



Department of Administration  
 Purchasing Division  
 2019 Washington Street East  
 Post Office Box 50130  
 Charleston, WV 25305-0130

State of West Virginia  
**Master Agreement**

Order Date: 09-25-2020

CORRECT ORDER NUMBER MUST  
 APPEAR ON ALL PACKAGES, INVOICES,  
 AND SHIPPING PAPERS. QUESTIONS  
 CONCERNING THIS ORDER SHOULD BE  
 DIRECTED TO THE DEPARTMENT  
 CONTACT.

Order Number:	CMA 0212 0212 GSUITE20 1	Procurement Folder:	786322
Document Name:	G-Suite products and services	Reason for Modification:	
Document Description:	G-Suite products and services		
Procurement Type:	Central Master Agreement		
Buyer Name:			
Telephone:			
Email:			
Shipping Method:	Best Way	Effective Start Date:	2020-09-28
Free on Board:	FOB Dest, Freight Prepaid	Effective End Date:	2025-09-27

VENDOR		DEPARTMENT CONTACT																				
Vendor Customer Code:	000000117794	Requestor Name:	Andrew C Lore																			
SHI INTERNATIONAL CORP 290 DAVIDSON AVE		Requestor Phone:	(304) 957-8267																			
SOMERSET NJ 08873		Requestor Email:	andrew.c.lore@wv.gov																			
US																						
Vendor Contact Phone:	304-541-4288 Extension:																					
Discount Details:																						
	<table border="1"> <thead> <tr> <th></th> <th>Discount Allowed</th> <th>Discount Percentage</th> <th>Discount Days</th> </tr> </thead> <tbody> <tr> <td>#1</td> <td>No</td> <td>0.0000</td> <td>0</td> </tr> <tr> <td>#2</td> <td>No</td> <td></td> <td></td> </tr> <tr> <td>#3</td> <td>No</td> <td></td> <td></td> </tr> <tr> <td>#4</td> <td>No</td> <td></td> <td></td> </tr> </tbody> </table>		Discount Allowed	Discount Percentage	Discount Days	#1	No	0.0000	0	#2	No			#3	No			#4	No			
	Discount Allowed	Discount Percentage	Discount Days																			
#1	No	0.0000	0																			
#2	No																					
#3	No																					
#4	No																					

INVOICE TO	SHIP TO
VARIOUS AGENCY LOCATIONS AS INDICATED BY ORDER	STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER
No City WV 99999	No City WV 99999
US	US

Total Order Amount:	Open End
---------------------	----------

Purchasing Division's File Copy

**ENTERED**

*9-25-2020 BOT*  
*Ralston*

PURCHASING DIVISION AUTHORIZATION
DATE: <i>9/25/20</i>
ELECTRONIC SIGNATURE ON FILE

ATTORNEY GENERAL APPROVAL AS TO FORM
DATE: <i>9-25-20</i>
ELECTRONIC SIGNATURE ON FILE

ENCUMBRANCE CERTIFICATION
DATE: <i>9-28-2020</i>
ELECTRONIC SIGNATURE ON FILE

**Extended Description:**

Contract with SHI International Corp. (Master Agreement No. AR2488) to provide G-Suite products and services specified per the attached documentation.

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
1	43230000			EA	0.000000
	<b>Service From</b>	<b>Service To</b>			

**Commodity Line Description:** G-Suite Products and Services

**Extended Description:**

See Google G-Suite Pricing Sheets attached

	Document Phase	Document Description	Page
GSUITE20	Draft	G-Suite products and services	3

**ADDITIONAL TERMS AND CONDITIONS**

See attached document(s) for additional Terms and Conditions

**CLOUD SOLUTIONS 2016-2026**

Led by the State of Utah

---

Master Agreement #: AR2488

Contractor: **SHI INTERNATIONAL CORP.**

Participating Entity: **STATE OF WEST VIRGINIA**

The following products or services are included in this contract portfolio:

- *G-Suite products and services specified in the SADA Systems Scope of Work attached as Exhibit B.*

The following products or services are not included in this agreement:

- *This agreement shall not be used for any purchases outside of the products and services outlined in Exhibit B.*
- *Removable Example: Product modifications.*
- *Removable Example: Installation services.*

**Master Agreement Terms and Conditions:**

1. Scope: This addendum covers **Cloud Solutions**, specifically, the G-Suite products and services outlined in Exhibit B, offered through the cooperative contract led by the State of Utah. The G-Suite products will be for use by the Participating Entity and entities authorized by that State's statutes to utilize State contracts. For the avoidance of doubt, the parties agree that Contractor shall have no liability to Participating Entity for the G-Suite products and services outlined in Exhibit B beyond: a) liability associated with the processing of invoices and payment therefor, and b) liability necessary to prevent privity of contract being a defense against liability attributable to SADA and Google, both of which will be responsible for their respective liabilities associated with the G-Suite products and services as indicated in the Terms Agreements with SADA and Google attached as Exhibit D.
2. Access to Cloud Solutions Services Requires State CTO Approval: Unless otherwise stipulated in this Participating Addendum, G-Suite products accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Solutions by state executive branch agencies are subject to the authority and prior approval of the West Virginia Chief Technology Officer. The Chief Technology Officer means the individual designated by the Governor within the Executive Branch with enterprise-wide responsibilities for leadership and management of information technology resources of the state.
3. Primary Contacts: The primary contact individuals for this Participating Addendum are as follows (or their named successors):

**CLOUD SOLUTIONS 2016-2026**  
Led by the State of Utah

Contractor

Name:	Gary Wilson
Address:	290 Davidson Avenue, Somerset, NJ 08873
Telephone:	732-652-3081
Fax:	
Email:	<a href="mailto:PS_Contracts@shi.com">PS_Contracts@shi.com</a>

Participating Entity

Name:	West Virginia Office of Technology
Address:	1900 Kanawha Blvd, E-Building 5, 10th Floor, Charleston, WV 25305
Telephone:	304-957-8184
Fax:	
Email:	<a href="mailto:justin.t.mcallister@wv.gov">justin.t.mcallister@wv.gov</a>

**4. PARTICIPATING ENTITY MODIFICATIONS OR ADDITIONS TO THE MASTER AGREEMENT**

These modifications or additions apply only to actions and relationships within the Participating Entity.

Participating Entity must check one of the boxes below.

No changes to the terms and conditions of the Master Agreement are required.

The following changes are modifying or supplementing the Master Agreement terms and conditions.

- a. Order of Priority: The Contract is comprised of the documents listed in this section. The terms and conditions contained in the various documents shall be interpreted according to the priority given to the Contract document in this section. In that way, any terms and conditions contained in the first priority document shall prevail over conflicting terms in the second priority document, and so on.

Contract Documents:

1. **Participating Addendum** (this document) – First Priority
2. **WV-96 Agreement Addendum** (Attached as Exhibit A) – Second Priority
3. **Confidentiality Policies and Information Security Accountability Requirements** – (Attached as Exhibit C) – Third Priority
4. **Google Terms Agreement** (attached as Exhibit D) and **SADA Terms Agreement and SADA Scope of Work** (Attached as Exhibit B) – Fifth Priority
5. **Proposal Submitted to West Virginia NASPO ValuePoint Cloud Solutions RFQ**, dated July 31, 2020 – (Attached as Exhibit E) Sixth Priority
6. **NASPO Master Agreement** (Attached as Exhibit F) – Seventh Priority

- b. **Modifications:** The Participating Entity and SHI agree that the following documents are modified as follows:
1. WV-96: The parties agree that term 19 of the WV-96 is removed in its entirety.
- c. **Additional Terms:** The Parties Agree that the following terms and conditions are added to this Contract.
1. **PRIVACY, SECURITY, AND CONFIDENTIALITY:** Contractor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from Participating Entity, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to Participating Entity's policies, procedures, and rules. Contractor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in Exhibit E.
  2. **ANTITRUST:** In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the Participating Entity, Contractor agrees to convey, sell, assign, or transfer to the Participating Entity all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the Participating Entity. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Contractor.
  3. **BACKGROUND CHECK:** The Participating Entity reserves the right to prohibit Contractor's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Contractor should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.
5. **Orders:** Any order placed by a Participating Entity or Purchasing Entity for a product and/or service available from this Master Agreement shall be deemed to be a sale under (and governed by the prices and other terms and conditions of) the Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to such order.



**CLOUD SOLUTIONS 2016-2026**  
 Led by the State of Utah

IN WITNESS WHEREOF, the parties have executed this Addendum as of the date of execution by both parties below.

