offerings are tailored to your environment and help you achieve a desired outcome. These offerings include required pre-defined proactive services built-in.

The focus areas for DSE services:

- Help maintain a deep knowledge of your current, and future business requirements and configuration of your information technology environment to optimize performance
- Document and share with you recommendations of the use of support services-related deliverables (e.g. supportability reviews, health checks, workshops, and risk-assessment programs)
- Help make your deployment and operation activities consistent with your planned and current implementations of Microsoft technologies

- Enhance your IT staff's technical and operational skills
- Develop and implement strategies to help prevent future incidents and increase system availability of your covered Microsoft technologies
- Help determine the root cause of recurring incidents and to provide recommendations to prevent further disruptions in the designated Microsoft technologies

Regardless of how DSE is purchased, resources are allocated, prioritized and assigned based on the agreement of the parties during the initiation meeting and documented as part of your service delivery planning.

Service-specific prerequisites and limitations

- You must have a current Microsoft Unified Support services agreement to support your DSE services. If your Microsoft Unified Support services agreement expires or is terminated, your DSE service will be terminated on the same date.
- DSE services are available during normal business hours (09:00 to 17:30 Local Standard Time, excluding holidays and weekends).
- DSE services support the specific Microsoft products and technologies selected by you and listed in your Work Order.
- DSE services are delivered for a single support location in the designated support location identified in your Work Order.

Rapid Response

Rapid Response: Rapid Response provides accelerated reactive support for your cloud services by routing support incidents to technical experts and providing an escalation path to cloud service operations teams, as required.

To receive Rapid Response services for your Microsoft Azure components you must submit an incident through the applicable cloud service portal. Your Problem Resolution Support requests will be directly routed to a Rapid Response support queue which is staffed by a designated team of engineers with cloud service expertise. For this team to have basic knowledge of your deployment, you must provide documentation on basic Azure deployment and database topology, as well as scaling and load balancing plans where available. While incidents may require resources from standard product support professionals for resolution, the Rapid Response team retains primary responsibility for the incidents 24x7x365.

For your Azure components, the response times for problem resolution support are listed in the table below and supersede any expected Base Package support response times. Rapid Response does not cover Azure Media Services, Azure Stack, Azure StorSimple, GitHub AE, Azure Communication Services, Billing & Subscription Management, Universal Print, Test base for M365, or Microsoft Mesh.

Rapid Response purchase is subject to resource availability. Please consult your customer success account manager for availability details.

Rapid Response Severity and situation	Our expected response	Your expected response
Severity 1 Critical business system down: Business at risk. Complete loss of a critical application or solution Loss of a core business process and work cannot reasonably continue Needs attention within 15 minutes	First call response in 15 minutes or less Continuous effort on a 24x7 basis ¹ Access to Microsoft's experienced specialists ² Rapid escalation within Microsoft to cloud service operations teams	Notification of your senior executives, as requested by us Allocation of appropriate resources to sustain continuous effort on a 24x7 basis ¹ Rapid access and response
Severity A Critical business system degraded: Significant loss or degradation of services	Notification of our senior executives, as required	

¹ We may need to downgrade from 24x7 if you are not able to provide adequate resources or responses to enable us to continue with problem resolution efforts

² Rapid Response Problem Resolution Support services are only available in English and Japanese.

Azure Event Management

Microsoft Azure Event Management ("AEM"): provides enhanced support before, during, and after critical customer events ("Event"). A critical event is defined as a period of high business impact and/or peak demand for the customer, requiring the highest levels of service availability and performance. Events must be confirmed with your customer success account manager at least 8 weeks before the event.

AEM supports events that utilize core Microsoft Azure services. The details of the solution and what Azure services it leverages must be shared with the AEM team well in advance of the actual event, but no later than, as input to the assessment.

As part of the Pre-Event activities, the AEM team will:

- Assess and familiarize itself with your solution
- Identify possible issues and risks affecting uptime and stability
- Determine the desired outcomes from a resiliency perspective
- Develop and maintain the service delivery plan for the solution

The AEM support team will provide a list of recommended and required actions to remediate any problems which could affect the solution availability or performance the Day of Event.

During the Event, the AEM team will be aware of the Event details and be prepared to resolve issues affecting the solution.

You may request Problem Resolution Support for the solution two weeks before the Event, during the Event, and one week after the Event*.

Severity and situation	Our expected response	Your expected response
Severity 1 Critical business system down: Business at risk. Complete loss of a critical application or solution Loss of a core business process and work cannot reasonably continue Needs attention within 15 minutes	First call response in 15 minutes or less and rapid escalation within Microsoft to cloud operations teams for any Microsoft Azure services ² Critical situation manager assigned in 30 minutes or less. Continuous effort on a 24x7 basis ¹ Access to Microsoft experienced specialists and rapid escalation within Microsoft to product teams Engagement of support engineers who have knowledge of your Solution configuration. Where applicable, those engineers may assist and streamline the incident management process Notification of our senior executives, as required	For the Azure Services, incident service requests should be raised online through the Microsoft Azure portal, using a predefined template specified by your customer success account manager Notification of your senior executives, as requested by us Allocation of appropriate resources to sustain continuous effort on a 24x7 basis ¹ Rapid access and response
Severity A Critical business system degraded: Significant loss or degradation of services		

¹ We may need to downgrade from 24 x 7 if you are not able to provide adequate resources or responses to help us to continue with problem resolution effort.

² AEM Problem Resolution Support services are only available in English

*Problem Resolution Support submitted prior to and after the Event will be addressed as Severity B.

Post-Event, you may request root cause analysis on all Severity 1 and Severity A incidents for your solution. Where applicable, we will provide recommendations on how the issues may be prevented in the future.

Office 365 Engineering Direct

Office 365 Engineering Direct: Provides enhanced support for the core workloads of your Microsoft Office 365 production tenant or tenants that includes prioritized access to the Office 365 engineering team. This service will be available for the listed tenant or tenants, is available for an additional fee and is defined in an Exhibit referenced in your Work Order.

Developer Support

Developer Support: Provides deeper proactive support based on cloud and product knowledge across the application development lifecycle for Customer developers building, deploying and supporting applications on Microsoft's platform. Developer Support delivers comprehensive support providing

customers with cloud architecture, vulnerability assessments, ALM/DevOps solutions, security development lifecycle, code reviews, performance and monitoring, application modernization, internet of things (IoT) implementation and management, training, and testing. Developer Support is available for an additional fee.

Support for Mission Critical

Support for Mission Critical: Provides a higher level of support for a defined set of Microsoft products and Online Services that make up a part of your mission critical solution, as specified on your Work Order. Support for Mission Critical provides a customized program of support services, is available for an additional fee and is defined in an Exhibit referenced in your Work Order.

2.4 Multi-country Support

Multi-country Support Services Overview

In conjunction with Microsoft Unified Enterprise Support services, Multi-country Support provides support to you in multiple Support Locations, as described in your Work Order (or Work Orders). The description of the Multi-country Support structure follows:

- **Host:** This is the Support Location where you have contracted for Microsoft Unified Support in your Work Order. Unless otherwise noted, this will be the primary location of your designated customer success account manager.
- **Downstream:** This is a Support Location designated in your Work Order where you are to receive Microsoft Unified Enterprise Support services, other than the Host location, and are entitled to the services you purchase for that location.

How to Purchase

This USSD describes the Multi-country Support services available. The specific services and related quantity, if applicable, will be listed in the associated Work Order by Support Location.

The Services described herein may be delivered to your Support Location(s) designated in the Host Work Order and, as may be, allocated by the Host, as part of your Microsoft Unified Enterprise Support agreement with the following modifications:

- **Base Package Services:** Unless noted otherwise, Base Package Services (those denoted with a "✓") will be available to your designated Support Locations or as allocated to Support Location(s) by the Host on the Host Work Order.
- **Reactive Services:** Reactive Services may be provided remotely to locations other than and including the Host, except as follows:
 - **Onsite Support:** Pre-purchased reactive onsite support services will be available to Support Location(s) as designated in your Work Order, other than Exception Countries.
 - During a "Severity 1" Problem Resolution Support situation, pre-purchased Onsite Support resources may be dispatched to designated and non-designated Support Locations.
- **Service Delivery Management (SDM):** As designated in your Work Order, SDM may be delivered to designated Host and Downstream Support Location(s). The availability of SDM

services that are included in your Base Package will be allocated by the Host and managed by the Host customer success account manager. SDM delivery will be limited to the business hours of the Host location. Additional SDM services may be required when purchasing additional services or enhanced services and solutions.

- **Additional SDM:** Additional SDM resources may be purchased for the Host or Downstream Support Location(s), as indicated in a Work Order, and will be delivered to the designated Support Location. Subject to resource availability and the above.

Availability of optional services (those denoted with a "+" in the Support tables above) are as follows:

- **Proactive Services**
 - You may be eligible for Proactive Services, the quantity of which will be listed on your Work Order and available in the Support Location(s) designated in your Work Order, other than the Exception Countries.
- **Maintenance Services – Root Cause Analysis:** Services purchased will be available to staff in designated Support Location(s).
- **Support Technology Advisor (STA):** STA services will be available in the Support Location(s) designated in your Work Order, other than Exception Countries, and are subject to resource availability.
- **Enhanced services and solutions:** All enhanced services and solutions may be purchased for use in either Host or Downstream Support Locations. Subject to availability. Other restrictions may apply.
- Other purchased support services will be available in the Support Location(s) designated in your Work Order.

Multi-Country Support Additional Terms and Conditions

In addition to those terms and conditions outlined herein and your Work Order, our delivery of services, as outlined herein, is based upon the following prerequisites and assumptions:

- We may allow staff in non-designated support location(s) to participate in remote Proactive Services that have been purchased for the Host or a Downstream Support Location and designated in the Work Order. Such participation will be allowed at the discretion of Microsoft.
- Proactive Credits can only be exchanged between Host and Downstream Support Locations listed on your Work Order, except as noted. All exchanges will be completed based on current currencies and rates for Proactive Credits in the respective Support Locations. Current rates can be provided by your Microsoft Services representative. Any exchanges resulting in fractional Proactive Credits will be rounded up to the nearest unit. Proactive Credits may not be exchanged to or from Exception Countries.
- The Customer shall be solely responsible for any tax obligations that arise because of the distribution or exchange of purchased support services between Host and Downstream Support Location(s).
- Services changes or exchanges made during the Term of Work Order may require agreement in writing.

- **Billing Consolidation:** Unless otherwise noted, a single invoice will be issued for the amount due, inclusive of all Services for all Support Locations indicated on your Work Order. Taxes will be based on an assessment of the Microsoft Signatory and your Host Location. The Customer shall be solely responsible for any additional taxes due.
- **Exceptions to Billing Consolidation:** Services purchased for delivery in the Republic of India, the People's Republic of China, the Republic of China (Taiwan), the Republic of China (Hong Kong), the Republic of Korea, Japan, New Zealand, Macau and Australia (**all Exception Countries**) must each have a separate Work Order listing the Services to be delivered in that Support Location. Services will be invoiced to the respective Support Location and will include any applicable local tax.

2.5 Additional terms and conditions

Microsoft Unified Support services are delivered based on the following prerequisites and assumptions.

- Base Package reactive services are provided remotely to the location(s) of your designated support contacts. All other services are provided remotely to your location(s) designated or listed on your Work Order, unless otherwise set forth in writing.
- Base Package reactive services are provided in English and, where available, may be provided in your spoken language. All other services are provided in the spoken language of the Microsoft services location providing services, or in English, unless otherwise agreed to in writing.
- We provide support for all versions of commercially released, generally available Microsoft software and Online Services products that you have purchased based on the declared licensing enrollments and agreements and/or billing account ID in Appendix A of your Work Order and are identified on the Product Terms, published by Microsoft from time to time at <http://microsoft.com/licensing/contracts> (or at a successor site that Microsoft identifies), unless otherwise set forth in a Work Order, an Exhibit to this Unified Support Services Description, or specifically excluded on your online support portal at <http://serviceshub.microsoft.com>.
- Support for pre-release and beta products is not provided, except as otherwise noted in an attached exhibit.
- All services, including any additional services purchased as part of and during the Term of a Support Work Order, are forfeited if not utilized during the Term of the applicable Work Order.
- We can access your system via remote connection to analyze problems at your request. Our personnel will access only those systems authorized by you. To utilize remote connection assistance, you must provide us with the appropriate access and necessary equipment.
- Some services may require us to store, process, and access your customer data. When we do so, we use Microsoft-approved technologies which comply with our data protection policies and processes.

- When purchasing additional services, we may require the inclusion of service delivery management to facilitate delivery.
- If you ordered one type of service and wish to exchange it for another type of service, you may apply equivalent value to an alternative service where available, and agreed with your service delivery resource.
- Software Assurance Benefits 24x7 Problem Resolution Support Incidents (SA PRS Incidents, or "SAB"), may be converted to an equivalent value (as determined by Microsoft) and used towards the fees for Base Package support, eligible components of Designated Support Engineering (DSE) and/or eligible components of Enhanced services and solutions. Your delivery management resource can confirm such value(s) and fee(s), if applicable. After 30 days of the Support Commencement Date and/or multi-year Support annual anniversary date, we may invoice you for the equivalent value of any deficit SAB you commit for any such conversion, as designated in your Work Order. Software Assurance Benefits are subject to the terms stated herein and the Product Terms, including, but not limited to, Appendix B of the Product Terms. Further details are also available at www.microsoft.com/licensing/licensing-programs/software-assurance-by-benefits, such as changes to the Problem Resolution Support benefit beginning in February 2023 that will affect eligibility of Base Package or eligible components of your support agreement and which may result in adjustments to equivalent incident value.
- Not all additional services may be available in your country. Please contact your service delivery resource for details.
- You agree that the only non-Microsoft code to which you provide us access to is code that you own.
- The services may include Services Deliverables, advice and guidance related to code owned by you or by Microsoft, or the direct provision of other support services.
- When providing Reactive services, Microsoft does not provide code of any kind, other than sample code.
- Customer will assume all responsibility for, and risks associated with, implementing and maintaining any code provided in the performance of support services.
- There may be minimum platform requirements for the services purchased.
- Services may not be delivered through to your customers.
- Where onsite visits are mutually agreed upon and not pre-paid, we will bill you for reasonable travel and living expenses.
- GitHub Support Services are provided by GitHub, Inc., a wholly owned subsidiary of Microsoft Corporation. Notwithstanding anything to the contrary in your Work Order, the GitHub Privacy Statement available at https://aka.ms/github_privacy and the GitHub Data Protection Addendum and Security Exhibit located at https://aka.ms/github_dpa will apply to your procurement of GitHub Support Services.

- **Acceptable Use Policy** - Customer must not (and is not licensed to) use the Services Deliverables:
 - in a way prohibited by law, regulation, governmental order or decree;
 - to violate the rights of others; or
 - in any application or situation where use of the Service Deliverables could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage, except in accordance with the High Risk Use section below.

High Risk Use

WARNING: Modern technologies may be used in new and innovative ways, and Customer must consider whether its specific use of these technologies is safe. The Services Deliverables are not designed or intended to support any use in which a service interruption, defect, error, or other failure of a Services Deliverable could result in the death or serious bodily injury of any person or in physical or environmental damage (collectively, "High Risk Use").

Accordingly, Customer must design and implement the Services Deliverables such that, in the event of any interruption, defect, error, or other failure of the Services Deliverables, the safety of people, property, and the environment are not reduced below a level that is reasonable, appropriate, and legal, whether in general or for a specific industry. Customer's High Risk Use of the Services Deliverables is at its own risk. Customer agrees to defend, indemnify and hold Microsoft harmless from and against all damages, costs and attorneys' fees in connection with any claims arising from a High Risk Use associated with the Services Deliverables, including any claims based in strict liability or that Microsoft was negligent in designing or providing the Services Deliverables to Customer in accordance with Customer's specifications. The foregoing indemnification obligation is in addition to any defense obligation set forth in Customer's Agreement and is not subject to any limitation of, or exclusion from, liability contained in such agreements.

- Additional prerequisites and assumption may be set forth in relevant Exhibits.

2.6 Your responsibilities

Optimizing the benefits of your Microsoft Unified Support services is contingent upon you fulfilling the following responsibilities, in addition to those set forth in any applicable exhibits. Failure to comply with the following responsibilities may result in delays of service:

- You will designate a named support services administrator who is responsible for leading your team and managing all of your support activities and internal processes for submitting support incidents requests to us.
- If you purchase Multi-country Support Services, you will be required to designate a named support services administrator for your Host Support Location who is responsible for leading your local team and managing all your local support activities and internal processes for submitting support incident requests to us. And you may be required to designate a named support services administrator in other Support Locations.
- You can designate named reactive support contacts, as needed, who are responsible for creating support requests through the Microsoft support website or by phone. Cloud administrators for your cloud-based services may also submit cloud support requests through the applicable support portals.

- For online services support requests, Cloud administrators, for your cloud-based services, must submit support requests through the applicable online service support portal.
- When submitting a service request, your reactive support contacts should have a basic understanding of the problem you are encountering and an ability to reproduce the problem in order to assist Microsoft in diagnosing and triaging the problem. These contacts should also be knowledgeable about the supported Microsoft products and your Microsoft environment to help resolve system issues and to assist Microsoft in analyzing and resolving service requests.
- When submitting a service request, your reactive support contacts may be required to perform problem determination and resolution activities, as requested by us. These may include performing network traces, capturing error messages, collecting configuration information, changing product configurations, installing new versions of software or new components, or modifying processes.
- You agree to work with us to plan for the utilization of services, based upon the services you purchased.
- You agree to notify us of any changes to the named contacts designated in your Work Order.
- You are responsible for backing up your data and for reconstructing lost or altered files resulting from catastrophic failures. You are also responsible for implementing the procedures necessary to safeguard the integrity and security of your software and data.
- You agree, where possible, to respond to customer satisfaction surveys that we may provide from time to time regarding the services.
- You are responsible for any travel and expenses incurred by your employees or contractors.
- You may be asked by your service delivery resource to fulfill other responsibilities specific to the service you purchased.
- When using cloud services as part of this support, you must either purchase or have an existing subscription or data plan for the applicable online service.
- You agree to submit requests for Proactive services and enhanced services and solutions, along with any necessary or applicable data, no later than 60 days prior to the expiration date of the applicable Work Order.
- You agree to provide our service delivery team required to be onsite with reasonable telephone and high-speed Internet access and access to your internal systems and diagnostic tools, as applicable.

© 2021 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

EXHIBIT A-2

Statement of Work

Microsoft Consulting Support Description

Table of content

- 1 About this document..... 3
- 2 Consulting Services 24
 - 2.1 How to Purchase 24
 - 2.2 **Description of Services**24
 - 2.3 Your Responsibilities.....27

1 About this document

The Microsoft Consulting Services Description provides you with information on the support services that are available to purchase from Microsoft.

Please familiarize yourself with the descriptions of the services that you purchase, including any prerequisites, disclaimers, limitations and your responsibilities. The services that you purchase will be listed in your Statement of Services (SOS) or another applicable Statements of Work that reference and incorporates this document.

Not all services listed in this document are available globally. For details on which services are available for purchase in your location, contact your Microsoft Services representative. Available services are subject to change.

2 Consulting Services

2.1 How to Purchase

Consulting services are available as technical professional services for resources at labor hourly rates set forth in Exhibit B-2, Microsoft Consulting Services Published Price List. Customer will pay for fully burdened hourly rates in Exhibit B-2.

2.2 Description of Services

The County requires Microsoft Consulting Services (MCS) for a full range of project-based technical consulting needs, many involving, but not necessarily limited to, the provision of customized software and performance management solutions. MCS are the customer-facing onsite technical consulting services that specialize in the front-life-cycle stages (plan, design, architect, develop/code and deploy).

The County requires MCS to provide knowledge transfer, guidance, and assistance to the County in developing intranet/internet strategies, prototyping, implementation, and deployment of solutions spanning across infrastructure and application areas.

MCS support areas include, but are not limited to, the following types of work: Digital Advisory Services, Information Technology Strategic Architecture and Planning, Architecting and Deploying Core Infrastructure Technologies, Application Development Project Services, Collaboration Design and Deployment Services, Dynamics Suite Design and Deployment Services, Cyber Security Services from Microsoft Corporation, Cyber Security Incident Response Services from Microsoft Corporation, Industry Specific Services, Other Specialized Custom Projects.

a. Digital Advisory Services (DAS)

The contractor must provide Digital Advisors to provide, at a minimum, knowledge, experience, and innovation while partnering with the County Digital Advisors must drive a program of change to build the digital business. DAS must include, at a minimum, documentation and alignment of Microsoft technologies to key County business objectives; development of a business case for identifying the potential costs and benefits for each business or functional unit that would be affected by the project; creation of an Architecture Definition Document describing application and technology functional architecture and specification requirements to support recommendations; creation of a Measurement Plan that describes metrics to measure progress against desired business objectives, accountability and timing; tailoring Microsoft Recommended Practices in oversight/governance, adoption, and measurement to the County's environment; working with the County's management team to establish program governance; and regular review of County's progress against a business objectives scorecard.

b. Information Technology Strategic Architecture and Planning

The contractor must provide Information Technology ("IT") Strategic Architecture and Planning support that addresses areas required by the County. This support must include, at a minimum, Architecture, Digital Advisory and Planning Services – including Ongoing Advisory services for the County to facilitate a strategic relationship with Microsoft. The Advisors must combine broad IT experience with strong business knowledge and provide programmatic access to high-value Microsoft resources and know-how available through any other Microsoft channel. These services must equip senior IT executives at the County with the ability to realize and demonstrate the business value of their investment in Microsoft technologies.

c. Architecture Transformation

The contractor must provide project-based consulting with a focus on business architecture and/or enterprise architecture. This support must help the County reduce architectural risk, provide structure and focus for Architectural standards and decisions, and facilitate effective interoperability between the Microsoft platform and other platforms the County may have invested in.

d. Platform Rationalization

The contractor must provide project-based consulting with a focus on infrastructure and application rationalization and consolidation. This offering is targeted towards enabling customers to optimize operating/capital expenditures in IT and improve IT efficiency and effectiveness.

e. Microsoft IT Strategy Roadmap and Enterprise Architecture

The contractor must work with the County's key stakeholders to produce or update a Microsoft IT Strategy Roadmap and Enterprise Architecture.

f. IT and Capabilities Map

The contractor must provide a detailed approach to establishing a capabilities map of both business and IT capabilities based on the Microsoft approach to capturing Business Architecture.

g. Enterprise Architecture Plan

The contractor must provide high-level architectural design and guidance for Microsoft products and technologies by leveraging the Windows Server System Reference Architecture (WSSRA) in support of the Microsoft IT Strategy Roadmap. The contractor must develop appropriate technical standards and processes, in conjunction with County architects that will enable greater consistency, ease of integration, simpler maintenance and management. Examples of standards and processes that may be required include, at a minimum: architectural standards, security standards and processes, coding standards, performance testing standards and processes, configuration/release management processes, and quality review standards and processes.

h. Architecting and Deploying Core Infrastructure and Cloud Technologies

The contractor must provide Architecting and Deploying Core Infrastructure, which has long been a staple of the Systems Integrator community but Cloud technologies have created a need for

both customers and Systems Integrators to work directly with MCS for the best resources. MCS is ideally suited to provide an infusion of knowledge, design and preferred practices with the latest version of Microsoft's portfolio of core technologies and platforms: Azure, O365, Dynamic 365, Active Directory, Windows Server, etc. This offering is based on cloud and server architecture, planning, imaging, and deployment. This offering provides a framework for the end-to-end needs of a customer for solution that are cloud based or on premise. Components of this offering must include, but not limited to, digital transformations, Cloud and hybrid needs definition, assessing the infrastructure, planning the deployment, addressing application compatibility issues, creating standard deployment images, and operational guidance post deployment.

i. Application Development Project Services

The contractor must provide Microsoft Consulting Services providing application lifecycle management offerings that will help organizations identify opportunities to become more predictable and efficient throughout their application lifecycle. This support must provide a framework and preferred practices that will improve developer agility, productivity and time to value for business solutions utilizing Microsoft technologies. The range of application engagements under this required support is wide and varied to include Mission Critical applications as well as administrative functions. The contractor must support, at a minimum, requirement gathering, business process identification, business rule definition, prototyping a solution, piloting a solution through testing cycles, and, of course, application deployment using preferred practices of rapid, iterative processes based on Microsoft's own, Microsoft Solutions Framework.

j. Collaboration Design and Deployment Services

The contractor must provide Microsoft Consulting Services, providing collaboration services for customers who are attempting to use Microsoft collaboration technologies in their enterprise. This support may include, but is not limited to, Microsoft Enterprise Search engagement that is designed to assist with giving a customer the confidence needed to successfully plan their implementation of Enterprise Search in the enterprise with O365, Azure, Dynamics 365 and more. In addition, the requirement gathering, design and deployment of these solutions both technically and process and policy-wise must be provided by the contractor as part of MCS.

k. Cyber Security Services from Microsoft Corporation

The contractor must provide Cyber Security Service from Microsoft Corporation, providing customers innovative solutions to their most troublesome cybersecurity challenges. The contractor must leverage its deep relationships across the Microsoft security ecosystem, the Cybersecurity team to bring the power and knowledge of the "factory team" to the County. The contractor's Cybersecurity teams of specialists must help the County assess their greatest risks and build the strategic and tactical plans that will help manage those risks.

I. Dynamics 365 Suite Design and Deployment Services

The County requires access to Microsoft's suite of CRM and ERP products. The contractor must provide Microsoft Consulting Services to work with a customer in order to do the requirement gathering, design, prototyping, testing, piloting, integration and deployment of these technologies. MCS must provide, at a minimum, architectural support, project leadership, integration of the Dynamics 365 products with Microsoft Exchange Server, Microsoft Office SharePoint Server, Skype, Microsoft Office Outlook and many more options.

m. Industry Specific and Custom Services

MCS offers industry specific and custom services that are highly customized. The contractor must provide custom services that include, at a minimum, the design and deployment of Interactive Media Manager solutions, to imagery visualization technologies implementation, to mobile device deployments, to testing services providing by MCS Global Delivery focused on the work done by Customer IT for meet the standards of performance and scalability. Custom services are case-by-case defined, scoped and engaged with the customer for maximum impact in leveraging Microsoft assets through MCS. Industry specific and custom services typically use, require and take-advantage of Microsoft specific and proprietary resources that exist only within Microsoft Corporation as the intellectual property owner of Microsoft technologies. The overall goal of these services is to improve, advance and accelerate the use of your licensed Microsoft technologies licensed.

2.3 Your Responsibilities

Optimizing the benefits of your Microsoft Consulting services is contingent upon you fulfilling the following responsibilities, in addition to those set forth in any applicable exhibits. Failure to comply with the following responsibilities may result in delays of service:

- You will designate a named support services administrator who is responsible for leading your team and managing all of your support activities and internal processes for submitting support incidents requests to us.
- If you purchase Multi-country Support Services, you will be required to designate a named support services administrator for your Host Support Location who is responsible for leading your local team and managing all your local support activities and internal processes for submitting support incident requests to us. And you may be required to designate a named support services administrator in other Support Locations.
- You can designate named reactive support contacts, as needed, who are responsible for creating support requests through the Microsoft support website or by phone. Cloud administrators for your cloud-based services may also submit cloud support requests through the applicable support portals.
- For online services support requests, Cloud administrators, for your cloud-based services, must submit support requests through the applicable online service support portal.
- When submitting a service request, your reactive support contacts should have a basic understanding of the problem you are encountering and an ability to reproduce the problem in order to assist Microsoft in diagnosing and triaging the problem. These contacts should also be

knowledgeable about the supported Microsoft products and your Microsoft environment to help resolve system issues and to assist Microsoft in analyzing and resolving service requests.

- When submitting a service request, your reactive support contacts may be required to perform problem determination and resolution activities, as requested by us. These may include performing network traces, capturing error messages, collecting configuration information, changing product configurations, installing new versions of software or new components, or modifying processes.
- You agree to work with us to plan for the utilization of services, based upon the services you purchased.
- You agree to notify us of any changes to the named contacts designated in your Statement of Service.
- You are responsible for backing up your data and for reconstructing lost or altered files resulting from catastrophic failures. You are also responsible for implementing the procedures necessary to safeguard the integrity and security of your software and data.
- You agree, where possible, to respond to customer satisfaction surveys that we may provide from time to time regarding the services.
- You may be asked by your service delivery resource to fulfill other responsibilities specific to the service you purchased.
- When using cloud services as part of this support, you must either purchase or have an existing subscription or data plan for the applicable online service.
- You agree to provide our service delivery team required to be onsite with reasonable telephone and high-speed Internet access and access to your internal systems and diagnostic tools, as applicable.

© 2021 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Additional Definitions and Terms and Conditions

1. Definitions. Any capitalized term not otherwise defined herein will have the meaning given to it in the Contract. In addition to the definitions in the Contract, the following definitions apply:

“Developments” means any computer code or non-code based materials (other than Products or Pre-Existing Work) developed by Contractor in collaboration with County which is provided to County in the course of performance of a WO and/or SOS.

“Fixes” means Product fixes, modifications or enhancements or their derivatives that Contractor either releases generally, (such as commercial product service packs) or that Contractor provide to County when performing Services (such as workarounds, patches, bug fixes, beta fixes and beta builds).

“Joint Ownership” means each party has the right to independently exercise any and all rights of ownership now known or here after created or recognized, including without limitation the rights to use, reproduce, modify and distribute the Developments for any purpose, without the need for further authorization to exercise any such rights or any obligation of accounting or payment of royalties;

“Open Source License Terms” means license terms that require computer code to be generally (i) disclosed in source code form to third parties; (ii) licensed to third parties for the purpose of making derivative works; or (iii) redistributable to third parties at no charge.

“Pre-Existing Work” means computer code or materials (other than Products and Fixes) developed or otherwise obtained independently of the efforts of a party under a WO and/or SOS.

“Product” means any computer code, web-based services, or materials comprising commercially released, pre-release or beta products (whether licensed for a fee or no charge) and any derivatives of the foregoing Contractor makes available to County for license which is published by Contractor, its affiliates, or a third party.

“Service Deliverables” means (i) any computer code or materials, other than Products or Fixes, that Contractor leaves with County at the conclusion of its performance of Services; (ii) Contractor's Pre-existing Work licensed to County perpetually and the Developments.

2. Ownership and license of service deliverables.

- a. Products and Fixes.** All Products, related solutions and Fixes provided under a WO and/or SOS will be licensed according to the terms of the license agreement

packaged with or otherwise applicable to such product. County are responsible for paying any licensing fees associated with products.

- b. Pre-existing Work.** All Pre-existing Work will remain the sole property of the party providing the Pre-existing Work. During the performance of Services, each party grants to the other (and each party's contractors as necessary) a temporary, non-exclusive license to use, reproduce and modify any of its Pre-existing Work provided to the other party solely for the performance of such Services.

Contractor grants County a non-exclusive, perpetual, fully paid-up license to use, reproduce and modify (if applicable) Contractor's Pre-existing Work in the form delivered to County as part of the Service Deliverables and to distribute object code version of any of the foregoing and County's derivatives thereof, to end users as an integrated part of County's software, but not as a stand-alone product.

The perpetual license to Contractor's Pre-existing Work that Contractor leaves to County at the conclusion of its performance of the Services is conditioned upon County's compliance with the terms of the Contract and the applicable WO and/or SOS.

- c. Developments.** Except as may be otherwise explicitly agreed to in a WO and/or SOS, upon payment in full Contractor grants County joint ownership in the Developments. County agrees to exercise its rights for its business operations only and County will not resell or distribute the Developments to any third party. Each party shall be the sole owner of any modifications that it makes based upon the Developments.
- d. Sample Code.** Contractor grants County a nonexclusive, perpetual, royalty-free right to use and modify any software code provided by Contractor for the purposes of illustration ("Sample Code") and to reproduce and distribute the object code form of the Sample Code, provided that County agree: (i) to not use Contractor's name, logo, or trademarks to market County's software product in which the Sample Code is embedded; (ii) to include a valid copyright notice on County's software product in which the Sample Code is embedded; and (iii) Contractor shall not be liable for any damages or liability that arises or results from County's use or distribution of the Sample Code.
- e. Open source license restrictions.** Because certain third-party software is subject to Open Source License Terms, the license rights that each party has granted to any computer code (or any intellectual property associated therewith) do not include any license, right, power or authority to knowingly incorporate, modify, combine and/or distribute that computer code with any other computer code in a manner which would subject the other's computer code to Open Source License Terms. Furthermore, each party warrants that it will not provide or give to the other party computer code that is governed by open source license terms.

- f. No Product Provided.** No Product will be provided through or licensed under the Contract.
- g. Reservation of Rights.** All rights not expressly granted in this section are reserved.

3. Restrictions on use. County may not:

- a) Rent, lease, lend, host or otherwise distribute Service Deliverables or Fixes, except as otherwise provided in a WO and/or SOS; or
- b) Reverse engineer, de-compile, or disassemble Fixes or Service Deliverables, except to the extent expressly permitted by applicable law despite this limitation; or
- c) Transfer licenses to, or sub-license Fixes or Service Deliverables to any government entity or quasi-governmental entity, except as otherwise authorized by the Contract or any WO and/or SOS.

4. Supportability of Products.

- a. Discontinuation of Support.** If Contractor determines to discontinue support for a Product being supported under a WO and/or SOS, Contractor shall provide written notice of its intent to County's Program Director. Notwithstanding its notice to County, Contractor shall still be obligated to support the Product for the duration of the WO and/or SOS or for six (6) months from the date of notice, whichever is longer.
- b. Disposition of Product.** If Contractor sells, transfers or otherwise disposes completely of the intellectual property rights of a Product being supported under a WO and/or SOS, Contractor shall give County prior written notice of such action to County's Program Manager and appropriate County Project Managers at the earliest time possible and, after good faith consultation with County concerning County's best interest shall, at no additional cost to County, either (i) arrange for the transferee to continue the support under a subcontract in which event Contractor shall remain responsible for the Services of its subcontractor [and subject to any amendments to the Contract required to address the addition of a subcontractor]; or (ii) continue support for the Product for the duration of the WO and/or SOS or for six (6) months, whichever is longer.
- c. Notice to County Regarding County Environment.** If Contractor believes that a Product being supported under an existing WO and/or SOS cannot be effectively supported in County's environment, Contractor shall provide written notice to County's Project Manager of the WO and/or SOS with a copy to County's Program

Manager and shall work reasonably with personnel designated by County's Project Manager for a period not to exceed thirty (30) days to suggest workarounds or other remedial steps which will enable Contractor to support the Product in County's environment. If, at the conclusion of this process, Contractor reasonably determines that it cannot effectively support its Product in County's environment as it has been maintained and County declines to modify its environment, as recommended by Contractor, to permit effective support, Contractor shall give County written notice of that determination and the factual basis supporting its position. If County does not modify its environment to allow effective support for the Product within ten (10) working days after receipt of such notice, Contractor shall have no obligation to provide further support for that Product provided, however, that Contractor will continue to provide support for all County's other Products covered by the WO and/or SOS

c. Unsupportable Product.

Where a Product can no longer be supported, notwithstanding the steps taken above, then Contractor shall confer with County to make such adjustments in the prepaid Services as may be required or appropriate, which may include reallocation of service that County would have used for Products Contractor will no longer support.

1 CUSTOMER SERVICE REQUEST FOR SERVICES PROCESS

Customer Departments requiring Microsoft Unified Products Support or Consulting Support services falling under the purview of Microsoft Unified Support and Consulting Services Contract:

1.1 Submit a service request using the PCS Contracts SR Tool

1.1.1 SRs can be submitted by going to:

<https://lacounty.sharepoint.com/teams/GC>

6.1.2 This service request tool enables ISD customers to request services that include:

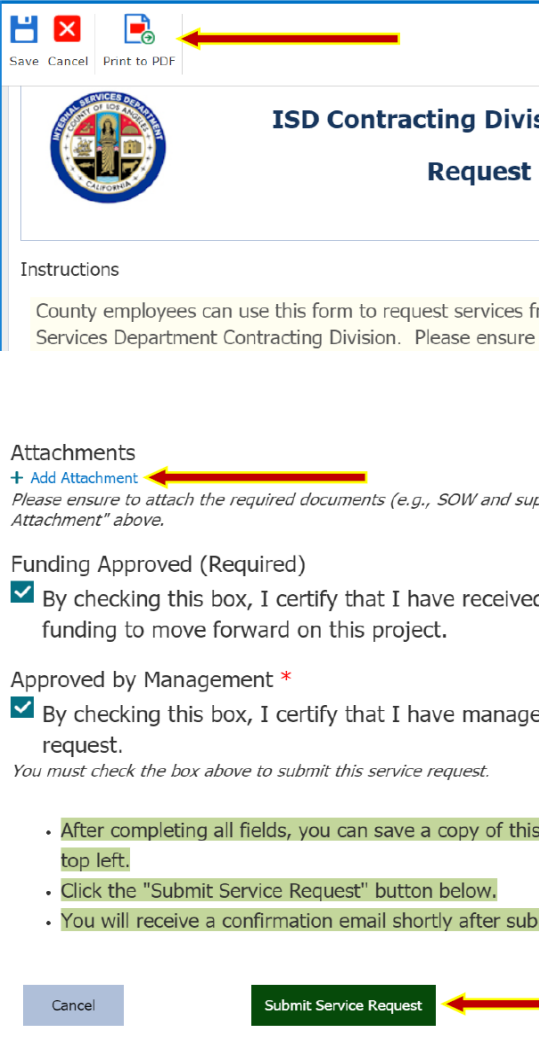
- Microsoft Unified Products Support

Item	Description
Base Package	A combination of proactive, reactive and delivery management services that support Microsoft products and/or Online Services in use within your organization. Part of your Base Package includes a Flex Allowance* to use to add proactive services (marked with "+"), enhanced services and solutions services and/or Custom Proactive services to your Base Package. Base Package included services are represented with a "□" throughout this section.
Additional services	Additional support services, including Proactive services are available to add to your Base Package during the term of your Work Order and are represented with a "+" throughout this section.
Enhanced services and solutions	Support services, which cover a specific Microsoft product or customer IT system, are available to add to your support Base Package during the term of your Work Order and are also represented with a "+" throughout this section.
Multi-country support	Multi-country Support provides support to you in multiple Support Locations, as described in your Work Order (or Work Orders).