Participating Entity: West Virginia Office of Technology	Contractor: SHI International Corp.
Signature: <i>Justin T. McAllister</i>	Signature: <i>Kristina Mann</i>
Name: Justin T. McAllister	Name: Kristina Mann
Title: Chief Financial Officer	Title: Senior Lead Contract Specialist
Date: September 24, 2020	Date: 9/24/20

*[Additional signatures may be added if required by the Participating Entity]*

For questions on executing a participating addendum, please contact:

NASPO ValuePoint

Cooperative Development Coordinator:	Shannon Berry
Telephone:	775-720-3404
Email:	<a href="mailto:sberry@naspovaluepoint.org">sberry@naspovaluepoint.org</a>

**Please email fully executed PDF copy of this document to [PA@naspovaluepoint.org](mailto:PA@naspovaluepoint.org) to support documentation of participation and posting in appropriate data bases.**

**NASPO ValuePoint  
PARTICIPATING ADDENDUM**

**CLOUD SOLUTIONS 2016-2026**  
Led by the State of Utah



---

**EXHIBIT A**



STATE OF WEST VIRGINIA  
ADDENDUM TO VENDOR'S STANDARD CONTRACTUAL FORMS

State Agency, Board, or Commission (the "State"): *WV Office of Technology*  
Vendor: *SHI International Corp.*  
Contract/Lease Number ("Contract"): *GSUITE20*  
Commodity/Service: *G-Suite Products and Services*

The State and the Vendor are entering into the Contract identified above. The Vendor desires to incorporate one or more forms it created into the Contract. Vendor's form(s), however, include(s) one or more contractual terms and conditions that the State cannot or will not accept. In consideration for the State's incorporating Vendor's form(s) into the Contract, the Vendor enters into this Addendum which specifically eliminates or alters the legal enforceability of certain terms and conditions contained in Vendor's form(s). Therefore, on the date shown below each signature line, the parties agree to the following contractual terms and conditions in this Addendum are dominate over any competing terms made a part of the Contract:

- 1. ORDER OF PRECEDENCE:** This Addendum modifies and supersedes anything contained on Vendor's form(s) whether or not they are submitted before or after the signing of this Addendum. **IN THE EVENT OF ANY CONFLICT BETWEEN VENDOR'S FORM(S) AND THIS ADDENDUM, THIS ADDENDUM SHALL CONTROL.**
- 2. PAYMENT** – Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software licenses, subscriptions, or maintenance may be paid annually in advance.  
Any language imposing any interest or charges due to late payment is deleted.
- 3. FISCAL YEAR FUNDING** – Performance of this Contract is contingent upon funds being appropriated by the WV Legislature or otherwise being available for this Contract. In the event funds are not appropriated or otherwise available, the Contract becomes of no effect and is null and void after June 30 of the current fiscal year. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.
- 4. RIGHT TO TERMINATE** – The State reserves the right to terminate this Contract upon thirty (30) days written notice to the Vendor. If this right is exercised, the State agrees to pay the Vendor only for all undisputed services rendered or goods received before the termination's effective date. All provisions are deleted that seek to require the State to (1) compensate Vendor, in whole or in part, for lost profit, (2) pay a termination fee, or (3) pay liquidated damages if the Contract is terminated early.  
Any language seeking to accelerate payments in the event of Contract termination, default, or non-funding is hereby deleted.
- 5. DISPUTES** – Any language binding the State to any arbitration or to the decision of any arbitration board, commission, panel or other entity is deleted; as is any requirement to waive a jury trial.  
Any language requiring or permitting disputes under this Contract to be resolved in the courts of any state other than the State of West Virginia is deleted. All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.  
Any language requiring the State to agree to, or be subject to, any form of equitable relief not authorized by the Constitution or laws of State of West Virginia is deleted.
- 6. FEES OR COSTS:** Any language obligating the State to pay costs of collection, court costs, or attorney's fees, unless ordered by a court of competent jurisdiction is deleted.
- 7. GOVERNING LAW** – Any language requiring the application of the law of any state other than the State of West Virginia in interpreting or enforcing the Contract is deleted. The Contract shall be governed by the laws of the State of West Virginia.
- 8. RISK SHIFTING** – Any provision requiring the State to bear the costs of all or a majority of business/legal risks associated with this Contract, to indemnify the Vendor, or hold the Vendor or a third party harmless for any act or omission is hereby deleted.
- 9. LIMITING LIABILITY** – Any language limiting the Vendor's liability for direct damages to person or property is deleted.
- 10. TAXES** – Any provisions requiring the State to pay Federal, State or local taxes or file tax returns or reports on behalf of Vendor are deleted. The State will, upon request, provide a tax exempt certificate to confirm its tax exempt status.
- 11. NO WAIVER** – Any provision requiring the State to waive any rights, claims or defenses is hereby deleted.

- 12. **STATUTE OF LIMITATIONS** – Any clauses limiting the time in which the State may bring suit against the Vendor or any other third party are deleted.
- 13. **ASSIGNMENT** – The Vendor agrees not to assign the Contract to any person or entity without the State’s prior written consent, which will not be unreasonably delayed or denied. The State reserves the right to assign this Contract to another State agency, board or commission upon thirty (30) days written notice to the Vendor. These restrictions do not apply to the payments made by the State. Any assignment will not become effective and binding upon the State until the State is notified of the assignment, and the State and Vendor execute a change order to the Contract.
- 14. **RENEWAL** – Any language that seeks to automatically renew, modify, or extend the Contract beyond the initial term or automatically continue the Contract period from term to term is deleted. The Contract may be renewed or continued only upon mutual written agreement of the Parties.
- 15. **INSURANCE** – Any provision requiring the State to maintain any type of insurance for either its or the Vendor’s benefit is deleted.
- 16. **RIGHT TO REPOSSESSION NOTICE** – Any provision for repossession of equipment without notice is hereby deleted. However, the State does recognize a right of repossession with notice.
- 17. **DELIVERY** – All deliveries under the Contract will be FOB destination unless the State expressly and knowingly agrees otherwise. Any contrary delivery terms are hereby deleted.
- 18. **CONFIDENTIALITY** – Any provisions regarding confidential treatment or non-disclosure of the terms and conditions of the Contract are hereby deleted. State contracts are public records under the West Virginia Freedom of Information Act (“FOIA”) (W. Va. Code §29B-a-1, et seq.) and public procurement laws. This Contract and other public records may be disclosed without notice to the vendor at the State’s sole discretion.

Any provisions regarding confidentiality or non-disclosure related to contract performance are only effective to the extent they are consistent with FOIA and incorporated into the Contract through a separately approved and signed non-disclosure agreement.

- 19. **THIRD-PARTY SOFTWARE** – If this Contract contemplates or requires the use of third-party software, the vendor represents that none of the mandatory click-through, unsigned, or web-linked terms and conditions presented or required before using such third-party software conflict with any term of this Addendum or that it has the authority to modify such third-party software’s terms and conditions to be subordinate to this Addendum. The Vendor shall indemnify and defend the State against all claims resulting from an assertion that such third-party terms and conditions are not in accord with, or subordinate to, this Addendum.
- 20. **AMENDMENTS** – The parties agree that all amendments, modifications, alterations or changes to the Contract shall be by mutual agreement, in writing, and signed by both parties. Any language to the contrary is deleted.

Notwithstanding the foregoing, this Addendum can only be amended by (1) identifying the alterations to this form by using *Italics* to identify language being added and ~~strikethrough~~ for language being deleted (do not use track-changes) and (2) having the Office of the West Virginia Attorney General’s authorized representative expressly agree to and knowingly approve those alterations.

State: West Virginia Office of Technology

Vendor: SHI International Corp.

By: *Justin T. McAllister*

By: *Kristina Mann*

Printed Name: Justin T. McAllister

Printed Name: Kristina Mann

Title: Chief Financial Officer

Title: Senior Lead Contract Specialist

Date: September 24, 2020

Date: 9/24/20

NASPO ValuePoint  
**PARTICIPATING ADDENDUM**

**CLOUD SOLUTIONS 2016-2026**  
Led by the State of Utah



---

**EXHIBIT B**

## SADA TERMS AND ORDER OF PRECEDENCE AGREEMENT

THIS SADA TERMS AND ORDER OF PRECEDENCE AGREEMENT, (hereinafter "Terms Agreement") by and between SAD Systems, Inc. (hereinafter "SADA") and State of West Virginia (hereinafter "State"), (both referred to as "Parties"), is intended to identify the various documents that comprise the terms agreement between the parties that will govern the provision of services related to the purchase of G-Suite products under the State's contract with SHI International Corp. ("SHI") identified as CMA Oala GSUITEAD.

**NOW THEREFORE**, the Parties hereto hereby agree as follows:

1. **Order of Precedence:** The Terms Agreement is comprised of the documents listed in this section. The terms and conditions contained in the various documents shall be interpreted according to the priority given to the document in this section. In that way, any terms and conditions contained in the first priority document shall prevail over conflicting terms in the second priority document, and so on.