- Microsoft Consulting Support
- Amendment Requests for existing Work Orders and/or Statement of Services
- Consulting Support Statements of Work Reviews
- Investigation and resolution of issues related to contract compliance

ISD CONTRACTING DIVISION SERVICE REQUEST USER GUIDE (FOR ISD CUSTOMERS)

Introduction: The ISD Contracting Division has created a convenient and easy method to request and track service requests. This guide helps you navigate the ISD Contracting Division Service Request Website to submit and track an online service request (SR) form.

1.		Service Request Form & Website Using a browser (Chrome, Edge or IE), go to: https://lacounty.sharepoint.com/teams/GC Click the “Launch Service Request Form” button to open the service request form *If prompted, you may need to login with your employee # in the format e123456 as your User ID, and Timesheet Password.
2.		Service Request Form 1. Fill out each required field 2. Attach all required documents by clicking on “+ Add Attachment” 3. Checkmark applicable checkboxes 4. Click on the green “Submit Service Request” button Please note: a. The submit button does not appear unless you click the management approval checkbox. b. You can save (and also print) a copy of the form prior to submitting it by clicking on “Print to PDF” at the top left. Service Request Form Fields for Reference: • Title of Your Request • Service Request Indicator • Requested Completion Date • Service Type • Request Type • Solicitation Type (if applicable) • Requestor Name (Customer) • Requestor Email (Customer) • Department ○ ISD Service (if applicable) ○ ISD Division (if applicable) • Description of Request and Comments • Attachments • Funding Approved • Approved by Management

ISD CONTRACTING DIVISION SERVICE REQUEST USER GUIDE (FOR ISD CUSTOMERS)

3.  FW: Service Request ID# 14 for INTERNAL SERVICES DEPARTMENT Retention Policy LACOUNTY 3 Year Delete (3 years)  Exhibit C.pdf 701 KB CAUTION: External Email. Proceed Responsibly. Thank you for submitting your service request to the ISD Contracting Division. Title of Request: Custodial Services - Amendment to Increase Services Service Request ID: 14 Service Request Indicator: New Contract # (if applicable): 79024 Requested Completion Date: 2/28/2020 12:00:00 AM Service Type: Custodial Services Request Type: Amendment Solicitation Type: Not Applicable Department: INTERNAL SERVICES DEPARTMENT Requestor (Customer): Diaz, Maribel Requestor Email: MDiaz@isd.lacounty.gov Request submitted by: Diaz, Maribel Description of Request and Comments: Amend Contract 79024 to increase services to facility 2. Click here to view the form you submitted. Click here to view the status of your request. Thank you, ISD Contracting Division contractservicerequests@isd.lacounty.gov	Confirmation and Status Update Emails 1. Upon submission of the service request form, the person physically submitting the form and the Requestor (if different) will receive a confirmation email (including all completed form fields, attachments and a link to check the status of the request). 2. Although the person physically submitting the form receives subsequent status update emails after each completed stage of the service request, it is recommended that Requestor view the status of their SR using the link in step 4 below.
4.  departments in proposals/bids, to the Board of Director compliance ment of contract ited to: Launch Service Request Form Service Request User Instructions Status of Open Service Requests Closed and Completed Service Requests contractservicerequests@isd.lacounty.gov	Checking Status of Service Request 1. It is recommended to view the status of your Service Request on the Contracting Division website at: https://lacounty.sharepoint.com/teams/GC 2. At the top right part of the website, you will find links to checking the status of the service requests.

ACCEPTANCE CERTIFICATE FORM

Agreement #:

Department:	WO/SOS number:
WO/SOS Date From:	WO/SOS Date To:
Service Description:	
Service Description:	
Services Resource Name:	Date:
Service Status:	
Service Status:	
Services Resource Name:	Date:
Service Attestation of Completion:	
Service Attestation of Completion	Date:
Services Manager Name:	Services Manager Signature:
Email:	Phone #:
Services Manager Comments:	
Certificate of Acceptance of Work	
County Project Manager Certification:	Date:
Name:	Signature:
Email:	Phone #:
Project Manager Comments:	

Copy to County Program Manager, INTERNAL SERVICES DEPARTMENT



Microsoft Enterprise Services Work Order (UNIFIED SERVICES)

Work Order Number

This Work Order consists of the terms and conditions below, and the provisions of the reference **insert reference**, effective as of **insert date** to **insert date** (the "Agreement") and shall expire (X months) following the Commencement Date (the Support Expiration Date). This Work Order may be amended and the Period of Performance extended prior to the Support Expiration Date. The provisions of the Support Services Description applicable to the Support Services identified in this Work Order, and any attachments or exhibits referenced in this Work Order, all of which are incorporated herein by this reference. In this Work Order "Customer," "you," or "your" means the undersigned customer or its affiliate and "Microsoft", "we," "us," or "our" means the undersigned Microsoft affiliate.

By signing below the parties acknowledge and agree to be bound to the terms of this Work Order, the Agreement and all other provisions incorporated in them. Regardless of any terms and conditions contained in a purchase order, if any, the terms of this Work Order apply.

County Program Director	Microsoft Affiliate
Name of County Program Director (Customer) (please print)	Name
Signature	Signature
Name of person signing (please print)	Name of person signing (please print)
Title of person signing (please print)	Title of person signing (please print)
Signature date	Signature date (effective date)
County Project Manager:	

Department Customer invoice information		
Name of Department		Contact name (Receives invoices under this Work Order)
Street address		Contact e-mail address
City	State/Province	Phone
Country	Postal code	Fax

1. Support Services and Fees

1.1. Term.

Microsoft Enterprise Support Services shall be effective and will commence on **insert date** or the last above Signature Date, whichever is later (the "Support Commencement Date") and shall expire twelve (12) months following the Support Commencement Date (the "Support Expiration Date"). This Work Order may be amended and the Period of Performance extended prior to the Support Expiration Date. In order for Microsoft to continue performing Services after the Support Expiration Date of this Work Order, Customer and Microsoft shall agree in writing to a new Work Order identifying the new terms upon which Customer and Microsoft agree.

1.2. Description of the Services.

Please refer to the current Support Services Description ("SSD") which will be incorporated by reference and is published by Microsoft from time to time at <http://www.microsoft.com/en-us/microsoftservices/PubSec-support-services-description>. The support services you purchase under this agreement may be updated from time to time and that update will supersede any services previously listed. Services shall be as described in Exhibit A-1 to the Contract.

Services by Support Location

Microsoft Support Services for XXXXXX	Location/Dept.	DATES
Quantity	Service	Service Type and Description

1.3. Support Services Fees.

The items listed in the table above represent the services that Customer has pre-purchased for use during the term of this Work Order, and applicable fees are shown in the table below. Microsoft Support Services are a non-refundable prepaid service. Microsoft must receive Customer purchase order or payment before Microsoft commences or continues, as applicable, provision of Microsoft Support Services. If Customer issues a purchase order, Microsoft will invoice Customer, and Customer agrees to pay Microsoft within 30 calendar days of the date of Microsoft invoice. Microsoft reserves the right to adjust Microsoft fees prior to entering into any changes to the Microsoft Support Services ordered herein.

Services Summary	Billing Date	Fee
Support Location 1		
Total Fees (excluding taxes)		

Support for Microsoft Products

Microsoft will provide support for Customer's licensed, commercially released and generally available Microsoft products, and cloud services subscriptions by Customer in Appendix A.

1.4. Customer Named Contacts.

Any changes to the named contacts should be submitted to Microsoft Contact.

Name of Customer Support Manager (CSM)
--

Street Address		Contact e-mail address
City	State/Province	Phone
Country	Postal code	Fax

Attachments

The following documents are attached at the execution of this Work Order:

- ☐ Exhibit: reference exhibits
- ☐ Other: reference document

Microsoft Contact

Customer contact for questions and notices about this Work Order.

Microsoft contact name	
Phone	Contact e-mail address

Appendix A

Below is a list of your declared licensed products and cloud services for which Microsoft will provide support services as defined within this document.

Customer Name	Licensing Program	Licensing Enrollment/Agreement Number	Product Family	Number of Licenses

FORM OF**Microsoft Consulting Services (MCS) Statement of Services (SOS)****for****[Insert Name of County Department]**

This Microsoft Consulting Services (MCS) Statement of Services (SOS) is made pursuant to the County of Los Angeles Contract for Microsoft Unified Support Services ("Contract"), number _____, effective on _____, by and between the County of Los Angeles ("County") and Microsoft Corporation ("Contractor") and is incorporated therein. Capitalized terms not otherwise defined have the meanings provided in the Contract.

1. Term. The term of this SOS will be (X) months, commencing on _____ and expiring on _____ ("Standard Period of Performance")
2. Services and Fees.
3. Services shall be as described in Exhibit A-2 to the Contract

OPTION SELECTED	QUANTITY
<u>Digital Advisory Services (DAS)</u>	
<u>Information Technology Strategic Architecture and Planning</u>	
<u>Architecture Transformation</u>	
<u>Platform Rationalization</u>	
<u>Microsoft IT Strategy Roadmap and Enterprise Architecture</u>	
<u>IT and Capabilities Map</u>	
<u>Enterprise Architecture Plan</u>	
<u>Architecting and Deploying Core Infrastructure and Cloud Technologies</u>	
<u>Application Development Project Services</u>	
<u>Collaboration Design and Deployment Services</u>	
<u>Cyber Security Services from Microsoft Corporation</u>	
<u>Dynamics 365 Suite Design and Deployment Services</u>	
<u>Industry Specific and Custom Services</u>	

Total Due From County Department (including cost breakdown):	\$

3. Provisions unchanged All provisions of the Contract shall remain unchanged and in full force and effect.

Services are deemed Accepted upon delivery.

SOS #.: _ _ _ - _ _ _

The signature below certifies that the County Project Manager has complied with the requirements of Exhibit C. The signature by the County Project Manager on this SOS shall not serve in any manner to obligate the County of Los Angeles to any expenditure of funds. Only the signature by the County Program Director on this SOS, in conjunction with the corresponding signature by Contractor, shall obligate the County of Los Angeles to the expenditure of funds.

LOS ANGELES COUNTY DEPARTMENT PROJECT MANAGER
By:
Signature
Name (Print)
Title
Date

MICROSOFT CORPORATION	LOS ANGELES COUNTY PROGRAM DIRECTOR
By:	By:
Signature	Signature
Name (Print) David Gallagher	Name (Print)
Title Public Sector Contracts Director	Title
Date Executed:	Date Executed:

The services listed in this SOS will be invoiced by Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, in accordance with the applicable payment terms of the Contract, including the County authorization and approval provisions, upon receipt of this fully executed SOS. All invoices must include the established SOS Number, "SOS #" reflected on this executed document and all other information required under the terms of the Contract.

LA County Agency Billing Contact

Billing Contact (if other than Project Director)
Name:
Address:
Phone: ()
Email:
Facsimile: ()

Unified Customer Named Contacts: Any subsequent changes to the Named Contacts should be submitted to the Services Resource CSM.

CSM Name:	Named Contact Name:
Address:	Address:
_____	_____
_____	_____
_____	_____
Phone: ()	Phone: ()
Email:	Email:
Facsimile: ()	Facsimile: ()

Named Contact Name:	Named Contact Name:
Address:	Address:
_____	_____
_____	_____
_____	_____
Phone: ()	Phone: ()
Email:	Email:
Facsimile: ()	Facsimile: ()

MICROSOFT PERSONNEL

CONTRACTOR ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENTCONTRACTOR NAME: MICROSOFT CORPORATION Contract No. _____**GENERAL INFORMATION:**

The Contractor referenced above has entered into a contract with the County of Los Angeles to provide certain services to the County. The County requires the Corporation to sign this Contractor Acknowledgement and Confidentiality Agreement for itself and on behalf and each of its agents and employees performing services under the contract.

CONTRACTOR ACKNOWLEDGEMENT:

Contractor understands and agrees that the Contractor employees, consultants, Outsourced Vendors and independent contractors (Contractor's Staff) that will provide services in the above referenced agreement are Contractor's sole responsibility. Contractor understands and agrees that Contractor's Staff must rely exclusively upon Contractor for payment of salary and any and all other benefits payable by virtue of Contractor's Staff's performance of work under the above-referenced contract.

Contractor understands and agrees that Contractor's Staff are not employees of the County of Los Angeles for any purpose whatsoever and that Contractor's Staff do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of their performance of work under the above-referenced contract. Contractor understands and agrees that Contractor's Staff will not acquire any rights or benefits from the County of Los Angeles pursuant to this agreement.

CONFIDENTIALITY AGREEMENT:

Contractor and Contractor's Staff may be involved with work pertaining to services provided by the County of Los Angeles and, if so, Contractor and Contractor's Staff may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, Contractor and Contractor's Staff may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. Contractor and Contractor's Staff understand that if they are involved in County work, the County must ensure that Contractor and Contractor's Staff, will protect the confidentiality of such data and information. Consequently, Contractor must sign this Confidentiality Agreement as a condition of work to be provided by Contractor's Staff for the County.

Contractor and Contractor's Staff hereby agree that they will not divulge to any unauthorized person any of the aforementioned data or information obtained while performing work pursuant to the above-referenced contract between Contractor and the County of Los Angeles. Contractor and Contractor's Staff agree to forward all requests for the release of any such data or information received to County Project Manager and the County Program Manager.

Contractor and Contractor's Staff agree to keep confidential all County Confidential Information (as defined in the Contract), health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County. Contractor and Contractor's Staff agree to protect these confidential materials against disclosure to other than Contractor or County employees who have a need to know the information. Contractor and Contractor's Staff agree that if proprietary information supplied by other County vendors is provided to me during the performance of this contract, Contractor and Contractor's Staff shall keep such information confidential.

Contractor and Contractor's Staff agree to report any and all violations of this agreement by Contractor and Contractor's Staff and/or by any other person of whom Contractor and Contractor's Staff become aware.

Contractor and Contractor's Staff acknowledge that violation of this agreement may subject Contractor and Contractor's Staff to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

SIGNATURE: _____

DATE: ____/____/____

PRINTED NAME: _____

POSITION: _____



Project Name/Description
Status Summary
1st Feb – 28th Feb 2022

Overall Health of Execution					
Project Start	Targeted End	Schedule	Cost	Benefit	Overall
3/22/2021	6/30/2022	G	G	G	G

Workstream Lead(s): *List Consultant Name(s) as applicable*

Work Stream	Summary of Tasks Completed this Period	Summary of Upcoming Tasks and Key Dates	Key Risks, Issues, Decisions, Dependency
Describe key activity / scope / milestone item	List completed activities for the current status period	List upcoming tasks and estimated dates of completion	List key risks, decisions, dependencies as applicable
Continue this table as needed			



O365 Collaboration- Technical Assistance

Status Summary

1st Feb – 28th Feb 2022

EXHIBIT A-8

Overall Health of Execution					
Project Start	Targeted End	Schedule	Cost	Benefit	Overall
3/22/2021	6/30/2022	G	G	G	G

Workstream Lead(s):

Hours consumed during Reporting period – *For Time & Materials Projects*

Role	Name	Planned Hours	Hours worked this reporting period	Total Hours worked till date	Hours Remaining
Senior Consultant	<Resource Name>	Complete table per headings above			
Senior Consultant	<Resource Name>				
Project Manager	<Resource Name>				
Account Delivery Executive	<Resource Name>				

Vacation Plan

List planned time out of office for key project resources





O365 Collaboration- Technical Assistance

Status Summary
1st Feb – 28th Feb 2022

Overall Health of Execution					
Project Start	Targeted End	Schedule	Cost	Benefit	Overall
3/22/2021	6/30/2022	G	G	G	G

Workstream Lead(s):

Milestone Status – For Fixed Fee/Priced Projects

Milestone / Deliverable	Description	Status	Estimated Completion Date	Completion Date	Deliverable Acceptance Received
<Milestone 1>	<Description>	Complete table per headings above			
<Milestone 2>	<Description>				

Vacation Plan

List planned time out of office for key project resources

PRICE LISTS

B-1 Microsoft Unified Support Published Price List

B-2 Microsoft Consulting Services Published Price List



US Public Sector Unified Support Published Price List

Effective: July 26, 2021

Unified Support Base ("Foundational") Pricing	Enterprise Support
Server Products	10% for the first \$0 to \$1.5M 9% from \$1.5M to \$3M 8% from \$3M to \$6M 7% from \$6M to \$15M 6% over \$15M
User Products	8% for first \$0 to \$1.5M 7% from \$1.5M to \$3M 6% from \$3M to \$6M 5% from \$6M to \$15M 4% over \$15M
Azure 12-month Historic Spend	10% for the first \$0 to \$1.8M 7.00% from \$1.8M to \$6M 5.00% from \$6M to \$12M 3.00% from \$12M to \$30M 2.25% from \$30M to \$60M 2.00% from \$60M to \$120M 1.75% from \$120M and up
Minimum Unified Support Contract Price	\$50,000
Unified Support Add On Pricing	
Proactive Credits	\$130.96 per Credit (includes Extended Service Delivery Management)
Extended Service Delivery Management	\$258 Per Hour
Designated Support Engineer	\$304 Per Hour with 200 Hour Minimum* (base support required)
Designated Support Engineer - Office 365 Pod	\$304 Per Hour with 600 Hour Minimum (base support required)
Designated Support Engineer - M365 Pod	\$304 Per Hour with 1,200 Hour Minimum (base support required)
Application Development Manager	\$294 Per Hour with 200 Hour Minimum (base support required)
Onsite Resource Visits	Negotiated Fixed Fee Per Contract
Support for Mission Critical	Custom scoped and priced support with a \$350,000 entry point
Azure Rapid Response	Custom scoped and priced support with a \$75,000 entry point up to 2.5M annually
Azure Event Management	Custom scoped and priced support with a \$10,000 entry point for a single engagement
Office 365 Engineering Direct	10% of Office 365 licensing spend with a minimum of \$200,000 entry <u>point</u> **

*200 hour minimum is specific to LA County as DSE resources are "shared" across departments; 400 hour minimum is standard non-negotiated requirement.

**Minimum requirement of 20,000 or more Office 365 seats.

1.0 **Microsoft Services Background**

Microsoft Consulting Services (MCS) helps customers achieve value from digital transformation at scale. MCS has been an integral part of Microsoft since 1990, helping thousands of customers worldwide build and implement information technology solutions, while empowering every customer to achieve more using Microsoft's latest products, services and technologies to drive Digital Transformation. MCS Practices are located at Microsoft field offices around the world.

1.1 **U. S. SLGE Services Mission**

Our mission is to serve as Trusted Technical Advisors and Architects to Microsoft's State and Local Government / Educational Institution Customers and Partners, helping them architect, plan, design and implement solutions leveraging Microsoft products, tools and technologies. MCS Consultants work with customers on specific projects and strategic initiatives and enable customers to gain knowledge in Microsoft product sets and methodologies to build self-sufficiency over time. MCS is the appropriate Microsoft resource to utilize when customer project requirements demand direct Microsoft involvement.

1.2 **Microsoft Services Rates**

<u>MCS LABOR CATEGORIES</u>	<u>Hourly Rates</u>
DELIVERY DATA SCIENTIST	\$330.00
DIGITAL ARCHITECT	\$330.00
SOLUTION ARCHITECT	\$330.00
SOFTWARE ENGINEER	\$330.00
PRINCIPAL CONSULTANT	\$320.00
SENIOR CONSULTANT	\$305.00
CONSULTANT	\$270.00
ASSOCIATE CONSULTANT	\$240.00
ACCOUNT DELIVERY EXECUTIVE	\$290.00
SENIOR PROJECT MANAGER	\$305.00
PROJECT MANAGER	\$290.00

MCS PARTNER-SUBCON RATES:	
	Hourly Rates
TECHNICIAN V	\$275.00
TECHNICIAN IV	\$260.00
TECHNICIAN III	\$230.00
TECHNICIAN II	\$205.00
TECHNICIAN I	\$175.00
TECHNICIAN	\$145.00
ASSOCIATE TECHNICIAN	\$115.00
GITHUB LABOR CATEGORIES:	
SERVICES DELIVERY	\$330.00
PROJ MANAGEMENT OFFICE	\$290.00
US DELIVERY CENTER, "USDC" (REMOTE SERVICES - LAS COLINAS, TX)	
USDC SENIOR CONSULTANT	\$230.00
USDC CONSULTANT	\$190.00
USDC SENIOR PROJECT MANAGER	\$230.00
USDC PROJECT MANAGER	\$190.00

Microsoft Global Delivery (GD)
Offshore Rates

- MSFT GD Consulting – (FTE) \$85.00/Hr.

Onshore Rates:

- MSFT GD Consulting – (FTE) \$230.00/Hr.
 - Daily per diem and other travel is charged IAW government travel regulations.
 - Note: Initial air fare to/from India is not charged to customer.

Note:

- *The labor category from which personnel will be assigned will be specified by Microsoft in a Work Order based on the nature of the services to be provided.*
- *Microsoft may revise the rates as per the Microsoft Unified Support and Consulting Support Services Contract.*

COUNTY'S WORK ORDER/STATEMENT OF SERVICES PROCESSES

COUNTY'S WORK ORDER/STATEMENT OF SERVICES PROCESS

WO/SOS Issuance Processes:

- A. Contractor shall, at no cost to the County, work closely with ISD and each participating County Department to right-size and customize the proposed Work Order (WO) and/or Statement of Service (SOS) so that it will be most appropriate for that County Department. The proposed WO and/or SOS shall be executed by the County Program Director and authorized officials of Contractor.
- B. County Department(s) shall submit a proposed Service Request using ISD's Contract SR Tool site described in Exhibit A-4, with a Work Order draft to County's Program Manager for approval, using the sample WO and/or SOS set forth in Exhibit A-6 or A-7 for Contractor Unified Product Support or Consulting Services. The proposed WO and/or SOS may only be for Services which are listed in Exhibit A-1 and A-2 ("Microsoft Unified Product Support and Microsoft Consulting Support Descriptions").
- C. ISD County Project Manager will first review the draft ISD WO and/or SOS, which it shall submit to the County Program Manager for review to best fulfill the needs. County will contact Contractor to review the required services and WO and/or SOS draft. Contractor shall not be authorized to begin work under an ISD WO and/or SOS and County shall not be obligated to pay Contractor for any work done under a WO unless and until County Program Director has approved the WO and it has been issued to and executed by Contractor's Contract Manager.
- D. Prior to submitting the proposed WO and/or SOS to County's Program Manager for final review, the County's Project Manager for the WO and/or SOS shall establish that sufficient funding for the WO and/or SOS has been secured by the applicable County Department.
- E. County Program Director may approve and execute the proposed WO and/or SOS, and issue it to Contractor.
- F. No additional payments shall be made by County associated with travel, meals, expenses, incidentals, or any other costs not explicitly defined in Exhibit B-1 or B-2 ("Price List") and stated in the respective WO and/or SOS.
- G. Under Subparagraph 8.1.5 (WO and/or SOS Amendments) of the Contract, County shall have the right to acquire supplemental Services including additional TAM Hours as well as those provided by Dedicated Support Engineers and Application Development Consultants. The Standard Period of Performance for the supplemental services shall be the same as under the initial WO and/or SOS.

- H. Under Subparagraph 8.1.5 (WO and/or SOS Amendments) of the Contract, County shall have the right to acquire additional Technical Account Hours in any increment during the Standard Period of Performance of an existing WO and/or SOS.
- I. Under Subsection 8.1.4 (WO and/or SOS Amendments) of the Contract, County shall have the right to acquire additional Problem Resolution Hours with a minimum of 25 hours during the Standard Period of Performance (12 months). Each break/fix incident typically averages 5-7 hours.
- J. At least 90 days prior to the end of the Standard Period of Performance of each WO and/or SOS, Contractor shall assess the usage under that WO and/or SOS, recommend in writing options for complete use of the remaining pre-purchased Services, and propose a WO and/or SOS for the following year that considers past and projected usage by that County Department. Through quarterly meetings with each County Department, Contractor will conduct these activities for the County Department, as part of their account management role.
- K. Under Subsection 8.1.5 (WO and/or SOS Amendments) of the Contract, County shall have the right to convert any unused services in any WO and/or SOS on a dollar for dollar value basis to any other services described in Exhibit A-1 and A-2 at the rates set forth in Exhibit B at any time during the Standard Period of Performance of any WO and/or SOS.
- L. Any Services that have not been used or delivered during the Standard Period of Performance, may be granted a 30-day extension ("Extended Delivery Period") to allow the use of such Services. This Extended Delivery Period requires the prior written approval of the County Program Manager and Contractor's Support Practice Manager. County Project Managers, as identified in the applicable Statement of Services, shall provide sufficient notice to the County Program Manager identifying the Service(s) that are at risk of not be provided prior to the expiration date of the WO and/or SOS, and shall work with Contractor staff and the County Program Manager to effectuate such extension. Any Services not performed by the end of an Extended Delivery Period shall be forfeited.
- M. Services provided under a WO and/or SOS shall be charged by Contractor in the manner most cost-effective to the County and within Microsoft Unified Product Support programmatic rules.
- N. Each WO and/or SOS shall have a Standard Period of Performance that begins at the WO's/SOS's Effective Date and ends one year later or at the end of the term of this Contract, whichever comes first. Each WO and/or SOS shall also specifically state the type, level and quantity of Services to be provided and the maximum payment for the Services. The WO and/or SOS shall also state the expected Service level(s) and technical contacts information.
- O. Contractor and County shall schedule and hold quarterly meetings between Contractor's Support Practice Manager and Contractor's Services Account Executive, and other Microsoft personnel, as necessary or desired, and County's Program Manager, County's Project Manager(s), and other County management personnel, or as otherwise agreed upon by the parties, to review Contractor's performance hereunder, the status of each then current WO and/or SOS, to resolve any Services or billing problems, introduce new Services, and discuss any other issues, at no cost to County. Contractor and County shall arrange for the meeting

location, prepare the agenda for each meeting, and record and publish minutes and assignments to all the participants.

Problem Resolution Case Process:

- Problem Resolution Support (PRS) cases are opened by County personnel that have been authorized by the County and have a valid Access ID. County Departments may open a PRS case through the Premier Portal or by calling the Premier Support toll free number. A Contractor PRS ticket is then opened by Department. Access to PRS Cases is available on a 24 X 7 basis, 365 days per year. Lower severity cases are worked during standard business hours (6 AM to 6 PM PST).
- The County Department will establish the initial severity level of the PRS case. The severity classification of the case can be raised or lowered at the County's request. PRS cases are billed for the time actually worked by Contractor support engineers in 1 minute increments. There are cases where multiple engineers may be engaged with, and charging to, the same PRS case.
- For Reactive Support, the County's Service Level Agreements (SLAs) for each level of Services performed within the County Department's WO and/or SOS are described in the Exhibit A-1 (Unified Products Service Descriptions: Paragraph 2.2.1). For Proactive Support, dates are negotiated with such County Department.
- Any PRS Incident that involves Contractor accessing data within any County applications that maintain PHI data shall be submitted to the County Program Manager for approval prior to initiating the PRS Incident. Such PRS Incident may require the negotiation and execution of a Business Associate Agreement prior to commencement of any such Services.
- Normally PRS cases will remain open until the County Department has determined that the case should be closed and the Contractor PRS ticket is closed. Closed cases may be re-opened by the County Department for further support effort and additional time spent by Contractor's support engineers will be billed to the case.
- On a monthly basis (or more frequent if requested by the County Department) the Technical Account Manager (TAM) will review the open and closed PRS cases with the County Department. This review is intended to confirm that the open cases continue to be worked as appropriate and that closed cases have been properly billed. Billing occurs by Decrementing the WO and/or SOS hours purchased by the County Department executing the WO and/or SOS. The summary of these WO and/or SOS hours are detailed in the County Department's Customer Status Report.
- Any questions regarding billings to PRS cases should be raised with the TAM in writing.

Customer Status Report Process:

1. Contractor's Technical Account Manager (TAM) will meet monthly with each County Department that has an active WO and/or SOS to review the Department's Status Report. Contractor will conduct quarterly meetings to review all activity (Proactive projects, hours available etc.).
2. The Activity Report portion of the Customer Status Report details the Consumption Summary, Service Consumption Mix, and Service Consumption Trend review. It is in this area of the Customer Status Report where the contracted number of WO and/or SOS Technical Account Hours, Problem Resolution Hours and Support Assistance Hours are Decrementated by each Case to show a new total of Services for those areas that are left under this WO and/or SOS.
3. The Support Assistance (SA) portion of the Customer Status Report details SA Summary, SA by Technology, Cumulative SA Usage, and SA Details.
4. The Problem Resolution (PR) portion of the Customer Status Report details PR Hourly Summary, PR Cases by Type, Cumulative PR Hourly Usage, PR Cases by Technology & Severity, and PR Hourly Details.
5. The Activity portion of the Customer Status Report provides contact information versus Proactive/Reactive cases and labor.

Escalation Process:

Management Escalation Path

Customer Success Account Manager	Each Department has individual CSAM
Customer Success Account Manager Director	Kris Caceres: krisc@microsoft.com
Support Practice Manager	Kiersten Keester: kkeest@microsoft.com
General Manager, State & Local Government	Sarah Jackson: sajackson@microsoft.com

CONTRACTOR'S EEO CERTIFICATION

Microsoft Corporation

Contractor Name

One Microsoft Way, Redmond WA 98052

Address

91-1144442

Internal Revenue Service Employer Identification Number

GENERAL CERTIFICATION

In accordance with Section 4.32.010 of the Code of the County of Los Angeles, the contractor, supplier, or vendor certifies and agrees that all persons employed by such firm, its affiliates, subsidiaries, or holding companies are and will be treated equally by the firm without regard to or because of race, religion, ancestry, national origin, or sex and in compliance with all anti-discrimination laws of the United States of America and the State of California.

CONTRACTOR'S SPECIFIC CERTIFICATIONS

- | | | |
|--|---|-----------------------------|
| 1. The Contractor has a written policy statement prohibiting discrimination in all phases of employment. | Yes ☒ | No ☐ |
| 2. The Contractor periodically conducts a self analysis or utilization analysis of its work force. | Yes ☒ | No ☐ |
| 3. The Contractor has a system for determining if its employment practices are discriminatory against protected groups. | Yes ☒ | No ☐ |
| 4. Where problem areas are identified in employment practices, the Contractor has a system for taking reasonable corrective action, to include establishment of goals or timetables. | Yes ☒ | No ☐ |

Shelton Sunday, Principal Delivery Executive

Authorized Official's Printed Name and Title

Shelton Sunday

Authorized Official's Signature

Apr 28, 2022

Date

COUNTY'S ADMINISTRATION

CONTRACT NO. _____

COUNTY PROJECT DIRECTOR:

Name: _____

Title: _____

Address: _____

Telephone: _____ Facsimile: _____

E-Mail Address: _____

COUNTY PROGRAM MANAGER:

Name: _____

Title: _____

Address: _____

Telephone: _____ Facsimile: _____

E-Mail Address: _____

COUNTY PROJECT MANAGER:

Name: _____

Title: _____

Address: _____

Telephone: _____ Facsimile: _____

E-Mail Address: _____

CONTRACTOR'S ADMINISTRATION**CONTRACTOR'S NAME:** MICROSOFT CORPORATION**CONTRACT NO:** MICROSOFT UNIFIED SUPPORT AND CONSULTING SERVICES**CONTRACTOR'S PROJECT MANAGER:** _____

Name: Shelton Sunday
Title: Principal Delivery Executive
Address: 27316 Ardella Pl
SANTA CLARITA, CA 91350
Telephone: 213-806-7506
Facsimile: _____
E-Mail Address: sheltons@microsoft.com

CONTRACTOR'S AUTHORIZED OFFICIAL(S)

Name: For Microsoft Unified Service: **Steve Honn**
Title: Director of Support Sales – SLG & EDU
Address: 1 Redmond Way
Redmond, WA. 98052
Telephone: (425) 722-2556
Facsimile: _____
E-Mail Address: shonn@microsoft.com

Name: For Microsoft Consulting Services: **Shelton Sunday**
Title: Principal Delivery Executive
Address: 1 Redmond Way
Redmond, WA. 98052
Telephone: 213-806-7506
Facsimile: _____
E-Mail Address: sheltons@microsoft.com

Notices to Contractor shall be sent to the following:

Name: SHELTON SUNDAY
Title: PRINCIPAL DELIVERY EXECUTIVE
Address: 1 Redmond Way
Redmond, WA. 98052
Telephone: 213-806-7506
Facsimile: _____
E-Mail Address: lacountymrsa@microsoft.com

FORMS REQUIRED AT THE TIME OF CONTRACT EXECUTION

G COVID-19 VACCINATION CERTIFICATION OF COMPLIANCE

G1-IT CONTRACTOR ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT
ASSIGNMENT AGREEMENT

**Urgency Ordinance, County Code Title 2 – Administration, Division 4 – Miscellaneous –
Chapter 2.212 (COVID-19 Vaccinations of County Contractor Personnel)**

I, **Hollis Williams**, on behalf of **Microsoft Corporation**, (the "Contractor"), certify that on County Contract **MICROSOFT UNIFIED SUPPORT AND CONSULTING SERVICES**:

 X All Contractor Personnel* on this Contract are fully vaccinated as required by the Ordinance.

 Most Contractor Personnel* on this Contract are fully vaccinated as required by the Ordinance. The Contractor or its employer of record, has granted a valid medical or religious exemption to the below identified Contractor Personnel. Contractor will certify weekly that the following unvaccinated Contractor Personnel have tested negative within 72 hours of starting their work week under the County Contract, unless the contracting County department requires otherwise. The Contractor Personnel who have been granted a valid medical or religious exemption are [LIST ALL CONTRACTOR PERSONNEL]:

*Contractor Personnel includes subcontractors.

I have authority to bind the Contractor and have reviewed the requirements above and further certify that I will comply with said requirements.


Hollis Williams (Apr 28, 2022 23:08 EDT)

Signature

Apr 28, 2022

Date

Chief Operating Officer - State and Local Government

Title

Microsoft
Company/Contractor Name

Released December 14, 2021

Version 2.0

**G1-IT CONTRACTOR ACKNOWLEDGEMENT, CONFIDENTIALITY, AND
COPYRIGHT ASSIGNMENT AGREEMENT**

CONTRACTOR ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

Page 1 of 2

(Note: This certification is to be executed and returned to County with Contractor's executed Contract. Work cannot begin on the Contract until County receives this executed document.)

CONTRACTOR NAME _____ Contract No. _____

GENERAL INFORMATION:

The Contractor referenced above has entered into a contract with the County of Los Angeles to provide certain services to the County. The County requires the Corporation to sign this Contractor Acknowledgement and Confidentiality Agreement.

CONTRACTOR ACKNOWLEDGEMENT:

Contractor understands and agrees that the Contractor employees, consultants, Outsourced Vendors and independent contractors (Contractor's Staff) that will provide services in the above referenced agreement are Contractor's sole responsibility. Contractor understands and agrees that Contractor's Staff must rely exclusively upon Contractor for payment of salary and any and all other benefits payable by virtue of Contractor's Staff's performance of work under the above-referenced contract.

Contractor understands and agrees that Contractor's Staff are not employees of the County of Los Angeles for any purpose whatsoever and that Contractor's Staff do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. Contractor understands and agrees that Contractor's Staff will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

CONFIDENTIALITY AGREEMENT:

Contractor and Contractor's Staff may be involved with work pertaining to services provided by the County of Los Angeles and, if so, Contractor and Contractor's Staff may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, Contractor and Contractor's Staff may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. Contractor and Contractor's Staff understand that if they are involved in County work, the County must ensure that Contractor and Contractor's Staff, will protect the confidentiality of such data and information. Consequently, Contractor must sign this Confidentiality Agreement as a condition of work to be provided by Contractor's Staff for the County.

Contractor and Contractor's Staff hereby agrees that they will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced contract between Contractor and the County of Los Angeles. Contractor and Contractor's Staff agree to forward all requests for the release of any data or information received to County's Project Manager.

Contractor and Contractor's Staff agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information and all other

CONTRACTOR ACKNOWLEDGEMENT AND CONFIDENTIALITY AGREEMENT

Page 2 of 2

original materials produced, created, or provided to Contractor and Contractor's Staff under the above-referenced contract. Contractor and Contractor's Staff agree to protect these confidential materials against disclosure to other than Contractor or County employees who have a need to know the information. Contractor and Contractor's Staff agree that if proprietary information supplied by other County vendors is provided to me during this employment, Contractor and Contractor's Staff shall keep such information confidential.

Contractor and Contractor's Staff agree to report any and all violations of this agreement by Contractor and Contractor's Staff and/or by any other person of whom Contractor and Contractor's Staff become aware.

Contractor and Contractor's Staff acknowledge that violation of this agreement may subject Contractor and Contractor's Staff to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

Contractor and Contractor's Staff acknowledge that violation of this agreement may subject them to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

SIGNATURE: _____

DATE: ____/____/____

PRINTED NAME: _____

POSITION: _____

CONTRACTOR EMPLOYEE JURY SERVICE

Title 2 ADMINISTRATION
Chapter 2.203.010 through 2.203.090
CONTRACTOR EMPLOYEE JURY SERVICE

2.203.010 Findings.

The board of supervisors makes the following findings. The county of Los Angeles allows its permanent, full-time employees unlimited jury service at their regular pay. Unfortunately, many businesses do not offer or are reducing or even eliminating compensation to employees who serve on juries. This creates a potential financial hardship for employees who do not receive their pay when called to jury service, and those employees often seek to be excused from having to serve. Although changes in the court rules make it more difficult to excuse a potential juror on grounds of financial hardship, potential jurors continue to be excused on this basis, especially from longer trials. This reduces the number of potential jurors and increases the burden on those employers, such as the county of Los Angeles, who pay their permanent, full-time employees while on juror duty. For these reasons, the county of Los Angeles has determined that it is appropriate to require that the businesses with which the county contracts possess reasonable jury service policies. (Ord. 2002-0015 § 1 (part), 2002)

2.203.020 Definitions.

The following definitions shall be applicable to this chapter:

- A. “Contractor” means a person, partnership, corporation or other entity which has a contract with the county or a subcontract with a county contractor and has received or will receive an aggregate sum of \$50,000 or more in any 12-month period under one or more such contracts or subcontracts.
- B. “Employee” means any California resident who is a full-time employee of a contractor under the laws of California.
- C. “Contract” means any agreement to provide goods to, or perform services for or on behalf of, the county but does not include:
 - 1. A contract where the board finds that special circumstances exist that justify a waiver of the requirements of this chapter; or
 - 2. A contract where federal or state law or a condition of a federal or state program mandates the use of a particular contractor; or
 - 3. A purchase made through a state or federal contract; or
 - 4. A monopoly purchase that is exclusive and proprietary to a specific manufacturer, distributor, or reseller, and must match and inter-member with existing supplies, equipment or systems maintained by the county pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section P-3700 or a successor provision; or
 - 5. A revolving fund (petty cash) purchase pursuant to the Los Angeles County Fiscal Manual, Section 4.4.0 or a successor provision; or
 - 6. A purchase card purchase pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section P-2810 or a successor provision; or
 - 7. A non-agreement purchase with a value of less than \$5,000 pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section A-0300 or a successor provision; or

Title 2 ADMINISTRATION
Chapter 2.203.010 through 2.203.090
CONTRACTOR EMPLOYEE JURY SERVICE

8. A bona fide emergency purchase pursuant to the Los Angeles County Purchasing Policy and Procedures Manual, Section PP-1100 or a successor provision.