### **Terms Agreement Documents:**

- a. **SADA Terms and Order of Precedent Agreement** (this document) – First Priority
- b. **WV-96 Agreement Addendum** (Attached as Exhibit A) – Second Priority
- c. **State Business Associate Addendum** (Attached as Exhibit B) – Third Priority
- d. **State SaaS Addendum** – (Exhibit C) – Fourth Priority
- e. **Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements** (Exhibit D) – Fifth Priority
- f. **SADA Systems Inc. Master Professional Services Agreement** (Exhibit E) – Sixth Priority

### **2. Modifications:**

#### **a. WV-96:**

- i. **Fiscal year Funding:** The term entitled "3. FISCAL YEAR FUNDING" is modified by adding " and it shall not excuse non-payment by the State for services performed by Vendor." to the last sentence.
- ii. **Assignment:** The term entitled "13. ASSIGNMENT" is modified by adding " provided the State remains jointly and severally liable until such time as Vendor approves of the assignment in writing" to the end of the second sentence.

#### **b. SADA Documents:**

- i. **Weblinks:** The Parties agree that any click-through or weblinked terms are inapplicable to this Terms Agreement unless the weblinked document containing the terms is expressly listed herein.
- j. **Additional Terms:** The Parties Agree that the following terms and conditions are added to this Terms Agreement.

- a. **PRIVACY, SECURITY, AND CONFIDENTIALITY:** The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in Exhibit D.
- b. **ANTITRUST:** In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.
- c. **BACKGROUND CHECK:** In accordance with W. Va. Code § 15-2D-3, the Director of the Division of Protective Services shall require any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol complex or who have access to sensitive or critical information to submit to a fingerprint-based state and federal background inquiry through the state repository. The service provider is responsible for any costs associated with the fingerprint-based state and federal background inquiry. After the contract for such services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the Capitol complex or have access to sensitive or critical information, the service provider shall submit a list of all persons who will be physically present and working at the Capitol complex to the Director of the Division of Protective Services for purposes of verifying compliance with this provision. The State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

IN WITNESS WHEREOF, the Parties have entered into this Terms Agreement as of the date of the last signature below.

**STATE OF WEST VIRGINIA**  
**Office of Technology**

By: Justin T. McAllister

Name: Justin T. McAllister

Its: Chief Financial Officer

Date: September 23, 2020

**SADA Systems, Inc.**

By: Patrick J. Monaghan

Name: Patrick Monaghan

Its: Chief Legal Officer

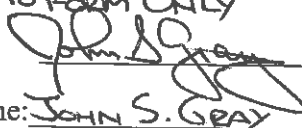
Date: 9/22/2020

STATE OF WEST VIRGINIA

Attorney General's Office

As to Form Only

By:

  
\_\_\_\_\_

Name:

JOHN S. GRAY  
\_\_\_\_\_

Its:

Deputy Attorney General  
\_\_\_\_\_

Date:

September 25, 2020  
\_\_\_\_\_

Date: \_\_\_\_\_

STATE OF WEST VIRGINIA

Purchasing Division

By:

  
\_\_\_\_\_

Name:

Frank W.H. Hales  
\_\_\_\_\_

Its:

Assistant Director  
\_\_\_\_\_

Date:

9/25/20  
\_\_\_\_\_

Date: \_\_\_\_\_

**SADA TERMS AND ORDER OF PRECEDENT AGREEMENT**

**EXHIBIT A**

**STATE OF WEST VIRGINIA  
ADDENDUM TO VENDOR'S STANDARD CONTRACTUAL FORMS**

State Agency, Board, or Commission (the "State"): West Virginia Office of Technology

Vendor: SADA Systems, Inc.

Contract/Lease Number ("Contract"):

Commodity/Service: G-Suite Implementation Services

The State and the Vendor are entering into the Contract identified above. The Vendor desires to incorporate one or more forms it created into the Contract. Vendor's form(s), however, include(s) one or more contractual terms and conditions that the State cannot or will not accept. In consideration for the State's incorporating Vendor's form(s) into the Contract, the Vendor enters into this Addendum which specifically eliminates or alters the legal enforceability of certain terms and conditions contained in Vendor's form(s). Therefore, on the date shown below each signature line, the parties agree to the following contractual terms and conditions in this Addendum are dominate over any competing terms made a part of the Contract:

1. **ORDER OF PRECEDENCE:** This Addendum modifies and supersedes anything contained on Vendor's form(s) whether or not they are submitted before or after the signing of this Addendum. **IN THE EVENT OF ANY CONFLICT BETWEEN VENDOR'S FORM(S) AND THIS ADDENDUM, THIS ADDENDUM SHALL CONTROL.**
2. **PAYMENT** – Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software licenses, subscriptions, or maintenance may be paid annually in advance.  
  
Any language imposing any interest or charges due to late payment is deleted.
3. **FISCAL YEAR FUNDING** – Performance of this Contract is contingent upon funds being appropriated by the WV Legislature or otherwise being available for this Contract. In the event funds are not appropriated or otherwise available, the Contract becomes of no effect and is null and void after June 30 of the current fiscal year. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.
4. **RIGHT TO TERMINATE** – The State reserves the right to terminate this Contract upon thirty (30) days written notice to the Vendor. If this right is exercised, the State agrees to pay the Vendor only for all undisputed services rendered or goods received before the termination's effective date. All provisions are deleted that seek to require the State to (1) compensate Vendor, in whole or in part, for lost profit, (2) pay a termination fee, or (3) pay liquidated damages if the Contract is terminated early.  
  
Any language seeking to accelerate payments in the event of Contract termination, default, or non-funding is hereby deleted.
5. **DISPUTES** – Any language binding the State to any arbitration or to the decision of any arbitration board, commission, panel or other entity is deleted; as is any requirement to waive a jury trial.  
  
Any language requiring or permitting disputes under this Contract to be resolved in the courts of any state other than the State of West Virginia is deleted. All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.  
  
Any language requiring the State to agree to, or be subject to, any form of equitable relief not authorized by the Constitution or laws of State of West Virginia is deleted.
6. **FEES OR COSTS:** Any language obligating the State to pay costs of collection, court costs, or attorney's fees, unless ordered by a court of competent jurisdiction is deleted.
7. **GOVERNING LAW** – Any language requiring the application of the law of any state other than the State of West Virginia in interpreting or enforcing the Contract is deleted. The Contract shall be governed by the laws of the State of West Virginia.
8. **RISK SHIFTING** -- Any provision requiring the State to bear the costs of all or a majority of business/legal risks associated with this Contract, to indemnify the Vendor, or hold the Vendor or a third party harmless for any act or omission is hereby deleted.
9. **LIMITING LIABILITY** – Any language limiting the Vendor's liability for direct damages to person or property is deleted.
10. **TAXES** – Any provisions requiring the State to pay Federal, State or local taxes or file tax returns or reports on behalf of Vendor are deleted. The State will, upon request, provide a tax exempt certificate to confirm its tax exempt status.
11. **NO WAIVER** – Any provision requiring the State to waive any rights, claims or defenses is hereby deleted.



12. **STATUTE OF LIMITATIONS** – Any clauses limiting the time in which the State may bring suit against the Vendor or any other third party are deleted.
13. **ASSIGNMENT** – The Vendor agrees not to assign the Contract to any person or entity without the State’s prior written consent, which will not be unreasonably delayed or denied. The State reserves the right to assign this Contract to another State agency, board or commission upon thirty (30) days written notice to the Vendor. These restrictions do not apply to the payments made by the State. Any assignment will not become effective and binding upon the State until the State is notified of the assignment, and the State and Vendor execute a change order to the Contract.
14. **RENEWAL** – Any language that seeks to automatically renew, modify, or extend the Contract beyond the initial term or automatically continue the Contract period from term to term is deleted. The Contract may be renewed or continued only upon mutual written agreement of the Parties.
15. **INSURANCE** – Any provision requiring the State to maintain any type of insurance for either its or the Vendor’s benefit is deleted.
16. **RIGHT TO REPOSSESSION NOTICE** – Any provision for repossession of equipment without notice is hereby deleted. However, the State does recognize a right of repossession with notice.
17. **DELIVERY** – All deliveries under the Contract will be FOB destination unless the State expressly and knowingly agrees otherwise. Any contrary delivery terms are hereby deleted.
18. **CONFIDENTIALITY** – Any provisions regarding confidential treatment or non-disclosure of the terms and conditions of the Contract are hereby deleted. State contracts are public records under the West Virginia Freedom of Information Act (“FOIA”) (W. Va. Code §29B-a-1, et seq.) and public procurement laws. This Contract and other public records may be disclosed without notice to the vendor at the State’s sole discretion.  
  
Any provisions regarding confidentiality or non-disclosure related to contract performance are only effective to the extent they are consistent with FOIA and incorporated into the Contract through a separately approved and signed non-disclosure agreement.
19. **THIRD-PARTY SOFTWARE** – If this Contract contemplates or requires the use of third-party software, the vendor represents that none of the mandatory click-through, unsigned, or web-linked terms and conditions presented or required before using such third-party software conflict with any term of this Addendum or that is has the authority to modify such third-party software’s terms and conditions to be subordinate to this Addendum. The Vendor shall indemnify and defend the State against all claims resulting from an assertion that such third-party terms and conditions are not in accord with, or subordinate to, this Addendum.
20. **AMENDMENTS** – The parties agree that all amendments, modifications, alterations or changes to the Contract shall be by mutual agreement, in writing, and signed by both parties. Any language to the contrary is deleted.

Notwithstanding the foregoing, this Addendum can only be amended by (1) identifying the alterations to this form by using *Italics* to identify language being added and ~~strike through~~ for language being deleted (do not use track-changes) and (2) having the Office of the West Virginia Attorney General’s authorized representative expressly agree to and knowingly approve those alterations.

State: West Virginia Office of Technology

Vendor: SADA Systems, Inc.

By: *Justin T. McAllister*

By: *Patrick J. Monaghan*

Printed Name: Justin T. McAllister

Printed Name: Patrick Monaghan

Title: Chief Financial Officer

Title: Chief Legal Officer

Date: September 23, 2020

Date: 9/22/2020

**SADA TERMS AND ORDER OF PRECEDENT AGREEMENT**

**EXHIBIT B**

## WV STATE GOVERNMENT

### HIPAA BUSINESS ASSOCIATE ADDENDUM

This Health Insurance Portability and Accountability Act of 1996 (hereafter, HIPAA) Business Associate Addendum ("Addendum") is made a part of the Agreement ("Agreement") by and between the State of West Virginia ("Agency"), and Business Associate ("Associate"), and is effective as of the date of execution of the Addendum.

The Associate performs certain services on behalf of or for the Agency pursuant to the underlying Agreement that requires the exchange of information including protected health information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA"). The Agency is a "Covered Entity" as that term is defined in HIPAA, and the parties to the underlying Agreement are entering into this Addendum to establish the responsibilities of both parties regarding HIPAA-covered information and to bring the underlying Agreement into compliance with HIPAA.

Whereas it is desirable, in order to further the continued efficient operations of Agency to disclose to its Associate certain information which may contain confidential individually identifiable health information (hereafter, Protected Health Information or PHI); and

Whereas, it is the desire of both parties that the confidentiality of the PHI disclosed hereunder be maintained and treated in accordance with all applicable laws relating to confidentiality, including the Privacy and Security Rules, the HITECH Act and its associated regulations, and the parties do agree to at all times treat the PHI and interpret this Addendum consistent with that desire.

NOW THEREFORE: the parties agree that in consideration of the mutual promises herein, in the Agreement, and of the exchange of PHI hereunder that:

1. **Definitions.** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
  - a. **Agency Procurement Officer** shall mean the appropriate Agency individual listed at: <http://www.state.wv.us/admin/purchase/vrc/agencyli.html>.
  - b. **Agent** shall mean those person(s) who are agent(s) of the Business Associate, in accordance with the Federal common law of agency, as referenced in 45 CFR § 160.402(c).
  - c. **Breach** shall mean the acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except as excluded in the definition of Breach in 45 CFR § 164.402.
  - d. **Business Associate** shall have the meaning given to such term in 45 CFR § 160.103.
  - e. **HITECH Act** shall mean the Health Information Technology for Economic and Clinical Health Act. Public Law No. 111-05. 111<sup>th</sup> Congress (2009).

- f. **Privacy Rule** means the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Parts 160 and 164.
- g. **Protected Health Information or PHI** shall have the meaning given to such term in 45 CFR § 160.103, limited to the information created or received by Associate from or on behalf of Agency.
- h. **Security Incident** means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information or interference with system operations in an information system.
- i. **Security Rule** means the Security Standards for the Protection of Electronic Protected Health Information found at 45 CFR Parts 160 and 164.
- j. **Subcontractor** means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

## 2. Permitted Uses and Disclosures.

- a. **PHI Described.** This means PHI created, received, maintained or transmitted on behalf of the Agency by the Associate. This PHI is governed by this Addendum and is limited to the minimum necessary, to complete the tasks or to provide the services associated with the terms of the original Agreement, and is described in Appendix A.
- b. **Purposes.** Except as otherwise limited in this Addendum, Associate may use or disclose the PHI on behalf of, or to provide services to, Agency for the purposes necessary to complete the tasks, or provide the services, associated with, and required by the terms of the original Agreement, or as required by law, if such use or disclosure of the PHI would not violate the Privacy or Security Rules or applicable state law if done by Agency or Associate, or violate the minimum necessary and related Privacy and Security policies and procedures of the Agency. The Associate is directly liable under HIPAA for impermissible uses and disclosures of the PHI it handles on behalf of Agency.
- c. **Further Uses and Disclosures.** Except as otherwise limited in this Addendum, the Associate may disclose PHI to third parties for the purpose of its own proper management and administration, or as required by law, provided that (i) the disclosure is required by law, or (ii) the Associate has obtained from the third party reasonable assurances that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party by the Associate; and, (iii) an agreement to notify the Associate and Agency of any instances of which it (the third party) is aware in which the confidentiality of the information has been breached. To the extent practical, the information should be in a limited data set or the minimum necessary information pursuant to 45 CFR § 164.502, or take other measures as necessary to satisfy the Agency's obligations under 45 CFR § 164.502.

### 3. Obligations of Associate.

- a. **Stated Purposes Only.** The PHI may not be used by the Associate for any purpose other than as stated in this Addendum or as required or permitted by law.
- b. **Limited Disclosure.** The PHI is confidential and will not be disclosed by the Associate other than as stated in this Addendum or as required or permitted by law. Associate is prohibited from directly or indirectly receiving any remuneration in exchange for an individual's PHI unless Agency gives written approval and the individual provides a valid authorization. Associate will refrain from marketing activities that would violate HIPAA, including specifically Section 13406 of the HITECH Act. Associate will report to Agency any use or disclosure of the PHI, including any Security Incident not provided for by this Agreement of which it becomes aware.
- c. **Safeguards.** The Associate will use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of the PHI, except as provided for in this Addendum. This shall include, but not be limited to:
  - i. Limitation of the groups of its workforce and agents, to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Addendum, and the use and disclosure of the minimum PHI necessary or a Limited Data Set;
  - ii. Appropriate notification and training of its workforce and agents in order to protect the PHI from unauthorized use and disclosure;
  - iii. Maintenance of a comprehensive, reasonable and appropriate written PHI privacy and security program that includes administrative, technical and physical safeguards appropriate to the size, nature, scope and complexity of the Associate's operations, in compliance with the Security Rule;
  - iv. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.
- d. **Compliance With Law.** The Associate will not use or disclose the PHI in a manner in violation of existing law and specifically not in violation of laws relating to confidentiality of PHI, including but not limited to, the Privacy and Security Rules.
- e. **Mitigation.** Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Associate of a use or disclosure of the PHI by Associate in violation of the requirements of this Addendum, and report its mitigation activity back to the Agency.

- f. **Support of Individual Rights.**
- i. **Access to PHI.** Associate shall make the PHI maintained by Associate or its agents or subcontractors in Designated Record Sets available to Agency for inspection and copying, and in electronic format, if requested, within ten (10) days of a request by Agency to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.524 and consistent with Section 13405 of the HITECH Act.
  - ii. **Amendment of PHI.** Within ten (10) days of receipt of a request from Agency for an amendment of the PHI or a record about an individual contained in a Designated Record Set, Associate or its agents or subcontractors shall make such PHI available to Agency for amendment and incorporate any such amendment to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.526.
  - iii. **Accounting Rights.** Within ten (10) days of notice of a request for an accounting of disclosures of the PHI, Associate and its agents or subcontractors shall make available to Agency the documentation required to provide an accounting of disclosures to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR §164.528 and consistent with Section 13405 of the HITECH Act. Associate agrees to document disclosures of the PHI and information related to such disclosures as would be required for Agency to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. This should include a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years from the date of disclosure, or longer if required by state law. At a minimum, such documentation shall include:
    - the date of disclosure;
    - the name of the entity or person who received the PHI, and if known, the address of the entity or person;
    - a brief description of the PHI disclosed; and
    - a brief statement of purposes of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.
  - iv. **Request for Restriction.** Under the direction of the Agency, abide by any individual's request to restrict the disclosure of PHI, consistent with the requirements of Section 13405 of the HITECH Act and 45 CFR § 164.522, when the Agency determines to do so (except as required by law) and if the disclosure is to a health plan for payment or health care operations and it pertains to a health care item or service for which the health care provider was paid in full "out-of-pocket."
  - v. **Immediate Discontinuance of Use or Disclosure.** The Associate will immediately discontinue use or disclosure of Agency PHI pertaining to any individual when so requested by Agency. This includes, but is not limited to, cases in which an individual has withdrawn or modified an authorization to use or disclose PHI.