Page 2 of 3

- D. "Full time" means 40 hours or more worked per week, or a lesser number of hours if:
 1. The lesser number is a recognized industry standard as determined by the chief administrative officer, or
 2. The contractor has a long-standing practice that defines the lesser number of hours as full time.
- E. "County" means the county of Los Angeles or any public entities for which the board of supervisors is the governing body. (Ord. 2002-0040 § 1, 2002: Ord. 2002-0015 § 1 (part), 2002)

2.203.030 Applicability.

This chapter shall apply to contractors who enter into contracts that commence after July 11, 2002. This chapter shall also apply to contractors with existing contracts which are extended into option years that commence after July 11, 2002. Contracts that commence after May 28, 2002, but before July 11, 2002, shall be subject to the provisions of this chapter only if the solicitations for such contracts stated that the chapter would be applicable. (Ord. 2002-0040 § 2, 2002: Ord. 2002-0015 § 1 (part), 2002)

2.203.040 Contractor Jury Service Policy.

A contractor shall have and adhere to a written policy that provides that its employees shall receive from the contractor, on an annual basis, no less than five days of regular pay for actual jury service. The policy may provide that employees deposit any fees received for such jury service with the contractor or that the contractor deduct from the employees' regular pay the fees received for jury service. (Ord. 2002-0015 § 1 (part), 2002)

2.203.050 Other Provisions.

- A. Administration. The chief administrative officer shall be responsible for the administration of this chapter. The chief administrative officer may, with the advice of county counsel, issue interpretations of the provisions of this chapter and shall issue written instructions on the implementation and ongoing administration of this chapter. Such instructions may provide for the delegation of functions to other county departments.
- B. Compliance Certification. At the time of seeking a contract, a contractor shall certify to the county that it has and adheres to a policy consistent with this chapter or will have and adhere to such a policy prior to award of the contract. (Ord. 2002-0015 § 1 (part), 2002)

2.203.060 Enforcement and Remedies.

For a contractor's violation of any provision of this chapter, the county department head responsible for administering the contract may do one or more of the following:

1. Recommend to the board of supervisors the termination of the contract; and/or,
2. Pursuant to chapter 2.202, seek the debarment of the contractor. (Ord. 2002-0015 § 1 (part), 2002)

Title 2 ADMINISTRATION
Chapter 2.203.010 through 2.203.090
CONTRACTOR EMPLOYEE JURY SERVICE

Page 3 of 3

2.203.070. Exceptions.

- A. Other Laws. This chapter shall not be interpreted or applied to any contractor or to any employee in a manner inconsistent with the laws of the United States or California.
- B. Collective Bargaining Agreements. This chapter shall be superseded by a collective bargaining agreement that expressly so provides.
- C. Small Business. This chapter shall not be applied to any contractor that meets all of the following:
 - 1. Has ten or fewer employees during the contract period; and,
 - 2. Has annual gross revenues in the preceding twelve months which, if added to the annual amount of the contract awarded, are less than \$500,000; and,
 - 3. Is not an affiliate or subsidiary of a business dominant in its field of operation.

“Dominant in its field of operation” means having more than ten employees and annual gross revenues in the preceding twelve months which, if added to the annual amount of the contract awarded, exceed \$500,000.

“Affiliate or subsidiary of a business dominant in its field of operation” means a business which is at least 20 percent owned by a business dominant in its field of operation, or by partners, officers, directors, majority stockholders, or their equivalent, of a business dominant in that field of operation. (Ord. 2002-0015 § 1 (part), 2002)

2.203.090. Severability.

If any provision of this chapter is found invalid by a court of competent jurisdiction, the remaining provisions shall remain in full force and effect. (Ord. 2002-0015 § 1 (part), 2002)

SAFELY SURRENDERED BABY LAW

Safely Surrendered



No shame. No blame. No names.

In Los Angeles County: 1-877-BABY SAFE • 1-877-222-9723

www.babysafela.org



In Los Angeles County: 1-877-BABY SAFE • 1-877-222-9723

www.babysafela.org

Safely Surrendered Baby Law

What is the Safely Surrendered Baby Law?

California's Safely Surrendered Baby Law allows parents or other persons, with lawful custody, which means anyone to whom the parent has given permission to confidentially surrender a baby. As long as the baby is three days (72 hours) of age or younger and has not been abused or neglected, the baby may be surrendered without fear of arrest or prosecution.

Every baby deserves a chance for a healthy life. If someone you know is considering abandoning a baby, let her know there are other options. For three days (72 hours) after birth, a baby can be surrendered to staff at any hospital or fire station in Los Angeles County.

How does it work?

A distressed parent who is unable or unwilling to care for a baby can legally, confidentially, and safely surrender a baby within three days (72 hours) of birth. The baby must be handed to an employee at a hospital or fire station in Los Angeles County. As long as the baby shows no sign of abuse or neglect, no name or other information is required. In case the parent changes his or her mind at a later date and wants the baby back, staff will use bracelets to help connect them to each other. One bracelet will be placed on the baby, and a matching bracelet will be given to the parent or other surrendering adult.

What if a parent wants the baby back?

Parents who change their minds can begin the process of reclaiming their baby within 14 days. These parents should call the Los Angeles County Department of Children and Family Services at 1-800-540-4000.

Can only a parent bring in the baby?

No. While in most cases a parent will bring in the baby, the Law allows other people to bring in the baby if they have lawful custody.

Does the parent or surrendering adult have to call before bringing in the baby?

No. A parent or surrendering adult can bring in a baby anytime, 24 hours a day, 7 days a week, as long as the parent or surrendering adult surrenders the baby to someone who works at the hospital or fire station.

Does the parent or surrendering adult have to tell anything to the people taking the baby?

No. However, hospital or fire station personnel will ask the surrendering party to fill out a questionnaire designed to gather important medical history information, which is very useful in caring for the baby. The questionnaire includes a stamped return envelope and can be sent in at a later time.

What happens to the baby?

The baby will be examined and given medical treatment. Upon release from the hospital, social workers immediately place the baby in a safe and loving home and begin the adoption process.

What happens to the parent or surrendering adult?

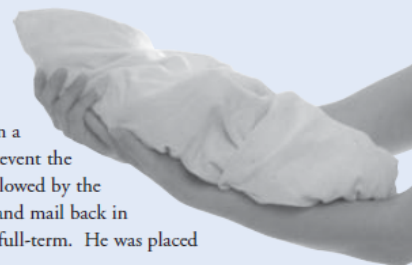
Once the parent or surrendering adult surrenders the baby to hospital or fire station personnel, they may leave at any time.

Why is California doing this?

The purpose of the Safely Surrendered Baby Law is to protect babies from being abandoned, hurt or killed by their parents. You may have heard tragic stories of babies left in dumpsters or public bathrooms. Their parents may have been under severe emotional distress. The mothers may have hidden their pregnancies, fearful of what would happen if their families found out. Because they were afraid and had no one or nowhere to turn for help, they abandoned their babies. Abandoning a baby is illegal and places the baby in extreme danger. Too often, it results in the baby's death. The Safely Surrendered Baby Law prevents this tragedy from ever happening again in California.

A baby's story

Early in the morning on April 9, 2005, a healthy baby boy was safely surrendered to nurses at Harbor-UCLA Medical Center. The woman who brought the baby to the hospital identified herself as the baby's aunt and stated the baby's mother had asked her to bring the baby to the hospital on her behalf. The aunt was given a bracelet with a number matching the anklet placed on the baby; this would provide some identification in the event the mother changed her mind about surrendering the baby and wished to reclaim the baby in the 14-day period allowed by the Law. The aunt was also provided with a medical questionnaire and said she would have the mother complete and mail back in the stamped return envelope provided. The baby was examined by medical staff and pronounced healthy and full-term. He was placed with a loving family that had been approved to adopt him by the Department of Children and Family Services.



Ley de Entrega de Bebés *Sin Peligro*



Los recién nacidos pueden ser entregados en forma segura al personal de cualquier hospital o cuartel de bomberos del Condado de Los Ángeles

Sin pena. Sin culpa. Sin nombres.

En el Condado de Los Ángeles: 1-877-BABY SAFE • 1-877-222-9723

www.babysafela.org



En el Condado de Los Ángeles: 1-877-BABY SAFE • 1-877-222-9723

www.babysafela.org

Ley de Entrega de Bebés Sin Peligro

¿Qué es la Ley de Entrega de Bebés sin Peligro?

La Ley de Entrega de Bebés sin Peligro de California permite la entrega confidencial de un recién nacido por parte de sus padres u otras personas con custodia legal, es decir cualquier persona a quien los padres le hayan dado permiso. Siempre que el bebé tenga tres días (72 horas) de vida o menos, y no haya sufrido abuso ni negligencia, pueden entregar al recién nacido sin temor de ser arrestados o procesados.

Cada recién nacido se merece la oportunidad de tener una vida saludable. Si alguien que usted conoce está pensando en abandonar a un recién nacido, infórmele que tiene otras opciones. Hasta tres días (72 horas) después del nacimiento, se puede entregar un recién nacido al personal de cualquier hospital o cuartel de bomberos del condado de Los Angeles.

¿Cómo funciona?

El padre/madre con dificultades que no pueda o no quiera cuidar de su recién nacido puede entregarlo en forma legal, confidencial y segura dentro de los tres días (72 horas) del nacimiento. El bebé debe ser entregado a un empleado de cualquier hospital o cuartel de bomberos del Condado de Los Ángeles. Siempre que el bebé no presente signos de abuso o negligencia, no será necesario suministrar nombres ni información alguna. Si el padre/madre cambia de opinión posteriormente y desea recuperar a su bebé, los trabajadores utilizarán brazaletes para poder vincularlos. El bebé llevará un brazaletes y el padre/madre o el adulto que lo entregue recibirá un brazaletes igual.

¿Qué pasa si el padre/madre desea recuperar a su bebé?

Los padres que cambien de opinión pueden comenzar el proceso de reclamar a su recién nacido dentro de los 14 días. Estos padres deberán llamar al Departamento de Servicios para Niños y Familias (Department of Children and Family Services) del Condado de Los Ángeles al 1-800-540-4000.

¿Sólo los padres podrán llevar al recién nacido?

No. Si bien en la mayoría de los casos son los padres los que llevan al bebé, la ley permite que otras personas lo hagan si tienen custodia legal.

¿Los padres o el adulto que entrega al bebé deben llamar antes de llevar al bebé?

No. El padre/madre o adulto puede llevar al bebé en cualquier momento, las 24 horas del día, los 7 días de la semana, siempre y cuando entreguen a su bebé a un empleado del hospital o cuartel de bomberos.

¿Es necesario que el padre/madre o adulto diga algo a las personas que reciben al bebé?

No. Sin embargo, el personal del hospital o cuartel de bomberos le pedirá a la persona que entregue al bebé que llene un cuestionario con la finalidad de recabar antecedentes médicos importantes, que resultan de gran utilidad para cuidar bien del bebé. El cuestionario incluye un sobre con el sello postal pagado para enviarlo en otro momento.

¿Qué pasará con el bebé?

El bebé será examinado y le brindarán atención médica. Cuando le den el alta del hospital, los trabajadores sociales inmediatamente ubicarán al bebé en un hogar seguro donde estará bien atendido, y se comenzará el proceso de adopción.

¿Qué pasará con el padre/madre o adulto que entregue al bebé?

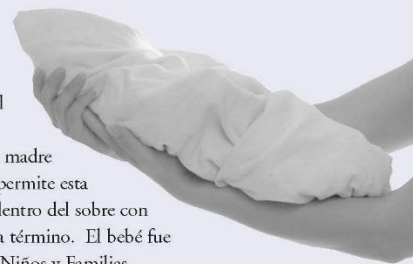
Una vez que los padres o adulto hayan entregado al bebé al personal del hospital o cuartel de bomberos, pueden irse en cualquier momento.

¿Por qué se está haciendo esto en California?

La finalidad de la Ley de Entrega de Bebés sin Peligro es proteger a los bebés para que no sean abandonados, lastimados o muertos por sus padres. Usted probablemente haya escuchado historias trágicas sobre bebés abandonados en basureros o en baños públicos. Los padres de esos bebés probablemente hayan estado pasando por dificultades emocionales graves. Las madres pueden haber ocultado su embarazo, por temor a lo que pasaría si sus familias se enteraran. Abandonaron a sus bebés porque tenían miedo y no tenían nadie a quien pedir ayuda. El abandono de un recién nacido es ilegal y pone al bebé en una situación de peligro extremo. Muy a menudo el abandono provoca la muerte del bebé. La Ley de Entrega de Bebés sin Peligro impide que vuelva a suceder esta tragedia en California.

Historia de un bebé

A la mañana temprano del día 9 de abril de 2005, se entregó un recién nacido saludable a las enfermeras del Harbor-UCLA Medical Center. La mujer que llevó el recién nacido al hospital se dio a conocer como la tía del bebé, y dijo que la madre le había pedido que llevara al bebé al hospital en su nombre. Le entregaron a la tía un brazaletes con un número que coincidía con la pulsera del bebé; esto serviría como identificación en caso de que la madre cambiara de opinión con respecto a la entrega del bebé y decidiera recuperarlo dentro del período de 14 días que permite esta ley. También le dieron a la tía un cuestionario médico, y ella dijo que la madre lo llenaría y lo enviaría de vuelta dentro del sobre con franqueo pagado que le habían dado. El personal médico examinó al bebé y se determinó que estaba saludable y a término. El bebé fue ubicado con una buena familia que ya había sido aprobada para adoptarlo por el Departamento de Servicios para Niños y Familias.



INFORMATION SECURITY AND PRIVACY REQUIREMENTS

INFORMATION SECURITY AND PRIVACY REQUIREMENTS

The County of Los Angeles ("County") is committed to safeguarding the Integrity of the County systems, Data, Information and protecting the privacy rights of the individuals that it serves. The Microsoft Products and Services Data Protection Addendum (the "DPA") at Exhibit K sets forth the County and the Contractor's commitment and agreement to fulfill each of their obligations under applicable state or federal laws, rules, or regulations, as well as applicable industry standards concerning privacy, Data protections, Information Security, Confidentiality, Availability, and Integrity of such Information. The Information Security and privacy requirements and procedures in the DPA are to be established by the Contractor before the Effective Date of the Contract and maintained throughout the term of the Contract.

These requirements and procedures are a minimum standard and are in addition to the requirements of the underlying base agreement between the County and Contractor (the "Contract") and any other agreements between the parties. However, it is the Contractor's sole obligation to: (i) implement appropriate and reasonable measures to secure and protect its systems and all County Information against internal and external Threats and Risks; and (ii) continuously review and revise those measures to address ongoing Threats and Risks. Failure to comply with the minimum requirements and procedures set forth in this Exhibit J (Information Security and Privacy Requirements) and the DPA will constitute a material, non-curable breach of Contract by the Contractor, entitling the County, in addition to the cumulative of all other remedies available to it at law, in equity, or under the Contract, to immediately terminate the Contract as set forth in the Contract. To the extent there are conflicts between the DPA and the Contract, the DPA shall prevail unless stated otherwise.

For clarity, the terms below apply only to the processing of data in environments controlled by Microsoft and Microsoft's subprocessors. This includes data sent to Microsoft by Products and Services but does not include data that remains on County's premises or in any County selected third party operating environments. County is responsible for implementing and maintaining privacy protections and security measures for components County provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer's virtual machine or application).

1. DEFINITIONS

In addition to the defined terms in the Contract, including the DPA, the following defined terms apply to this Exhibit. Unless otherwise defined in the Contract, the definitions herein contained are specific to the uses within this exhibit.

- a. **Availability:** the condition of Information being accessible and usable upon demand by an authorized entity (Workforce Member or process).
- b. **Confidentiality:** the condition that Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the Information.
- c. **County Information:** all Data and Information belonging to the County.
- d. **Data:** a subset of Information comprised of qualitative or quantitative values.
- e. **Incident:** a suspected, attempted, successful, or imminent Threat of unauthorized electronic and/or physical access, use, disclosure, breach, modification, or destruction of information; interference with Information Technology operations; or significant violation of County policy.

- f. **Information:** any communication or representation of knowledge or understanding such as facts, Data, or opinions in any medium or form, including electronic, textual, numerical, graphic, cartographic, narrative, or audiovisual.
- g. **Information Security Policy:** high level statements of intention and direction of an organization used to create an organization's Information Security Program as formally expressed by its top management.
- h. **Information Security Program:** formalized and implemented Information Security Policies, standards and procedures that are documented describing the program management safeguards and common controls in place or those planned for meeting the County's information security requirements.
- i. **Information Technology:** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of Data or Information.
- j. **Integrity:** the condition whereby Data or Information has not been improperly modified or destroyed and authenticity of the Data or Information can be ensured.
- k. **Mobile Device Management (MDM):** software that allows Information Technology administrators to control, secure, and enforce policies on smartphones, tablets, and other endpoints.
- l. **Privacy Policy:** high level statements of intention and direction of an organization used to create an organization's Privacy Program as formally expressed by its top management.
- m. **Privacy Program:** A formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the organization's privacy official and other staff, the strategic goals and objectives of the Privacy Program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
- n. **Risk:** a measure of the extent to which the County is threatened by a potential circumstance or event, Risk is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
- o. **Threat:** any circumstance or event with the potential to adversely impact County operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an Information System via unauthorized access, destruction, disclosure, modification of Information, and/or denial of service.
- p. **Vulnerability:** a weakness in a system, application, network or process that is subject to exploitation or misuse.
- q. **Workforce Member:** employees, volunteers, and other persons whose conduct, in the performance of work for Los Angeles County, is under the direct control of Los Angeles County, whether or not they are paid by Los Angeles County. This includes, but may not be limited to, full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the County.

2. INFORMATION SECURITY AND PRIVACY PROGRAMS

- a. **Information Security Program.** As set forth in the DPA Contractor shall maintain a company-wide Information Security Program designed to evaluate Risks to the Confidentiality, Availability, and Integrity of the County Information covered under this Contract.

Contractor's Information Security Program shall include the creation and maintenance of Information Security Policies, standards, and procedures. Information Security Policies, standards, and procedures will be communicated to all Contractor employees in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure operational effectiveness, compliance with all applicable laws and regulations, and addresses new and emerging Threats and Risks.