- g. Retention of PHI.** Notwithstanding section 4.a. of this Addendum, Associate and its subcontractors or agents shall retain all PHI pursuant to state and federal law and shall continue to maintain the PHI required under Section 3.f. of this Addendum for a period of six (6) years after termination of the Agreement, or longer if required under state law.
- h. Agent's, Subcontractor's Compliance.** The Associate shall notify the Agency of all subcontracts and agreements relating to the Agreement, where the subcontractor or agent receives PHI as described in section 2.a. of this Addendum. Such notification shall occur within 30 (thirty) calendar days of the execution of the subcontract and shall be delivered to the Agency Procurement Officer. The Associate will ensure that any of its subcontractors, to whom it provides any of the PHI it receives hereunder, or to whom it provides any PHI which the Associate creates or receives on behalf of the Agency, agree to the restrictions and conditions which apply to the Associate hereunder. The Agency may request copies of downstream subcontracts and agreements to determine whether all restrictions, terms and conditions have been flowed down. Failure to ensure that downstream contracts, subcontracts and agreements contain the required restrictions, terms and conditions may result in termination of the Agreement.
- j. Federal and Agency Access.** The Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI, as well as the PHI, received from, or created or received by the Associate on behalf of the Agency available to the U.S. Secretary of Health and Human Services consistent with 45 CFR § 164.504. The Associate shall also make these records available to Agency, or Agency's contractor, for periodic audit of Associate's compliance with the Privacy and Security Rules. Upon Agency's request, the Associate shall provide proof of compliance with HIPAA and HITECH data privacy/protection guidelines, certification of a secure network and other assurance relative to compliance with the Privacy and Security Rules. This section shall also apply to Associate's subcontractors, if any.
- k. Security.** The Associate shall take all steps necessary to ensure the continuous security of all PHI and data systems containing PHI. In addition, compliance with 74 FR 19006 Guidance Specifying the Technologies and Methodologies That Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII is required, to the extent practicable. If Associate chooses not to adopt such methodologies as defined in 74 FR 19006 to secure the PHI governed by this Addendum, it must submit such written rationale, including its Security Risk Analysis, to the Agency Procurement Officer for review prior to the execution of the Addendum. This review may take up to ten (10) days.
- l. Notification of Breach.** During the term of this Addendum, the Associate shall notify the Agency and, unless otherwise directed by the Agency in writing, the WV Office of Technology immediately by e-mail or web form upon the discovery of any Breach of unsecured PHI; or within 24 hours by e-mail or web form of any suspected Security Incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the Agency Procurement Officer at [www.state.wv.us/admin/purchase/vrc/agencyli.htm](http://www.state.wv.us/admin/purchase/vrc/agencyli.htm) and,

unless otherwise directed by the Agency in writing, the Office of Technology at [incident@wv.gov](mailto:incident@wv.gov) or <https://apps.wv.gov/ot/ir/Default.aspx>.

The Associate shall immediately investigate such Security Incident, Breach, or unauthorized use or disclosure of PHI or confidential data. Within 72 hours of the discovery, the Associate shall notify the Agency Procurement Officer, and, unless otherwise directed by the Agency in writing, the Office of Technology of: (a) Date of discovery; (b) What data elements were involved and the extent of the data involved in the Breach; (c) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data; (d) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized; (e) A description of the probable causes of the improper use or disclosure; and (f) Whether any federal or state laws requiring individual notifications of Breaches are triggered.

Agency will coordinate with Associate to determine additional specific actions that will be required of the Associate for mitigation of the Breach, which may include notification to the individual or other authorities.

All associated costs shall be borne by the Associate. This may include, but not be limited to costs associated with notifying affected individuals.

If the Associate enters into a subcontract relating to the Agreement where the subcontractor or agent receives PHI as described in section 2.a. of this Addendum, all such subcontracts or downstream agreements shall contain the same incident notification requirements as contained herein, with reporting directly to the Agency Procurement Officer. Failure to include such requirement in any subcontract or agreement may result in the Agency's termination of the Agreement.

- m. **Assistance in Litigation or Administrative Proceedings.** The Associate shall make itself and any subcontractors, workforce or agents assisting Associate in the performance of its obligations under this Agreement, available to the Agency at no cost to the Agency to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Agency, its officers or employees based upon claimed violations of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inaction or actions by the Associate, except where Associate or its subcontractor, workforce or agent is a named as an adverse party.

#### 4. Addendum Administration.

- a. **Term.** This Addendum shall terminate on termination of the underlying Agreement or on the date the Agency terminates for cause as authorized in paragraph (c) of this Section, whichever is sooner.
- b. **Duties at Termination.** Upon any termination of the underlying Agreement, the Associate shall return or destroy, at the Agency's option, all PHI received from, or created or received by the Associate on behalf of the Agency that the Associate still maintains in any form and retain no copies of such PHI or, if such return or destruction is not feasible, the Associate shall extend the protections of this Addendum to the PHI and limit further uses and disclosures to the purposes that make the return or destruction of the PHI infeasible. This shall also apply to all agents and subcontractors of Associate. The duty of the Associate and its agents



and subcontractors to assist the Agency with any HIPAA required accounting of disclosures survives the termination of the underlying Agreement.

- c. **Termination for Cause.** Associate authorizes termination of this Agreement by Agency, if Agency determines Associate has violated a material term of the Agreement. Agency may, at its sole discretion, allow Associate a reasonable period of time to cure the material breach before termination.
- d. **Judicial or Administrative Proceedings.** The Agency may terminate this Agreement if the Associate is found guilty of a criminal violation of HIPAA. The Agency may terminate this Agreement if a finding or stipulation that the Associate has violated any standard or requirement of HIPAA/HITECH, or other security or privacy laws is made in any administrative or civil proceeding in which the Associate is a party or has been joined. Associate shall be subject to prosecution by the Department of Justice for violations of HIPAA/HITECH and shall be responsible for any and all costs associated with prosecution.
- e. **Survival.** The respective rights and obligations of Associate under this Addendum shall survive the termination of the underlying Agreement.

#### 5. General Provisions/Ownership of PHI.

- a. **Retention of Ownership.** Ownership of the PHI resides with the Agency and is to be returned on demand or destroyed at the Agency's option, at any time, and subject to the restrictions found within section 4.b. above.
- b. **Secondary PHI.** Any data or PHI generated from the PHI disclosed hereunder which would permit identification of an individual must be held confidential and is also the property of Agency.
- c. **Electronic Transmission.** Except as permitted by law or this Addendum, the PHI or any data generated from the PHI which would permit identification of an individual must not be transmitted to another party by electronic or other means for additional uses or disclosures not authorized by this Addendum or to another contractor, or allied agency, or affiliate without prior written approval of Agency.
- d. **No Sales.** Reports or data containing the PHI may not be sold without Agency's or the affected individual's written consent.
- e. **No Third-Party Beneficiaries.** Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than Agency, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.
- f. **Interpretation.** The provisions of this Addendum shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provisions in this Addendum. The interpretation of this Addendum shall be made under the laws of the state of West Virginia.
- g. **Amendment.** The parties agree that to the extent necessary to comply with applicable law they will agree to further amend this Addendum.
- h. **Additional Terms and Conditions.** Additional discretionary terms may be included in the release order or change order process.

AGREED:

Name of Agency: WV Office of Technology

Name of Associate: SADA Systems, Inc.

Signature: Justin T. McAllister

Signature: Patrick J. Monaghan


Title: Justin T. McAllister-Chief Financial Officer

Title: Patrick Monaghan - Chief Legal Officer

Date: September 23, 2020

Date: 9/22/2020

Form - WVBA-012004  
Amended 06.26.2013

APPROVED AS TO FORM THIS 26<sup>th</sup>  
DAY OF Jan 20 13  
**Patrick Morrisey**  
**Attorney General**  


Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. PHI not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Associate: \_\_\_\_\_

Name of Agency: \_\_\_\_\_

Describe the PHI (do not include any actual PHI). If not applicable, please indicate the same.

**SADA TERMS AND ORDER OF PRECEDENT AGREEMENT**

**EXHIBIT C**

## Software as a Service Addendum

### 1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at <https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN>.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

**Public Jurisdiction** means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

**Public Jurisdiction Data** means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

**Public Jurisdiction Identified Contact** means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

**Restricted data** means personal data and non-public data.

**Security Incident** means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

**Service Provider** means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

**Software-as-a-Service (SaaS)** means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

**2. Data Ownership:** The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

**3. Data Protection and Privacy:** Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

- a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

- b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.
- c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.
- d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.
- e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.
- f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.
- g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
- h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.
- i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

**4. Security Incident or Data Breach Notification:** The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

- a) **Incident Response:** The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.
- b) **Security Incident Reporting Requirements:** The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.
- c) **Breach Reporting Requirements:** Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and the public jurisdiction point of contact for general contract oversight/administration.

**5. Breach Responsibilities:** This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

- a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.



- b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.
- c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.
- d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
- e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

**6. Notification of Legal Requests:** The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

**7. Termination and Suspension of Service:**

- a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.
- b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
- c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:
  - 10 days after the effective date of termination, if the termination is in accordance with the contract period
  - 30 days after the effective date of termination, if the termination is for convenience
  - 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

- d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.
- e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

**8. Background Checks:** The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

**9. Oversight of Authorized Persons:** During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

**10. Access to Security Logs and Reports:** The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

**11. Data Protection Self-Assessment:** The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

**12. Data Center Audit:** The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

**13. Change Control and Advance Notice:** The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

**14. Security:**

- a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

- b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.
- c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

**15. Non-disclosure and Separation of Duties:** The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

**16. Import and Export of Data:** The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

**17. Responsibilities:** The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

**18. Subcontractor Compliance:** The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

**19. Right to Remove Individuals:** The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

**20. Business Continuity and Disaster Recovery:** The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

**21. Compliance with Accessibility Standards:** The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

**22. Web Services:** The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

**23. Encryption of Data at Rest:** The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

**24. Subscription Terms:** Service provider grants to a public jurisdiction a license to:

- a. Access and use the service for its business purposes;
- b. For SaaS, use underlying software as embodied or used in the service; and
- c. View, copy, upload, download (where applicable), and use service provider's documentation.

**25. Equitable Relief:** Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency: WV Office of Technology

Name of Vendor: SADA Systems, inc.

Signature: *Justin T. McAllister*

Signature: *Patrick J. Monaghan*

Title: Justin T. McAllister-Chief Financial Officer

Title: Patrick Monaghan - Chief Legal Officer

Date: September 23, 2020

Date: 9/22/2020

## Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: \_\_\_\_\_

Name of Agency: \_\_\_\_\_

### Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?  
Yes   
No
2. If yes to #1, does the restricted information include personal data?  
Yes   
No
3. If yes to #1, does the restricted information include non-public data?  
Yes   
No
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?  
Yes   
No
5. Provide name and email address for the Department privacy officer:  
Name: \_\_\_\_\_  
Email address: \_\_\_\_\_

### Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:  
Name: \_\_\_\_\_  
Email address: \_\_\_\_\_  
Phone Number: \_\_\_\_\_

**SADA TERMS AND ORDER OF PRECEDENT AGREEMENT**

**EXHIBIT D**



# **Notice of State of West Virginia**

## **Confidentiality Policies and Information Security Accountability Requirements**

### **1.0 INTRODUCTION**

The Executive Branch has adopted privacy and information security policies to protect confidential and personally identifiable information (hereinafter all referred to as Confidential Information). This Notice sets forth the vendor's responsibilities for safeguarding this information.

### **2.0 DEFINITIONS**

- 2.1 Breach** shall mean the acquisition, access, use or disclosure of Confidential Information which compromises the security or privacy of such information.
- 2.2 Confidential Information**, shall include, but is not limited to, trade secrets, personally identifiable information, protected health information, financial information, financial account number, credit card numbers, debit card numbers, driver's license numbers, State ID numbers, social security numbers, employee home addresses, employee marital status, employee maiden name, etc.
- 2.3 Security Incident** means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information.

### **3.0 BACKGROUND**

Agencies maintain Confidential Information, including, but not limited to, trade secrets, personally identifiable information, protected health information, financial information, financial account numbers, credit card numbers, debit card numbers, driver's license numbers, State ID numbers, social security numbers, employee home addresses, etc. Federal laws, including, but not limited to, the Health Insurance Portability and Accountability Act, the Privacy Act of 1974, Fair Credit Reporting Act and State laws require that certain information be safeguarded. In some situations, Agencies delegate, through contract provisions, functions to vendors that involve the vendor's collection, use and/or disclosure of Confidential Information. WV State government must take appropriate steps to ensure its compliance with those laws and desires to protect its citizens' and employees' privacy, and therefore, must require that its vendors also obey those laws.

Utilization of safeguards can greatly minimize potential exposure to sensitive information, and vendors are expected to adhere to industry standard best practices in the management of data collected by, or on behalf of, the State, and in the vendor's possession for a business purpose. Even when sound practices and safeguards are in use, exposures can occur as the result of a

## **Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements**

theft, loss, or compromise of data, or systems containing data. At these times, vendors must be accountable for the loss of data in their possession by ***immediately reporting*** the incident surrounding the loss, and by absorbing any cost associated with the appropriate response actions deemed by the State to be reasonable and necessary. Additional vendor funding may be needed for required activities, such as: rapid notification to affected persons, and provision of a call center to handle inquiries. Notification and call handling will use a State-specified method, format, language, and personnel staffing level.

### **4.0 POLICY**

- 4.1** All vendors for the Executive Branch of West Virginia State government shall sign both the RFP or RFQ, as applicable, and the Purchase Order which contain the confidentiality statement, incident response accountability acknowledgement, and adopt this policy by reference.
- 4.2** Vendors must contact the Privacy Officer of the Agency with which they are contracting to obtain Agency-specific privacy policies, procedures and rules, when applicable.
- 4.3** For vendors' information, Agencies generally require at least the following minimum standards of care in the handling of their Confidential Information:
  - 4.3.1** Confidential Information shall only be used or disclosed for the purposes designated in the underlying contract and at no time shall it be disclosed or used for a personal, non-work or non-contract related reason, unless specifically authorized in writing by the Agency.
  - 4.3.2** In all circumstances, vendors shall have no ownership rights or interests in any data or information, including Confidential Information. All data collected by the vendor on behalf of the Agency, or received by the vendor from the Agency, is owned by the Agency. There are no exceptions to this provision.
  - 4.3.3** In no circumstance shall a vendor use Confidential Information, or data, in any way detrimental to the Agency or to any individual whose records reside in the vendor's control. This prohibition shall not be construed to curtail a vendor's whistleblower rights under Federal and State law. If, in the process of making a good faith report under the provisions of W. Va. Code § 6C-1-1 et seq. or the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), (Pub. L. No. 104-191) as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the Federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA") or any other relevant whistleblower law, a vendor finds it necessary to

## **Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements**

disclose Confidential Information to an appropriate authority in accordance with those statutes, the disclosure will not be treated as a Breach of the Agency's security, privacy or confidentiality policies, as long as the confidential nature of the information is explicitly conveyed to the authorized recipient.

- 4.3.4 The State may periodically monitor and/or audit use of the information systems and other record-keeping systems at a vendor location or a State location in an effort to ensure compliance with this policy. In addition, the State may audit, and require strengthening of, vendor policies and/or practices as they impact security of State data within the vendor's possession.
- 4.3.5 Any collection, use or disclosure of information that is determined by the Agency to be contrary to the confidentiality statement, law or Agency policy may result in termination of the underlying contract.
- 4.3.6 The confidentiality and incident response accountability statement contained within the RFP or RFQ, as applicable, and the Purchase Order shall survive termination of the underlying contract.
- 4.4 If there is an incident that involves theft, loss, or compromise of State Confidential Information, the following reporting and/or actions must be taken by the vendor, on its own behalf, or on behalf of its subcontractor:
  - 4.4.1 If the event involves a theft, or is incidental to another crime, appropriate law enforcement officials shall be notified and a police report generated to document the circumstances of the crime, with a goal to establish whether the crime involved a motive to obtain the sensitive data. A copy of the police report will be forwarded in accordance with 4.4.2.3.
  - 4.4.2 Notification of Breach.
    - 4.4.2.1 Upon the **discovery** of Breach of security of Confidential Information, if the Confidential Information was, or is reasonably believed to have been, acquired by an unauthorized person, the vendor shall notify the individuals identified in 4.4.2.3 immediately by telephone call plus e-mail, web form or fax; or,
    - 4.4.2.2 Within 24 hours by e-mail or fax of any **suspected** Security Incident, intrusion or unauthorized use or disclosure of Confidential Information, in violation of the underlying contract and this Notice, of **potential** loss of confidential data affecting the underlying contract.
    - 4.4.2.3 Notification required by the above two sections shall be provided to:

**Notice of State of West Virginia**  
**Confidentiality Policies and Information Security Accountability Requirements**

(1) the Agency contract manager whose contact information may be found at [www.state.wv.us/admin/purchase/vrc/agencyli.htm](http://www.state.wv.us/admin/purchase/vrc/agencyli.htm) and,  
(2) unless otherwise directed by the Agency in writing, the Office of Technology at [incident@wv.gov](mailto:incident@wv.gov).