The Contractor shall exercise the same degree of care in safeguarding and protecting County Information that the Contractor exercises with respect to its own Information and Data, but in no event less than a reasonable degree of care. The Contractor will implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the Confidentiality, Integrity, and Availability of County Information.

The Contractor's Information Security Program as set forth in the DPA shall:

- Protect the Confidentiality, Integrity, and Availability of County Information in the Contractor's possession or control;
- Protect against any anticipated Threats or hazards to the Confidentiality, Integrity, and Availability of County Information;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information;
- Protect against accidental loss or destruction of, or damage to, County Information; and
- Safeguard County Information in compliance with any applicable laws and regulations which apply to the Contractor.

- b. **Privacy Program.** As set forth in the DPA, the Contractor shall establish and maintain a company-wide Privacy Program designed to incorporate Privacy Policies and practices in its business operations to provide safeguards for Information, including County Information. The Contractor's Privacy Program shall include the development of, and ongoing reviews and updates to Privacy Policies, guidelines, procedures and appropriate workforce privacy training within its organization. These Privacy Policies, guidelines, procedures, and appropriate training will be provided to all Contractor employees, agents, and volunteers. The Contractor's Privacy Policies, guidelines, and procedures shall be continuously reviewed and updated for effectiveness and compliance with applicable laws and regulations, and to appropriately respond to new and emerging Threats and Risks. The Contractor's Privacy Program shall perform ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

The Contractor shall exercise the same degree of care in safeguarding the privacy of County Information that the Contractor exercises with respect to its own Information, but in no event less than a reasonable degree of care. The Contractor will implement, maintain, and use appropriate privacy practices and protocols to preserve the Confidentiality of County Information.

The Contractor's Privacy Program as set forth in the DPA shall include:

- A Privacy Program framework that identifies and ensures that the Contractor complies with all applicable laws and regulations;
- External Privacy Policies, and internal privacy policies, procedures and controls to support the privacy program;

- Protections against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information;
- A training program that covers Privacy Policies, protocols and awareness;
- A response plan to address privacy Incidents and privacy breaches; and
- Ongoing privacy assessments and audits.

3. PROPERTY RIGHTS TO COUNTY INFORMATION

All County Information is deemed property of the County, and the County shall retain exclusive rights and ownership thereto. County Information shall not be used by the Contractor for any purpose other than as required under this Contract, including as set forth in the DPA, nor shall such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by the Contractor, or commercially exploited or otherwise used by, or on behalf of, the Contractor, its officers, directors, employees, or agents. The Contractor may assert no lien on or right to withhold from the County, any County Information it receives from, receives addressed to, or stores on behalf of, the County. Notwithstanding the foregoing, the Contractor may aggregate, compile, and use County Information in order to improve, develop or enhance the System Software and/or other services offered, or to be offered, by the Contractor, provided that (i) no County Information in such aggregated or compiled pool is identifiable as originating from, or can be traced back to the County, and (ii) such Data or Information cannot be associated or matched with the identity of an individual alone, or linkable to a specific individual. The County shall always have access to such County Information held, stored, or maintained in the Online Services as set forth in the DPA. For any County Information transferred to Microsoft through Microsoft's Data Transfer and Management system ("DTM"), County has the ability to delete the County Information files at any time on the interface of the DTM. For any data subject requests, County shall have the right to discover, access, rectify, restrict, delete, export/receive the County Information as set forth in the DPA.

4. CONTRACTOR'S USE OF COUNTY INFORMATION

The Contractor may use County Information only as necessary to carry out its obligations under this Contract. The Contractor shall collect, maintain, or use County Information only for the purposes specified in the Contract and, in all cases, in compliance with all applicable local, state, and federal laws and regulations governing the collection, maintenance, transmission, dissemination, storage, use, and destruction of County Information, all as applicable to its providing the Products and Services, including, but not limited to, (i) any state and federal law governing the protection of personal Information, (ii) any state and federal security breach notification laws, (iii) the rules, regulations and directives of the Federal Trade Commission, as amended from time to time, and (iv) as set forth in the DPA.

5. SHARING COUNTY INFORMATION AND DATA

The Contractor shall not share, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, County Information to a third party for monetary or other valuable consideration. Any use or disclosure of County Information shall be only as authorized in the Contract and the DPA. With respect to any Microsoft Consulting Services, Contractor shall also handle County Information to perform its work as provided for in the Contract and the Work Orders and Scope of Services within the United States, and Microsoft Consulting Services shall not cause County Data to leave the borders of the United States unless otherwise approved by County in advance.

6. CONFIDENTIALITY

- a. **Confidentiality of County Information.** The Contractor agrees that all County Information is Confidential and proprietary to the County regardless of whether such Information was disclosed intentionally or unintentionally, or marked as "confidential".
- b. **Disclosure of County Information.** The Contractor may disclose County Information only as necessary to carry out its obligations under this Contract, or as required by law, and is prohibited from using County Information for any other purpose without the prior express written approval of the County's contract administrator in consultation with the County's Chief Information Security Officer and/or Chief Privacy Officer. As provided for in the DPA, if required by a court of competent jurisdiction or an administrative body to disclose County Information, the Contractor shall notify the County's contract administrator immediately and prior to any such disclosure, to provide the County an opportunity to oppose or otherwise respond to such disclosure, unless prohibited by law from doing so.
- c. **Disclosure Restrictions of Non-Public Information.** While performing work under the Contract, the Contractor may encounter County Non-public Information ("NPI") in the course of performing this Contract, including, but not limited to, licensed technology, drawings, schematics, manuals, sealed court records, and other materials described and/or identified as "Internal Use", "Confidential" or "Restricted" as defined in [Board of Supervisors Policy 6.104 – Information Classification Policy](#) as NPI. The Contractor shall not disclose or publish any County NPI and material received or used in performance of this Contract. This obligation shall apply until the County NPI is returned or deleted or as otherwise provided for in the Contract.
- d. **Individual Requests.** The Contractor shall acknowledge any request or instructions from the County regarding the exercise of any individual's privacy rights provided under applicable federal or state laws. The Contractor shall have in place appropriate policies and procedures to promptly respond to such requests and comply with any request or instructions from the County as set forth in the DPA. If an individual makes a request directly to the Contractor involving County Information, the Contractor shall redirect the individual to make its requests directly to County as set forth in the DPA. Similarly, if the Contractor receives a privacy or security complaint from an individual regarding County Information, the Contractor shall redirect the individual to make its request directly to County as set forth in the DPA. For any Security Incidents, Contractor will notify the County as described in the DPA and Section 12 SECURITY AND PRIVACY INCIDENTS below, and the County will coordinate an appropriate response.
- e. **Retention of County Information.** The Contractor shall not retain any County Information for any period longer than necessary for the Contractor to fulfill its obligations under the Contract and applicable law, whichever is longest.
- f. **Contract Confidentiality Terms.** The confidentiality terms provided for in Section 7.8 of the Contract and the DPA apply.

7. SUBCONTRACTORS AND THIRD PARTIES

Subcontracting is strictly prohibited without prior authorization from the County. However, the County acknowledges that in the course of performing its services, the Contractor may desire or require the use of goods, services, and/or assistance of Subcontractors or other third parties or suppliers. The terms of this Exhibit and the DPA shall also apply to all Subprocessors and Subcontractors, if any. The Contractor or third party shall be subject to the following terms and conditions: (i) each Subcontractor and third party must agree in writing to comply with and be bound by the applicable terms and conditions of this Exhibit and the DPA, both for itself and to enable the Contractor to be and remain in compliance with its obligations hereunder, including those provisions

relating to Confidentiality, Integrity, Availability, disclosures, security, and such other terms and conditions as may be reasonably necessary to effectuate the Contract including this Exhibit and the DPA; and (ii) as provided for in the DPA, the Contractor shall be and remain fully liable for the acts and omissions of each Subprocessor and its Subcontractors, and fully responsible for the due and proper performance of all Contractor obligations under this Contract.

The County's Chief Information Security Officer and/or Chief Privacy Officer may review the list of Subprocessors at any time and have the notice and controls on the use of Subprocessors as set forth in the DPA.

8. STORAGE AND TRANSMISSION OF COUNTY INFORMATION

All County Information shall be encrypted as provided for in the DPA. Without limiting the generality of the foregoing, as provided for in the DPA the Contractor will encrypt all workstations, portable devices (such as mobile, wearables, tablets,) and removable media (such as portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) that store County Information in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise approved by the County's Chief Information Security Officer.

The Contractor will encrypt County Information, if transmitted by Contractor on networks outside of the Contractor's control, with Transport Layer Security (TLS) or Internet Protocol Security (IPSec), at a minimum cipher strength of 128 bit or an equivalent secure transmission protocol or method approved by County's Chief Information Security Officer.

In addition, the Contractor shall not store County Information in any other third party cloud or in any other online storage provider without written authorization from the County's Chief Information Security Officer. All Contractor mobile devices, if any, storing County Information shall be managed by a Mobile Device Management system. Such system must provide provisions to enforce a password/passcode on enrolled mobile devices. All workstations/Personal Computers (including laptops, 2-in-1s, and tablets) will maintain the latest operating system security patches, and the latest virus definitions. Virus scans must be performed at least monthly. Request for less frequent scanning must be approved in writing by the County's Chief Information Security Officer.

9. PHYSICAL AND ENVIRONMENTAL SECURITY

All Contractor facilities that process County Information will be located in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference as set forth in the DPA.

All Contractor facilities that process County Information will be maintained with physical and environmental controls (temperature and humidity) that meet or exceed applicable hardware manufacturer's specifications and as set forth in the DPA.

10. OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY

The Contractor shall: (i) monitor and manage all of its Information processing facilities, including, without limitation, implementing operational procedures, change management, and Incident response procedures consistent with Section 12 SECURITY AND PRIVACY INCIDENTS; and (ii) deploy adequate anti-malware software and adequate back-up systems to ensure essential business Information can be promptly recovered in the event of a disaster or media failure; and (iii)

ensure its operating procedures are adequately documented and designed to protect Information and computer media from theft and unauthorized access.

The Contractor must have business continuity and disaster recovery plans. These plans must include a geographically separate data center and a formal framework by which an unplanned event will be managed to minimize the loss of County Information and services. The formal framework includes a defined business continuity management policy and associated procedures, including documented policies and procedures designed to: (i) simultaneously process the data and system in more than one environment and location; (ii) provide effective controls to safeguard the data; (iii) securely transfer County Information to and from the locations; (iv) restore applications and operating systems; and (v) demonstrate periodic testing of business continuity management.

11. ACCESS CONTROL

Subject to and without limiting the requirements under Section 8 STORAGE AND TRANSMISSION OF COUNTY INFORMATION, County Information (i) may only be made available and accessible to those parties explicitly authorized under the Contract or otherwise expressly approved by the County Project Director or Project Manager in writing; and (ii) will be transferred to Contractor using DTM as provided for in Section 3 above.

12. SECURITY AND PRIVACY INCIDENTS

In the event of a Security or Privacy Incident, the Contractor shall as provided for in the DPA:

- a. Promptly and without undue delay notify the County's Chief Information Security Officer, the Departmental Information Security Officer, and the County's Chief Privacy Officer of any Incidents involving County Information, within the time frame provided for in the DPA of detection of the Incident. All notifications shall be by a means Microsoft selects, including email.

For each Enterprise Services Work Order, County will inform Microsoft who is the County point of contact for Security Incident notice:

County Chief Information Security Officer and Chief Privacy Officer email

CISO-CPO_Notify@lacounty.gov

Chief Information Security Officer:

Jeffrey Aguilar
Chief Information Security Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
(213) 253-5659

Chief Privacy Officer:

Lillian Russell
Chief Privacy Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
(213) 351-5363

Departmental Information Security Officer:

Joel Simangan

Departmental Information Security Officer and Privacy Officer
Internal Services Department

(562) 940-2373

jismangan@isd.lacounty.gov

- b. Include to the extent known the following Information in all notices:
 - i. The date and time of discovery of the Incident,
 - ii. The approximate date and time of the Incident,
 - iii. Information to enable Customer to determine the type of County Information involved in the reported Incident, and
 - iv. A summary of the relevant facts, including a description of measures being taken to respond to and remediate the Incident, and any planned corrective actions as they are identified.
 - v. The name and contact information for the organizations official representative(s), with relevant business and technical information relating to the incident.
- c. Investigate the Security Incident and provide Customer with detailed information about the Security Incident, and take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. In doing so, Microsoft will cooperate with the County's reasonable requests in the investigation the Incident and to the extent known to identify the specific County Information involved in the Incident upon the County's written request (Microsoft will identify what specific information was disclosed, and County determines the nature and classification of the information). As Information about the Incident is collected or otherwise becomes available to the Contractor, and unless prohibited by law, the Contractor shall provide Information regarding the nature and consequences of the Incident that are reasonably requested by the County to allow the County to notify affected individuals, government agencies, and/or credit bureaus.
- d. Immediately initiate, if applicable, the appropriate portions of their Business Continuity and/or Disaster Recovery plans in the event of an Incident causing an interference with Information Technology operations.
- e. Reasonably assist and cooperate with forensic investigators, the County, law firms, and and/or law enforcement agencies at the direction of the County to help determine the nature, extent, and source of any Incident, and reasonably assist and cooperate with the County on any additional disclosures that the County is required to make as a result of the Incident.
- f. Allow the County or its third-party designee at the County's election to perform audits and penetration tests of the applications you deploy in Azure. With regard to Contractor's environment, County has the rights set forth in the DPA regarding Auditing Compliance that may include, but are not limited to, review of audit reports, assessments, controls and documentation, or other technical inspection of systems, all as set forth in the Trust Center, as they relate to the receipt, maintenance, use, retention, and authorized destruction of County Information.

13. NON-EXCLUSIVE EQUITABLE REMEDY

The Contractor acknowledges and agrees that due to the unique nature of County Information there may be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to the County, and therefore, that upon any such breach, the County will be entitled to seek appropriate equitable remedies, and may seek injunctive relief from a court

of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies are available within law or equity.

14. AUDIT AND INSPECTION

- a. **Self-Audits.** As provided for in the DPA, the Contractor shall periodically conduct audits, assessments, testing of the system of controls, and testing of Information Security and privacy procedures, including penetration testing, intrusion detection, and firewall configuration reviews. These periodic audits will be conducted by staff certified to perform the specific audit in question at Contractor's sole cost and expense through either (i) an internal independent audit function, or (ii) qualified, external, independent auditors as set forth in the Microsoft Trust Center.

The Contractor shall have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. The Contractor shall provide the audit results and any corrective action documentation to the Microsoft Trust Center promptly upon its completion. Any reports and related materials provided to the County pursuant to this Section shall be provided at no additional charge to the County.

County Requested Audits. At its own expense, the County, or an independent third-party auditor commissioned by the County, shall have the right to audit as provided for in Section 8.38, Record Retention and Inspection-Audit Settlement of the MSA. As provided for in the DPA and when not prohibited by regulation, the Contractor will provide to the County a summary of: (i) the results of any security audits, security reviews, or other relevant audits, conducted by the Contractor or a third party; and (ii) corrective actions or modifications, if any, the Contractor will implement in response to such audits.

15. PRIVACY AND SECURITY INDEMNIFICATION

Contractor's privacy and security indemnification obligations are as set forth in the Contract, including the DPA.

Microsoft Products and Services Data Protection Addendum

Volume
Licensing

Microsoft Products and Services Data Protection Addendum

Last updated September 15, 2021

Published in English on September 15, 2021. Translations will be published by Microsoft when available. These commitments are binding on Microsoft as of September 15, 2021.

Table of Contents

INTRODUCTION	3	Notice and Controls on use of Subprocessors	10
Applicable DPA Terms and Updates	3	Educational Institutions	11
Electronic Notices	3	CJIS Customer Agreement	11
Prior Versions	3	HIPAA Business Associate	11
DEFINITIONS	4	California Consumer Privacy Act (CCPA)	11
GENERAL TERMS	5	Biometric Data	11
Compliance with Laws	5	Supplemental Professional Services	11
DATA PROTECTION TERMS	5	How to Contact Microsoft	12
Scope	5	APPENDIX A – SECURITY MEASURES	13
Nature of Data Processing; Ownership	5	APPENDIX B – DATA SUBJECTS AND CATEGORIES OF PERSONAL DATA	16
Disclosure of Processed Data	6	APPENDIX C – ADDITIONAL SAFEGUARDS ADDENDUM	18
Processing of Personal Data; GDPR	6	ATTACHMENT 1 – THE 2010 STANDARD CONTRACTUAL CLAUSES (PROCESSORS)	20
Data Security	8	ATTACHMENT 2 – EUROPEAN UNION GENERAL DATA PROTECTION REGULATION TERMS	25
Security Incident Notification	9		
Data Transfers and Location	9		
Data Retention and Deletion	10		
Processor Confidentiality Commitment	10		

Introduction

The parties agree that this Microsoft Products and Services Data Protection Addendum (“DPA”) sets forth their obligations with respect to the processing and security of Customer Data, Professional Services Data, and Personal Data in connection with the Products and Services. The DPA is incorporated by reference into the Product Terms and other Microsoft agreements. The parties also agree that, unless a separate Professional Services agreement exists, this DPA governs the processing and security of Professional Services Data. Separate terms, including different privacy and security terms, govern Customer’s use of Non-Microsoft Products.

In the event of any conflict or inconsistency between the DPA Terms and any other terms in Customer’s volume licensing agreement, the DPA Terms shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the Microsoft Privacy Statement that otherwise may apply to processing of Customer Data, Professional Services Data, or Personal Data, as defined herein. For clarity, consistent with Clause 10 of the 2010 Standard Contractual Clauses in [Attachment 1](#), when the 2010 Standard Contractual Clauses are applicable, the 2010 Standard Contractual Clauses prevail over any other term of the DPA Terms.

Microsoft makes the commitments in this DPA to all customers with volume license agreements. These commitments are binding on Microsoft with regard to Customer regardless of (1) the Product Terms that are otherwise applicable to any given Product subscription or license, or (2) any other agreement that references the Product Terms.

Applicable DPA Terms and Updates

Limits on Updates

When Customer renews or purchases a new subscription to a Product or enters into a work order for a Professional Service, the then-current DPA Terms will apply and will not change during Customer’s subscription for that Product or term for that Professional Service. When Customer obtains a perpetual license to Software, the then-current DPA Terms will apply (following the same provision for determining the applicable then-current Product Terms for that Software in Customer’s volume licensing) and will not change during Customer’s license for that Software.

New Features, Supplements, or Related Software

Notwithstanding the foregoing limits on updates, when Microsoft introduces features, offerings, supplements or related software that are new (i.e., that were not previously included with the Products or Services), Microsoft may provide terms or make updates to the DPA that apply to Customer’s use of those new features, offerings, supplements or related software. If those terms include any material adverse changes to the DPA Terms, Microsoft will provide Customer a choice to use the new features, offerings, supplements, or related software, without loss of existing functionality of a generally available Product or Professional Service. If Customer does not install or use the new features, offerings, supplements, or related software, the corresponding new terms will not apply.

Government Regulation and Requirements

Notwithstanding the foregoing limits on updates, Microsoft may modify or terminate a Product or Professional Service in any country or jurisdiction where 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 there, (2) presents a hardship for Microsoft to continue operating the Product or offering the Professional Service without modification, and/or (3) causes Microsoft to believe the DPA Terms or the Product or Professional Service may conflict with any such requirement or obligation.