**4.4.2.4** The vendor shall immediately investigate such actual or suspected Security Incident, Breach, or unauthorized use or disclosure of Confidential Information. Within 72 hours of the discovery, if an actual Breach has occurred, the vendor shall notify the individuals identified in 4.4.2.3 of the following: (a) What data elements were involved and the extent of the data involved in the Breach (e.g. number of records or affected individual's data); (b) The identity of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or Confidential Information; (c) A description of where the Confidential Information is believed to have been improperly transmitted, sent, or utilized; (d) A description of the probable causes of the improper use or disclosure; and (e) Whether any Federal or State laws requiring individual notifications of Breaches are triggered.

**4.4.2.5** Agency will coordinate with the vendor to determine additional specific actions that will be required of the vendor for mitigation of the Breach, which may include notification to the individual or other authorities.

**4.4.2.6** All associated costs shall be borne by the vendor. This may include, but not be limited to costs associated with notifying affected individuals.

**4.5** The State may require that a vendor provide evidence of adequate background checks, including a nationwide record search, for individuals who are entrusted by the vendor to work with State information.

**4.6** The State requires that any vendor taking possession of State data have comprehensive policies and practices to adequately safeguard that information, and further that the sensitivity of the information is clearly identified and documented in writing, with signed acknowledgement by the vendor that the sensitivity is understood, before it is conveyed to the vendor. Vendor policy should articulate all safeguards in place for the State information, including provisions for destruction of all data, including backup copies of the data, at the end of the vendor's legitimate need to possess the data. All State-owned media containing State information will be returned to the State when no longer legitimately needed by the vendor.

**4.7** All vendor owned devices that contain or transport any State Confidential Information must be encrypted using the AES algorithm, and an industry

**Notice of State of West Virginia**  
**Confidentiality Policies and Information Security Accountability Requirements**

standard methodology. This includes desktop and laptop computers (whole drive encryption – not file encryption), personal digital assistants (PDA), smart phones, thumb or flash-type drives, CDs, diskettes, backup tapes, etc.

**SADA TERMS AND ORDER OF PRECEDENT AGREEMENT**

**EXHIBIT E**

# Google G Suite With West Virginia



## SADA Systems, Inc. MASTER PROFESSIONAL SERVICES AGREEMENT

---

This **MASTER PROFESSIONAL SERVICES AGREEMENT** ("Agreement"), is made and entered into as of date of last signature (the "Effective Date"), by and between SADA Systems, Inc., a corporation organized under the laws of the state of California, with offices at 5250 Lankershim Blvd., Suite 620, North Hollywood, CA 91601 ("SADA"), and The State of West Virginia ("Customer"). SADA and Customer may be referred to in this Agreement individually as a "Party" and collectively as the "Parties."

### 1. BACKGROUND, OBJECTIVES, CONSTRUCTION AND INTERPRETATION

**1.1 Background and Objectives.** This Agreement will serve as a framework under which SADA will provide certain information technology services (the "Services"), as described in Exhibit A (Statement of Work), attached hereto and incorporated herein, and as further requested by Customer from time to time during the term of this Agreement and agreed upon in a Statement of Work (as defined in Section 2.1).

#### 1.2 Definitions.

- (A) Capitalized terms used in this Agreement have the meanings assigned to them in the applicable Section. Terms, acronyms and phrases that are used in the information technology industry or other pertinent business context should be interpreted in accordance with their generally understood meaning in such industries or business context.
- (B) The word "include" and its derivatives (such as "including" and "includes") mean "include without limitation."

#### 1.3 References and Interpretation.

- (A) Headings, captions and titles used in this Agreement are included for convenience only and in no way define the scope or content of this Agreement or are to be used in the construction or interpretation of this Agreement. Any reference to a particular article or section number or exhibit is a reference to that specified article, section or exhibit of this Agreement, except to the extent that the cross-reference expressly refers to another document.
- (B) If there is a conflict or inconsistency between the terms of this Agreement and any Statement of Work, the terms of this Agreement will prevail except to the extent that the Statement of Work specifically and expressly states an intent to supersede specific terms of this Agreement with applicability only to that executed Statement of Work. Notwithstanding the preceding sentence, no Statement of Work will be effective to: (1) expand, eliminate or restrict the scope of any indemnity obligation set forth in Article 11; (2) change any limitation of liability set forth in Article 12; or (3) settle or resolve any dispute between the Parties.

### 2. SCOPE OF SERVICES

**2.1 Provision of Services.** SADA will perform the Services identified in each statement of work entered into and executed by each of the Parties under the terms of this Agreement (each, a "Statement of Work"). Absent a Statement of Work, this Agreement does not, in and of itself, represent a commitment by either Party to provide any minimum amount of charges or services.

**2.2 Statements of Work.** From time to time during the term of this Agreement, Customer may ask SADA to perform services that are not described in a Statement of Work. Following any such request, SADA will prepare and deliver a new statement of work. Each Statement of Work will, at a minimum, contain:



- (A) a description of the work SADA is expected to perform in connection with such project, including a description of any deliverables;
- (B) a prospective schedule for commencing and completing such work; and
- (C) SADA's prospective charges for such work.

If a proposed Statement of Work is mutually acceptable to the Parties, the Parties will execute the Statement of Work. Each Statement of Work will be a separate agreement and, except for any provisions of this Agreement that are specifically excluded or modified in such Statement of Work (subject to Section 1.3(B)), each Statement of Work will incorporate and be subject to all the terms and conditions of this Agreement.

**2.3 Modification of a Statement of Work.** Either Party may request modifications to a Statement of Work by submitting a written change order request to the other Party (each, a "Change Order"). If acceptable to both Parties, the Change Order will be executed by the Parties and will become part of the applicable Statement of Work. Neither Party will not be bound by the terms of any Change Order until it is executed by such Party.

**2.4 Cooperation.** Customer understands SADA's performance is dependent on Customer's timely and effective cooperation, and that the quality of the Services is dependent on Customer providing timely and accurate information to SADA and access to the required Customer resources in accordance with the objectives of the applicable Statement of Work. Accordingly, any delay or nonperformance by SADA will be excused if and to the extent that such delay or nonperformance results from Customer's failure to perform its responsibilities so long as SADA uses commercially reasonable efforts to perform notwithstanding Customer's failure (it being agreed that SADA will have no obligation to incur additional expenses in connection with such efforts unless Customer agrees in writing to reimburse SADA for such expenditures).

### 3. TERM, TERMINATION AND SUSPENSION OF SERVICES

**3.1 Term.** The term of this Agreement will begin on the Effective Date and will continue in effect until the later of (A) three (3) years after the Effective Date, and (B) the expiration or earlier termination of the last remaining Statement of Work, unless extended or terminated earlier in accordance with the terms of this Agreement. The Parties may agree to extend the term by written agreement.

**3.2 Termination for Cause.** If a Party commits: (A) a material breach of this Agreement that is capable of being cured within 30 days after notice of breach from the non-breaching Party, but is not cured within such period, or (B) a material breach of this Agreement that is not subject to cure with due diligence within 30 days of written notice thereof, then the non-breaching Party may, by giving written notice to the breaching Party, terminate this Agreement or the applicable Statement of Work, as of a date specified in the notice of termination.

**3.3 Right to Suspend Services.** Without limiting any of its rights under this Agreement, if undisputed invoices under this Agreement are at any time delinquent for 30 days or more, SADA may partially or totally suspend its performance of Services under this Agreement and any Statement of Work, without liability to Customer until such time as Customer brings its account current and provides assurances, reasonably acceptable to SADA, that Customer can and will meet its future payment obligations under this Agreement.

**3.4 Termination for Convenience.** Customer may terminate this Agreement or any Statement of Work for convenience and without cause at any time by giving SADA at least 10 business days' prior written notice designating the termination date.