Electronic Notices

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

Prior Versions

The DPA Terms provide terms for Products and Services that are currently available. For earlier versions of the DPA Terms, Customer may refer to <https://aka.ms/licensingdocs> or contact its reseller or Microsoft Account Manager.

[Table of Contents](#) / [General Terms](#)

Definitions

Capitalized terms used but not defined in this DPA will have the meanings provided in the volume license agreement. The following defined terms are used in this DPA:

“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. Customer Data does not include Professional Services Data.

“Data Protection Requirements” means the GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

“DPA Terms” means the terms in the DPA and any Product-specific terms in the Product Terms that specifically supplement or modify the privacy and security terms in the DPA for a specific Product (or feature of a Product). In the event of any conflict or inconsistency between the DPA and such Product-specific terms, the Product-specific terms shall prevail as to the applicable Product (or feature of that Product).

“GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

“Local EU/EEA Data Protection Laws” means any subordinate legislation and regulation implementing the GDPR.

“GDPR Terms” means the terms in [Attachment 2](#), under which Microsoft makes binding commitments regarding its processing of Personal Data as required by Article 28 of the GDPR.

“Personal Data” means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Product” has the meaning provided in the volume license agreement. For ease of reference, “Product” includes Online Services and Software, each as defined in the volume license agreement.

“Products and Services” means Products and Professional Services. Product and Professional Service availability may vary by region and applicability of this DPA to specific Products and Professional Services is subject to the limitations in the Scope section in this DPA.

“Professional Services” means the following services: (a) Microsoft’s consulting services, consisting of planning, advice, guidance, data migration, deployment and solution/software development services provided under a Microsoft Enterprise Services Work Order that incorporates this DPA by reference; and (b) technical support services provided by Microsoft that help customers identify and resolve issues affecting Products, including technical support provided as part of Microsoft Unified Support or Premier Support Services (as described in the Services Consulting and Support Description or the Description of Services, respectively), and any other technical support services. The Professional Services do not include the Products or, for purposes of the DPA, Supplemental Professional Services.

“Professional Services Data” means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from a Product) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services.

“2010 Standard Contractual Clauses” means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010. The 2010 Standard Contractual Clauses are in [Attachment 1](#).

“2021 Standard Contractual Clauses” means the standard data protection clauses (processor-to-processor module) between Microsoft Ireland Operations Limited and Microsoft Corporation for the transfer of personal data from processors in the EEA to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission in decision 2021/914/EC, dated 4 June 2021.

“Subprocessor” means other processors used by Microsoft to process Customer Data, Professional Services Data, and Personal Data, as described in Article 28 of the GDPR.

“Supplemental Professional Services” means support requests escalated from support to a Product engineering team for resolution and other consulting and support from Microsoft provided in connection with Products or a volume license agreement that are not included in the definition of Professional Services.

Lower case terms used but not defined in this DPA, such as “personal data breach”, “processing”, “controller”, “processor”, “profiling”, “personal data”, and “data subject” will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies.

[Table of Contents](#) / [General Terms](#)

General Terms

Compliance with Laws

Microsoft will comply with all laws and regulations applicable to its providing the Products and Services, including security breach notification law and Data Protection Requirements. 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's 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 Products and Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Products and Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Products and Services in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of Products and Services, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

Data Protection Terms

This section of the DPA includes the following subsections:

- Scope
- Nature of Data Processing; Ownership
- Disclosure of Processed Data
- Processing of Personal Data; GDPR
- Data Security
- Security Incident Notification
- Data Transfers and Location
- Data Retention and Deletion
- Processor Confidentiality Commitment
- Notice and Controls on use of Subprocessors
- Educational Institutions
- CJIS Customer Agreement
- HIPAA Business Associate
- California Consumer Privacy Act (CCPA)
- Biometric Data
- Supplemental Professional Services
- How to Contact Microsoft
- Appendix A – Security Measures
- Appendix B – Data Subjects and Categories of Personal Data
- Appendix C – Additional Safeguards Addendum.

Scope

The DPA Terms apply to all Products and Services except as described in this section.

The DPA Terms will not apply to any Products specifically identified as excluded, or to the extent identified as excluded, in the Product Terms, which are governed by the privacy and security terms in the applicable Product-specific terms.

For clarity, the DPA Terms apply only to the processing of data in environments controlled by Microsoft and Microsoft's subprocessors. This includes data sent to Microsoft by Products and Services but does not include data that remains on Customer's premises or in any Customer selected third party operating environments.

For Supplemental Professional Services, Microsoft only makes the commitments in the Supplemental Professional Services section below.

Previews may employ lesser or different privacy and security measures than those typically present in the Products and Services. Unless otherwise noted, Customer should not use Previews to process Personal Data or other data that is subject to legal or regulatory compliance requirements. For Products, the following terms in this DPA do not apply to Previews: Processing of Personal Data; GDPR, Data Security, and HIPAA Business Associate. For Professional Services, offerings designated as Previews or Limited Release only meet the terms of the Supplemental Professional Services.

Nature of Data Processing; Ownership

Microsoft will use and otherwise process Customer Data, Professional Services Data, and Personal Data only as described and subject to the limitations provided below (a) to provide Customer the Products and Services in accordance with Customer's documented instructions, and (b) for business operations incident to providing the Products and Services to Customer. As between the parties, Customer retains all right, title and interest in and to Customer Data and Professional Services Data. Microsoft acquires no rights in Customer Data or Professional Services Data, other than the rights Customer grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Processing to Provide Customer the Products and Services

For purposes of this DPA, “to provide” a Product consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Ongoing improvement (installing the latest updates and making improvements to user productivity, reliability, efficacy, quality, and security).

For purposes of this DPA, “to provide” Professional Services consists of:

- Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.
- Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the Professional Services or relevant Product(s) during delivery of Professional Services); and
- Ongoing improvement (improving delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including installing the latest updates and fixing software defects).

When providing Products and Services, Microsoft will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer’s documented instructions.

Processing for Business Operations

For purposes of this DPA, “business operations” consist of the following, each as incident to delivery of the Products and Services to Customer: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Processed Data outlined below).

When processing for these business operations, Microsoft will apply principles of data minimization and will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section.

Disclosure of Processed Data

Microsoft will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, “Processed Data” means: (a) Customer Data; (b) Professional Services Data; (c) Personal Data; and (d) any other data processed by Microsoft in connection with the Products and Services that is Customer’s confidential information under the volume license agreement. All processing of Processed Data is subject to Microsoft’s obligation of confidentiality under the volume license agreement.

Microsoft will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed 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 Processed 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 Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed 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.

Processing of Personal Data; GDPR

All Personal Data processed by Microsoft in connection with providing the Products and Services is obtained as part of either (a) Customer Data, (b) Professional Services Data, or (c) data generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer’s use of service-based capabilities or obtained by Microsoft from locally installed software. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Online Service is also Customer Data. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Professional Services is also Professional Services Data. Pseudonymized identifiers may be included in data processed by Microsoft in connection with providing the Products and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in [Attachment 2](#) govern that processing and the parties also agree to the following terms in this sub-section ("Processing of Personal Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in the Product-specific terms or this DPA. When Microsoft acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its volume licensing agreement (including the DPA Terms and any applicable updates), along with the product documentation and Customer's use and configuration of features in the Products, are Customer's complete documented instructions to Microsoft for the processing of Personal Data, or the Professional Services documentation and Customer's use of the Professional Services. Information on use and configuration of the Products can be found at <https://docs.microsoft.com/en-us/> (or a successor location) or other agreement incorporating this DPA. Any additional or alternate instructions must be agreed to according to the process for amending Customer's agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Microsoft that Customer's instructions, including appointment of Microsoft as a processor or subprocessor, have been authorized by the relevant controller.

To the extent Microsoft uses or otherwise processes Personal Data subject to the GDPR for business operations incident to providing the Products and Services to Customer, Microsoft will comply with the obligations of an independent data controller under GDPR for such use. Microsoft is accepting the added responsibilities of a data "controller" under GDPR for processing in connection with its business operations to: (a) act consistent with regulatory requirements, to the extent required under GDPR; and (b) provide increased transparency to Customers and confirm Microsoft's accountability for such processing. Microsoft employs safeguards to protect Customer Data, Professional Services Data, and Personal Data in processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR. With respect to processing of Personal Data under this paragraph, Microsoft makes the commitments set forth in the Additional Safeguards section; for those purposes, (i) any Microsoft disclosure of Personal Data, as described in the Additional Safeguards section, that has been transferred in connection with business operations is deemed a "Relevant Disclosure" and (ii) the commitments in the Additional Safeguards section apply to such Personal Data.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled "Nature of Data Processing; Ownership" above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Products and Services pursuant to Customer's volume licensing agreement and for business operations incident to providing the Products and Services to Customer (as further described in the section of this DPA entitled "Nature of Data Processing; Ownership" above).
- **Categories of Data.** The types of Personal Data processed by Microsoft when providing the Products and Services include: (i) Personal Data that Customer elects to include in Customer Data and Professional Services Data; and (ii) those expressly identified in Article 4 of the GDPR that may be generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by Microsoft from locally installed software. The types of Personal Data that Customer elects to include in Customer Data and Professional Services Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in Appendix B.
- **Data Subjects.** The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Appendix B.

Data Subject Rights; Assistance with Requests

Microsoft will make available to Customer, in a manner consistent with the functionality of the Products and Services and Microsoft's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If Microsoft receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with the Products and Services for which Microsoft is a data processor or subprocessor, Microsoft will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Products and Services. Microsoft shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

Records of Processing Activities

To the extent the GDPR requires Microsoft to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Microsoft and keep it accurate and up-to-date. Microsoft may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data, Professional Services Data, and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.

In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. A description of the security controls for these requirements is available to Customers.

Each Core Online Service also complies with the control standards and frameworks shown in the table in the Product Terms. Each Core Online Service and Professional Service implements and maintains the security measures set forth in Appendix A for the protection of Customer Data and Professional Services Data.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate ISO 27001, ISO 27002, ISO 27018 or any standard or framework in the table for Core Online Services in the Product Terms, unless it is no longer used in the industry and it is replaced with a successor (if any).

Data Encryption

Customer Data and Professional Services Data (each including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default.

Microsoft also encrypts Customer Data stored at rest in Online Services and Professional Services Data stored at rest. In the case of Online Services on which Customer or a third-party acting on Customer's behalf may build applications (e.g., certain Azure Services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by Microsoft or obtained by Customer from third parties.

Data Access

Microsoft employs least privilege access mechanisms to control access to Customer Data and Professional Services Data (including any Personal Data therein). Role-based access controls are employed to ensure that access to Customer Data and Professional Services Data required for service operations is for an appropriate purpose and approved with management oversight. For Core Online Services and Professional Services, Microsoft maintains Access Control mechanisms described in the table entitled "Security Measures" in Appendix A. For Core Online Services, there is no standing access by Microsoft personnel to Customer Data and any required access is for a limited time.

Customer Responsibilities

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for Products and Services meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Microsoft provide a level of security appropriate to the risk with respect to its Personal Data. 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).

Auditing Compliance

Microsoft will conduct audits of the security of the computers, computing environment, and physical data centers that it uses in processing Customer Data, Professional Service Data, and 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.
- 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 Microsoft will make available at <https://servicetrust.microsoft.com/> or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and 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. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

To the extent Customer's audit requirements under the 2010 Standard Contractual Clauses or Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers, Microsoft will

promptly respond to Customer's additional audit instructions. Before the commencement of an audit, Customer and Microsoft will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Microsoft to unreasonably delay performance of the audit. To the extent needed to perform the audit, Microsoft will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data, Professional Services Data, and Personal Data by Microsoft, its Affiliates, and its Subprocessors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Microsoft, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Microsoft's other customers or to Microsoft systems or facilities not involved in providing the applicable Products and Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Microsoft expends for any such audit, in addition to the rates for services performed by Microsoft. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Microsoft and Microsoft shall promptly cure any material non-compliance.

If the 2010 Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the 2010 Standard Contractual Clauses. Nothing in this section of the DPA varies or modifies the 2010 Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority's or data subject's rights under the 2010 Standard Contractual Clauses or Data Protection Requirements. Microsoft Corporation is an intended third-party beneficiary of this section.

Security Incident Notification

If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, Professional Services Data, or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (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 Customer by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer maintains accurate contact information with Microsoft for each applicable Product and Professional Service. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Microsoft's notification of or response 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 the Products and Services.

Data Transfers and Location

Data Transfers

Customer Data, Professional Services Data, and Personal Data that Microsoft processes on Customer's behalf may not be transferred to, or stored and processed in a geographic location except in accordance with the DPA Terms and the safeguards provided below in this section. Taking into account such safeguards, Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms.

All transfers of Customer Data, Professional Services Data, and Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Products and Services shall be governed by the 2021 Standard Contractual Clauses implemented by Microsoft. In addition, transfers from the United Kingdom and Switzerland shall be governed by the 2010 Standard Contractual Clauses. In the case of any inconsistency between the 2021 Standard Contractual Clauses and the 2010 Standard Contractual Clauses, the inconsistency shall be resolved so as to provide an adequate level of data protection for the Customer Data, Professional Services Data, and Personal Data under applicable law. 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, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail, although Microsoft does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18. Microsoft agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

Location of Customer Data at Rest

For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as set forth in the Product Terms.

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

Data Retention and Deletion

At all times during the term of Customer's subscription or the applicable Professional Services engagement, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service and Professional Services Data.

Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services 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 and Personal Data stored in Online Services within an additional 90 days, unless authorized under this DPA to retain such data.

For Personal Data in connection with the Software and for Professional Services Data, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon Customer's request, unless authorized under this DPA to retain such 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, Professional Services Data, or Personal Data as described in this section.

Processor Confidentiality Commitment

Microsoft will ensure that its personnel engaged in the processing of Customer Data, Professional Services Data, and Personal Data (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Microsoft shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Customer Data, Professional Services Data, and Personal Data in accordance with applicable Data Protection Requirements and industry standards.

Notice and Controls on use of Subprocessors

Microsoft may hire Subprocessors to provide certain limited or ancillary services on its behalf. Customer consents to this engagement and to Microsoft Affiliates as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by Microsoft of the processing of Customer Data, Professional Services Data, and Personal Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

Microsoft is responsible for its Subprocessors' compliance with Microsoft's obligations in this DPA. Microsoft makes available information about Subprocessors on a Microsoft website. When engaging any Subprocessor, Microsoft will ensure via a written contract that the Subprocessor may access and use Customer Data, Professional Services Data, or Personal Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Customer Data, Professional Services Data, or Personal Data for any other purpose. Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the DPA, including the limitations on disclosure of Processed Data. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 6 months in advance of providing that Subprocessor with access to Customer Data. Additionally, Microsoft will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 30 days in advance of providing that Subprocessor with access to Professional Services Data or Personal Data other than that which is contained in Customer Data. If Microsoft engages a new Subprocessor for a new Product or Professional Service that processes Customer Data, Professional Services Data, or Personal Data, Microsoft will give Customer notice prior to availability of that Product or Professional Service.

If Customer does not approve of a new Subprocessor for an Online Service or Professional Services, then Customer may terminate any subscription for the affected Online Service or the applicable Statements of Service for the applicable Professional Service, respectively, without penalty or termination fee by providing, before the end of the relevant notice period, written notice of termination. If Customer does not approve of a new Subprocessor for Software, and Customer cannot reasonably avoid use of the Subprocessor by restricting Microsoft from processing data as set forth in the documentation or this DPA, then Customer may terminate any license for the affected software product without penalty by providing, before the end of the relevant notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Microsoft to re-evaluate any such new Subprocessor based on the applicable concerns. If the affected Product 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 any subscriptions or other applicable unpaid work for the terminated Products or Services from subsequent invoices to Customer or its reseller.

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 DPA, Microsoft is a “school official” with “legitimate educational interests” in the Customer Data and Professional Services 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 Products and Services 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 and Professional Services Data in Microsoft’s possession as may be required under applicable law.

CJIS Customer Agreement

Microsoft provides certain government cloud services (“Covered Services”) in accordance with the FBI Criminal Justice Information Services (“CJIS”) Security Policy (“CJIS Policy”). The CJIS Policy governs the use and transmission of criminal justice information. All Microsoft CJIS Covered Services shall be governed by the terms and conditions in the CJIS Customer Agreement located here: <http://aka.ms/CJISCustomerAgreement>.

HIPAA Business Associate

If Customer is a “covered entity” or a “business associate” and includes “protected health information” in Customer Data or Professional Services Data, as those terms are defined under the Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations promulgated thereunder (collectively, “HIPAA”), execution of Customer’s volume licensing agreement includes execution of the HIPAA Business Associate Agreement (“BAA”). The full text of the BAA identifies the Online Services or Professional 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; and
- if Customer has multiple volume licensing agreements, the volume licensing agreement to which the opt out applies.

California Consumer Privacy Act (CCPA)

If Microsoft is processing Personal Data within the scope of the CCPA, Microsoft makes the following additional commitments to Customer. Microsoft will process Customer Data, Professional Services Data, and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any “sale” exemption. In no event will Microsoft sell any such data. These CCPA terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the DPA Terms, Product Terms, or other agreement between Microsoft and Customer.

Biometric Data

If Customer uses Products and Services to process Biometric Data, Customer is responsible for: (i) providing notice to data subjects, including with respect to retention periods and destruction; (ii) obtaining consent from data subjects; and (iii) deleting the Biometric Data, all as appropriate and required under applicable Data Protection Requirements. Microsoft will process that Biometric Data following Customer’s documented instructions (as described in the “Processor and Controller Roles and Responsibilities” section above) and protect that Biometric Data in accordance with the data security and protection terms under this DPA. For purposes of this section, “Biometric Data” will have the meaning set forth in Article 4 of the GDPR and, if applicable, equivalent terms in other Data Protection Requirements.

Supplemental Professional Services

When used in the sections listed below, the defined term “Professional Services” includes Supplemental Professional Services, and the defined term “Professional Services Data” includes data obtained for Supplemental Professional Services.

For Supplemental Professional Services, the following sections of the DPA apply in the same manner as they apply to Professional Services: “Introduction”, “Compliance with Laws”, “Nature of Processing; Ownership”, “Disclosure of Processed Data”, “Processing of Personal Data; GDPR”, the first paragraph of “Security Practices and Policies”, “Customer Responsibilities”, “Security Incident Notification”, “Data Transfer” (including the terms regarding the 2010 Standard Contractual Clauses and 2021 Standard Contractual Clauses), the third paragraph of “Data Retention and Deletion”, “Processor Confidentiality Commitment”, “Notice and Controls on use of Subprocessors”, “HIPAA Business Associate” (to the extent applicable in the BAA), “California Consumer Privacy Act (CCPA)”, “Biometric Data”, “How to Contact Microsoft”, “Appendix B – Data Subjects and Categories of Personal Data”, and “Appendix C – Additional Safeguards Addendum”.

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
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland

[Table of Contents](#) / [General Terms](#)

Appendix A – Security Measures

Microsoft has implemented and will maintain for Customer Data in the Core Online Services and Professional Services Data the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms), are Microsoft's only responsibility with respect to the security of that 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 or Professional Services 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 and before processing Professional Service Data or launching the Professional Services. 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 or Professional Services 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 and Professional Services Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and Professional Services Data and has procedures for disposing of printed materials that contain such data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data or Professional Services Data on portable devices, remotely accessing such data, or processing such 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 or Professional Services Data are located to identified authorized individuals. Physical Access to Components. Microsoft maintains records of the incoming and outgoing media containing Customer Data or Professional Services Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of such 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. Component Disposal. Microsoft uses industry standard processes to delete Customer Data and Professional Services 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 or Professional Services Data. Data Recovery Procedures - On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Microsoft maintains multiple copies of Customer Data and Professional Services Data from which such data can be recovered. - Microsoft stores copies of Customer Data and Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data and Professional Services Data are located. - Microsoft has specific procedures in place governing access to copies of Customer Data and Professional Services Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Professional Services and for Azure Government Services, which are reviewed every twelve months.

Domain	Practices
	- 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 and Professional Services Data, including malicious software originating from public networks. Data Beyond Boundaries - Microsoft encrypts, or enables Customer to encrypt, Customer Data and Professional Services Data that is transmitted over public networks. - Microsoft restricts access to Customer Data and Professional Services Data in media leaving its facilities. Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data or Professional Services 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 or Professional Services Data. Access Authorization - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data or Professional Services 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 or Professional Services Data, the individuals have separate identifiers/log-ins. Least Privilege - Technical support personnel are only permitted to have access to Customer Data and Professional Services Data when needed. - Microsoft restricts access to Customer Data and Professional Services 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. - 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 or Professional Services Data they are not authorized to access.

Domain	Practices
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 undue delay and, in any event, within 72 hours. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data and Professional Services 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 or Professional Services Data are located. - Microsoft’s redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data and Professional Services Data in its original or last-replicated state from before the time it was lost or destroyed.

[Table of Contents](#) / [General Terms](#)

Appendix B – Data Subjects and Categories of Personal Data

Data subjects: Data subjects include the Customer's representatives and end-users including employees, contractors, collaborators, and customers of the Customer. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by Microsoft. Microsoft acknowledges that, depending on Customer's use of the Products and Services, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

- Employees, contractors and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of data: The personal data that is included in e-mail, documents and other data in an electronic form in the context of the Products and Services. Microsoft acknowledges that, depending on Customer's use of the Products and Services, Customer may elect to include personal data from any of the following categories in the personal data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);

- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified in Article 4 of the GDPR.

Appendix C – Additional Safeguards Addendum

By this Additional Safeguards Addendum to the DPA (this “Addendum”), Microsoft provides additional safeguards to Customer for the processing of personal data, within the scope of the GDPR, by Microsoft on behalf of Customer and additional redress to the data subjects to whom that personal data relates.

This Addendum supplements and is made part of, but is not in variation or modification of, the DPA.

1. Challenges to Orders. In the event Microsoft receives an order from any third party for compelled disclosure of any personal data processed under this DPA, Microsoft shall:

- a. use every reasonable effort to redirect the third party to request data directly from Customer;
- b. promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and
- c. use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with applicable law of the European Union or applicable Member State law.

If, after the steps described in a. through c. above, Microsoft or any of its affiliates remains compelled to disclose personal data, Microsoft will disclose only the minimum amount of that data necessary to satisfy the order for compelled disclosure.

For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2. Indemnification of Data Subjects. Subject to Sections 3 and 4, Microsoft shall indemnify a data subject for any material or non-material damage to the data subject caused by Microsoft’s disclosure of personal data of the data subject that has been transferred in response to an order from a non-EU/EEA government body or law enforcement agency in violation of Microsoft’s obligations under Chapter V of the GDPR (a “Relevant Disclosure”). Notwithstanding the foregoing, Microsoft shall have no obligation to indemnify the data subject under this Section 2 to the extent the data subject has already received compensation for the same damage, whether from Microsoft or otherwise.

3. Conditions of Indemnification. Indemnification under Section 2 is conditional upon the data subject establishing, to Microsoft’s reasonable satisfaction, that:

- a. Microsoft engaged in a Relevant Disclosure;
- b. the Relevant Disclosure was the basis of an official proceeding by the non-EU/EEA government body or law enforcement agency against the data subject; and
- c. the Relevant Disclosure directly caused the data subject to suffer material or non-material damage.

The data subject bears the burden of proof with respect to conditions a. through c.

Notwithstanding the foregoing, Microsoft shall have no obligation to indemnify the data subject under Section 2 if Microsoft establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

4. Scope of Damages. Indemnification under Section 2 is limited to material and non material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Microsoft’s infringement of the GDPR.

5. Exercise of Rights. Rights granted to data subjects under this Addendum may be enforced by the data subject against Microsoft irrespective of any restriction in Clauses 3 or 6 of the Standard Contractual Clauses. The data subject may only bring a claim under this Addendum on an individual basis, and not part of a class, collective, group or representative action. Rights granted to data subjects under this Addendum are personal to the data subject and may not be assigned.

6. Notice of Change. Microsoft agrees and warrants that it has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which personal data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from the data exporter and its obligations under this Addendum, the 2010 Standard Contractual Clauses, or the 2021 Standard Contractual Clauses and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Addendum or the Standard Contractual Clauses, it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of data and/or terminate the contract.

7. Termination. This Addendum shall automatically terminate if the European Commission, a competent Member State supervisory authority, or an EU or competent Member State court approves a different lawful transfer mechanism that would be applicable to the personal data in the Customer Data, Professional Services Data, or other Personal Data that is processed under the DPA (and if such mechanism applies only to some of

that data, this Addendum will terminate only with respect to that data) and that does not require the additional safeguards set forth in this Addendum.

Attachment 1 – The 2010 Standard Contractual Clauses (Processors)

Execution of the volume licensing agreement by Customer includes execution of this Attachment 1, which is countersigned by Microsoft Corporation. This Attachment 1 is in addition to Microsoft's execution of the 2021 Standard Contractual Clauses. In the case of any inconsistency between this Attachment 1 and the 2021 Standard Contractual Clauses, the inconsistency shall be resolved so as to provide an adequate level of data protection for the Customer Data, Professional Services Data, and Personal Data under applicable law. 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.

Beginning May 25, 2018, and thereafter, references to various Articles from the Directive 95/46/EC in the Standard Contractual Clauses below will be treated as references to the relevant and appropriate Articles in the GDPR.

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Customer (as data exporter) and Microsoft Corporation (as data importer, whose signature appears below), each a "party," together "the parties," have agreed on the following Contractual Clauses (the "Clauses" or "Standard Contractual Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1: Definitions

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as 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;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on

the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 below;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law.

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

Data exporter: Customer is the data exporter. The data exporter is a user of Products or Professional Services as defined in the DPA and Product Terms.

Data importer: The data importer is MICROSOFT CORPORATION, a global producer of software and services.

Data subjects: Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter as detailed in Appendix B to the DPA.

Categories of data: The personal data transferred that is included in e-mail, documents, and other data in an electronic form in the context of the Products or Professional Services. Microsoft acknowledges that, depending on Customer's use of the Products or Professional Services, Customer may elect to include personal data from any of the categories detailed in Appendix B to the DPA.

Processing operations: The personal data transferred will be subject to the following basic processing activities:

a. Duration and Object of Data Processing. The duration of data processing shall be for the term designated under the applicable volume licensing agreement between data exporter and the Microsoft entity to which these Standard Contractual Clauses are annexed ("Microsoft"). The objective of the data processing is the performance of Products and Services.

b. Scope and Purpose of Data Processing. The scope and purpose of processing personal data is described in the "Processing of Personal Data; GDPR" section of the DPA. The data importer operates a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities in accordance with the "Security Practices and Policies" section of the DPA.

c. Customer Data and Personal Data Access. For the term designated under the applicable volume licensing agreement data importer will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data and personal data, or (2) make such corrections, deletions, or blockages on its behalf.

d. Data Exporter's Instructions. For Products and Services, data importer will only act upon data exporter's instructions as conveyed by Microsoft.

e. Customer Data and Personal Data Deletion or Return. Upon expiration or termination of data exporter's use of Products or Professional Services, it may extract Customer Data and personal data and data importer will delete Customer Data and personal data, each in accordance with the DPA Terms applicable to the agreement.

Subcontractors: In accordance with the DPA, the data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data and personal data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data and personal data for any other purpose.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. Personnel. Data importer's personnel will not process Customer Data or personal data without authorization. Personnel are obligated to maintain the confidentiality of any such Customer Data and personal data and this obligation continues even after their engagement ends.

2. Data Privacy Contact. The data privacy officer of the data importer can be reached at the following address:

Microsoft Corporation
Attn: Chief Privacy Officer
1 Microsoft Way
Redmond, WA 98052 USA

3. Technical and Organization Measures. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data and personal data, as defined in the Security Practices and Policies section of the DPA, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in the Security Practices and Policies section of the DPA are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signing the Standard Contractual Clauses, Appendix 1, and Appendix 2 on behalf of the data importer:

Signature 
DocuSigned By: Rajesh Jha

Rajesh Jha, Executive Vice President

Microsoft Corporation

One Microsoft Way, Redmond WA, USA 98052

[Table of Contents](#) / [General Terms](#)

Attachment 2 – European Union General Data Protection Regulation Terms

Microsoft makes the commitments in these GDPR Terms, to all customers effective May 25, 2018. These commitments are binding upon Microsoft with regard to Customer regardless of (1) the version of the Product Terms and DPA that is otherwise applicable to any given Product subscription or license, or (2) any other agreement that references this attachment.

For purposes of these GDPR Terms, Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Microsoft on behalf of Customer. These GDPR Terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the Product Terms or other agreement between Microsoft and Customer. These GDPR Terms do not apply where Microsoft is a controller of Personal Data.

Relevant GDPR Obligations: Articles 28, 32, and 33

1. Microsoft shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, Microsoft shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))
2. Processing by Microsoft shall be governed by these GDPR Terms under European Union (hereafter “Union”) or Member State law and are binding on Microsoft with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer’s licensing agreement, including these GDPR Terms. In particular, Microsoft shall:
 - (a) process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which Microsoft is subject; in such a case, Microsoft shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 - (b) ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 - (c) take all measures required pursuant to Article 32 of the GDPR;
 - (d) respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;
 - (e) taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III of the GDPR;
 - (f) assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Microsoft;
 - (g) at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;
 - (h) make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

Microsoft shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

3. Where Microsoft engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, Microsoft shall remain fully liable to the Customer for the performance of that other processor’s obligations. (Article 28(4))

4. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and Microsoft shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) the pseudonymisation and encryption of Personal Data;

- (b)** the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c)** the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
- (d)** a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))

5. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Article 32(2))

6. Customer and Microsoft shall take steps to ensure that any natural person acting under the authority of Customer or Microsoft who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law. (Article 32(4))

7. Microsoft shall notify Customer without undue delay after becoming aware of a Personal Data breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Microsoft.

[Table of Contents](#) / [General Terms](#)



+
SELWYN HOLLINS
Director

County of Los Angeles
INTERNAL SERVICES DEPARTMENT

1100 North Eastern Avenue
Los Angeles, California 90063

"Trusted Partner and Provider of Choice"

Telephone: (323) 267-2101
FAX: (323) 264-7135

November 3, 2021

To: Supervisor Hilda Solis, Chair
Supervisor Holly Mitchell
Supervisor Sheila Kuehl
Supervisor Janice Hahn
Supervisor Kathryn Barger

From: Selwyn Hollins 
Director

NOTIFICATION OF INTENT TO ENTER INTO SOLE SOURCE NEGOTIATIONS WITH MICROSOFT CORPORATION FOR HIGHLY SPECIALIZED TECHNICAL SUPPORT SERVICES

This is to advise your Board of the Internal Services Department's (ISD) intent to enter into sole source negotiations for a contract with Microsoft Corporation (Microsoft) to replace the existing Microsoft Premier Support Services (PSS) contract, which provides highly technical advisory and support services for County departments.

BACKGROUND

On June 30, 2015, your Board awarded the PSS contract to Microsoft which provides access to internal Microsoft resources and highly technical advisory and support services to County departments. PSS includes technical planning and assessments, third-tier product support that provides direct high-end technical engineering resources and dedicated in the design and deployment of Microsoft products and technologies. ISD administers the PSS contract, and the current contract expires on June 29, 2022.

JUSTIFICATION

Microsoft is the sole provider for certain proprietary Microsoft support services. The proprietary services are developed in conjunction with Microsoft product groups and contain intellectual property that can only be provided by Microsoft. The scope of services will allow Microsoft to provide support services to the County to address emergent and time-sensitive consulting and performance management needs.

Therefore, a sole source contract with Microsoft is necessary to ensure that essential support services continue to be available and to allow the County to take advantage of cost saving solutions provided under the new Microsoft Unified Support Services program.

On October 15, 2021, ISD released a Request for Information (RFI) to survey the market for companies that can provide both support and consulting services for Microsoft products and technologies to determine the feasibility of releasing a competitive solicitation for the replacement services. Pending the responses received, it is ISD's intent to unbundle the current Microsoft services contract, and divide the contracted services into multiple smaller contracts as a viable procurement strategy to encourage small, local, and diverse business utilization. However, there will still be a need for a sole source contract with Microsoft to provide technical engineering resources and support services for customized and proprietary software.

Board Policy No. 5.100 requires written notice of a department's intent to enter into sole source negotiations for a new, or replacement, Board approved contract at least six months prior to the contract's expiration date. The subject contract expires on June 29, 2022; therefore, this notice is within the time frames required by the policy.

CONCLUSION

Unless otherwise instructed by your Board, ISD will proceed with negotiations of the replacement contract with Microsoft Corporation. ISD will work closely with County Counsel, Chief Information Officer and the Chief Executive Office during the contracting process.

If you have any questions, please call me at (323) 267-2101, via email: shollins@isd.lacounty.gov, or your staff may contact Christie Carr, Contract Manager, at (323) 267-3101, via email: ccarr@isd.lacounty.gov.

SH:MO:LG:CC:ew

c: Executive Office, Board of Supervisors
 Chief Executive Office
 ISD Board Deputies
 County Counsel

INTERNAL SERVICES DEPARTMENT
PURCHASING & CONTRACT SERVICES
M E M O R A N D U M

April 27, 2022

To: Linh Mok, Budget Manager
Chief Executive Office

From: Christie Carr, Contracts Division Manager *CC*
Internal Services Department

**JUSTIFICATION FOR SOLE A SOURCE CONTRACT FOR
MICROSOFT UNIFIED SUPPORT AND CONSULTING SERVICES**

This is to provide justification of the Internal Services Department's (ISD), with advice from County Counsel (CC), intent to award a new sole source contract with Microsoft Corporation (Microsoft).

BACKGROUND

On June 30, 2015, the Board awarded the Premier Support Services (PSS) agreement to Microsoft Corporation which provides access to internal Microsoft resources and highly technical advisory and support services to County departments. PSS includes technical planning and assessments, third-tier product support that provides direct high-end technical engineering resources and dedicated in the design and deployment of Microsoft products and technologies.

JUSTIFICATION

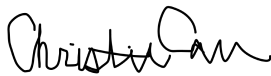
The maintenance/support that comes with Microsoft commercial software licenses is limited to software updates, bug fixes, and software/security patches. As such, County departments have been acquiring Microsoft support services through support specific contracts since 2005.

Microsoft is the sole provider for certain proprietary Microsoft support and consulting services. The proprietary services are developed in conjunction with Microsoft product groups and contain intellectual property that can only be provided by Microsoft. The scope of services in the recommended contract will allow Microsoft to provide support services to the County to address emergent and time-sensitive consulting and performance management needs. Therefore, a sole source contract with Microsoft is necessary to ensure that essential support services continue to be available.

CONCLUSION

On November 3, 2021, in compliance with Board Policy 5.100, Sole Source Contracts, ISD provided notification to the Board of its intent to enter into sole source negotiations for a contract with Microsoft to replace the existing contract, which provides highly technical advisory and support services for County departments. The notice was within the time frames required by the policy. During the contract development and negotiations process ISD worked closely with the CIO and County Counsel to ensure the contract best meets the needs of the County. In accordance with the Board's Policy, the Sole Source Justification and corresponding Sole Source Checklist herein is requested for CEO review and approval.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Christie Carr". The signature is fluid and cursive, with the first name "Christie" and last name "Carr" clearly distinguishable.

Christie Carr
ISD Contract Manager

Attachment

SOLE SOURCE CHECKLIST

Department Name: Internal Services Department

- ☒ New Sole Source Contract
- ☐ Sole Source Amendment to Existing Contract
- Date Existing Contract First Approved:

Check (✓)	JUSTIFICATION FOR SOLE SOURCE CONTRACTS AND AMENDMENTS Identify applicable justification and provide documentation for each checked item.
☒	➤ Only one bona fide source (monopoly) for the service exists; performance and price competition are not available. A monopoly is an <i>"Exclusive control of the supply of any service in a given market. If more than one source in a given market exists, a monopoly does not exist."</i>
☐	➤ Compliance with applicable statutory and/or regulatory provisions.
☐	➤ Compliance with State and/or federal programmatic requirements.
☐	➤ Services provided by other public or County-related entities.
☐	➤ Services are needed to address an emergent or related time-sensitive need.
☐	➤ The service provider(s) is required under the provisions of a grant or regulatory requirement.
☐	➤ Services are needed during the time period required to complete a solicitation for replacement services; provided services are needed for no more than 12 months from the expiration of an existing contract which has no available option periods.
☐	➤ Maintenance and support services are needed for an existing solution/system during the time to complete a solicitation for a new replacement solution/system; provided the services are needed for no more than 24 months from the expiration of an existing maintenance and support contract which has no available option periods.
☐	➤ Maintenance service agreements exist on equipment which must be serviced by the original equipment manufacturer or an authorized service representative.
☐	➤ It is more cost-effective to obtain services by exercising an option under an existing contract.
☐	➤ It is in the best economic interest of the County (e.g., significant costs and time to replace an existing system or infrastructure, administrative cost and time savings and excessive learning curve for a new service provider, etc.). In such cases, departments must demonstrate due diligence in qualifying the cost-savings or cost-avoidance associated with the best economic interest of the County.

Sheila Williams

Digitally signed by Sheila Williams
Date: 2022.04.28 11:42:01 -0700

Chief Executive Office

Date

Community Business Enterprise Program Information

FIRM INFORMATION*		MICROSOFT CORPORATION		
BUSINESS STRUCTURE		Corporation		
CULTURAL/ETHNIC COMPOSITION		NUMBER / % OF OWNERSHIP		
OWNERS/PARTNERS	Black/African American	PUBLICLY TRADED COMPANY (Numbers not available)		
	Hispanic/Latino			
	Asian or Pacific Islander			
	American Indian			
	Filipino			
	White			
	Female (included above)			
			NUMBER	
MANAGER	Black/African American			
	Hispanic/Latino			
	Asian or Pacific Islander			
	American Indian			
	Filipino			
	White			
	Female (included above)			
STAFF	Black/African American			
	Hispanic/Latino			
	Asian or Pacific Islander			
	American Indian			
	Filipino			
	White			
	Female (included above)			
Total # of Employees				
COUNTY CERTIFICATION				
CBE		N		
LSBE		N		
OTHER CERTIFYING AGENCY				

*On final analysis and consideration of award, vendor was selected without regard to race, creed or color.