**3.5 Consequences of Termination.** If this Agreement or any Statement of Work is terminated in accordance with the terms of this Article, SADA will be entitled to receive payment for all Services performed before termination in accordance with the terms of this Agreement or the applicable Statement

of Work, including the cost of any third-party licenses procured for Customer that cannot be canceled. Termination of a Statement of Work will not affect any other Statements of Work then in effect. Termination of this Agreement will result in immediate termination of all Statements of Work then in effect.

#### 4. SADA PERSONNEL

##### 4.1 Oversight and Responsibility.

- (A) SADA will assign an adequate number of SADA personnel to perform the Services. SADA personnel will be properly trained and fully qualified for the Services they are to perform.
- (B) SADA may utilize subcontractors and SADA affiliates to perform the Services, and elements of the Services may be performed from locations outside the United States.
- (C) SADA will be responsible for the appropriate oversight and supervision of all SADA employees and any subcontractors who perform Services hereunder, each considered "SADA personnel" for purposes of this Agreement. SADA will remain responsible for any Services performed by subcontractors to the same extent as if SADA performed such Services itself.

**4.2 Non-Solicitation.** From the effective date of the applicable Statement of Work until 12 months after completion of its obligations under such Statement of Work, a Party will not directly or indirectly solicit or seek to procure (other than by general advertising), without the prior written consent of the other Party, the employment of: (A) in the case of Customer, SADA's employees engaged in the provision of the Services under such Statement of Work; and (B) in the case of SADA, any Customer employees engaged in activities related to the Services, unless, in either case, such employee has resigned from working for or been terminated by the applicable Party.

#### 5. PROPRIETARY RIGHTS

**5.1 Customer IP.** As between Customer and SADA, all right, title and interest in and to Customer IP (as defined below) will remain the exclusive property of Customer. To the extent necessary to provide the Services, Customer hereby grants SADA, solely to provide the Services, a non-exclusive, non-transferable, fully paid-up and royalty-free, limited right to access and use Customer IP; provided that the rights granted to SADA hereunder will automatically expire effective upon the date that SADA ceases, for any reason, to provide the applicable Services. For purposes of this Agreement, "Customer IP" means (A) software and tools, (B) processes, procedures and methodologies, (C) formulas, templates and formats, and (D) documents and other written materials, whether proprietary to Customer or licensed to Customer from third parties (other than SADA), that are provided to SADA by Customer in order for SADA to provide the Services and fulfill its obligations under this Agreement.

##### 5.2 SADA IP.

- (A) As between SADA and Customer, all right, title and interest in and to SADA IP (as defined below) will remain the exclusive property of SADA. Except to the extent that the Parties enter into separate license agreements with respect to any software or other products provided by SADA (in which case such products will be governed by the terms of those license agreements), SADA hereby grants to Customer a perpetual, non-exclusive, worldwide, fully paid-up and royalty-free license to access and use (and to allow third parties to access and use solely for the benefit of Customer) the SADA IP, for no additional consideration to the extent necessary to receive or use the Services or any deliverable. Notwithstanding the foregoing, if a Statement of Work: (i) provides for Services and deliverables to be provided to Customer on a trial or pilot basis, Customer's license to access and use any SADA IP necessary to receive or use the Services or deliverables provided as part of such trial or pilot will not be perpetual, but will be limited to the period of such trial or pilot, or (ii) includes the purchase of a license to use a SADA proprietary product for a specific period of time,

Customer's license to use such product will not be perpetual, but will be limited to the period set forth in the applicable Statement of Work.

- (B) Nothing in this Section will be construed to grant Customer any right to separate SADA IP from the deliverable into which it is incorporated and Customer will not (and will not knowingly allow any third party to) adapt, modify, translate, reverse engineer, decompile, disassemble or attempt to decode or disassemble any source code or underlying algorithms of any SADA IP or part thereof. Customer will not sell, rent, lease, sublicense, license, lend, market or commercially exploit such SADA IP or use SADA IP for the benefit of any party not contemplated by the applicable Statement of Work, or assign or transfer any rights with respect to SADA IP granted under this Agreement (except as contemplated in Section 14.2).
- (C) For purposes of this Agreement, "SADA IP" means (i) software, code, and tools, (ii) processes, procedures and methodologies, (iii) formulas, templates and formats, and (iv) documents and other written materials, whether proprietary to SADA or licensed to SADA from third parties (other than Customer or its affiliates) that are used to provide the Services, together, in each case, with any modifications or enhancements thereto and derivative works based thereon. Customer acknowledges and agrees that with respect to any SADA IP licensed to SADA from third parties, any rights granted to Customer hereunder or under any Statement of Work, will be subject to all restrictions set forth in the applicable third-party agreements.

**5.3 Developed Property and Works for Hire.** Subject to Section 5.2, SADA acknowledges and agrees that Customer will have all right, title and interest in and to all Developed Property (as defined below) developed while providing the Services. All Developed Property developed under this Agreement in accordance with the terms of a Statement of Work will be deemed to be "works for hire." To the extent any Developed Property is not deemed "works for hire" by operation of law, SADA hereby irrevocably assigns, transfers and conveys to Customer, without further consideration, all of its right, title and interest in and to such Developed Property (including all patent, copyright, trademark, trade secret and other intellectual property and proprietary rights). SADA will execute any documents or take any other actions as may be reasonably necessary, or as Customer may reasonably request, to perfect the ownership rights defined in this Section. For purposes of this Agreement, "Developed Property" means intellectual property generated or developed specifically for Customer by SADA under a Statement of Work and paid for by Customer. To qualify as Developed Property under this Agreement, such intellectual property must be explicitly and specifically called out in a Statement of Work and such Statement of Work must include a written acknowledgement by SADA that the Parties intend to transfer the rights to such intellectual property to Customer upon payment by Customer.

**5.4 Residual Knowledge.** Nothing in this Agreement will restrict a Party from using Services-related ideas, concepts, know-how, methodologies, processes, technologies, algorithms or techniques that are general in nature and retained in the unaided mental impressions of the Party's personnel, which either Party, individually or jointly, develops or discloses under this Agreement; provided that, in doing so, each Party does not breach its obligations under Article 7 or infringe the intellectual property rights of the other Party or third parties who have licensed or provided materials to the other Party. The Parties acknowledge SADA has the right to: (A) provide consulting or other services of any kind or nature to any person or entity as SADA, in its sole discretion, deems appropriate, and (B) use any works of authorship or other intellectual property included in the deliverables (other than Developed Property, if any) to develop for itself, or for others, materials or processes similar to those contemplated or produced under this Agreement.

(A) **Reserved.**

## 6. CONFIDENTIALITY

**6.1 Disclosure of Confidential Information.** The Parties agree that during SADA's performance of the Services, each Party may access, receive or exchange information that is confidential in nature. For purposes of this Agreement "Confidential Information" will include all information, in any form, furnished or made available, directly or indirectly, by one Party ("Disclosing Party") to the other Party ("Recipient") that

is marked confidential, restricted, or is otherwise designated as confidential. Confidential Information will also include information that, by virtue of the nature of the information or the circumstances surrounding disclosure, a reasonable party would understand to be proprietary to Disclosing Party or confidential, including without limitation: (A) any personally identifiable information or financial information of any individual; (B) information concerning the operations, affairs and business of a Party, a Party's financial affairs, or a Party's relations with its customers and employees; (C) in the case of Customer, Customer IP; and (D) in the case of SADA, SADA IP.

**6.2 Exclusions.** Confidential Information does not include, and this Article does not apply to, information that (A) is or subsequently becomes published or available to the public through no fault of Recipient, (B) is received by Recipient from a third party without a duty of confidentiality; (C) is independently developed by Recipient without reference to Disclosing Party's Confidential Information, or (D) was in Recipient's possession or was known to Recipient before it was disclosed to Recipient by Disclosing Party.

**6.3 Restrictions on Disclosure and Use.** The Parties agree:

- (A) Neither Party will make any use of the other Party's Confidential Information or any copies thereof, for any purpose other than those contemplated by this Agreement.
- (B) Neither Party will reveal, disclose or provide access to the other Party's Confidential Information to any third party without the prior consent of such Party, provided that both Parties may share Confidential Information with their responsible employees who have a need to know such Confidential Information to perform their duties. Customer understands that all materials provided to Customer by SADA are provided solely for Customer's internal use. Notwithstanding anything to the contrary in this paragraph, SADA may disclose Confidential Information to properly authorized entities as and to the extent necessary for performance of the Services, so long as in each such case, the receiving entity first agrees to the obligations described in this Article.
- (C) Recipient will take security precautions at least as great as the precautions Recipient takes to protect its own confidential information, and at any rate will take commercially reasonable security precautions to ensure that no one, other than a person authorized pursuant to this Section, gains access to Disclosing Party's Confidential Information without Disclosing Party's prior written consent. If Recipient becomes aware of any unauthorized use or disclosure of Disclosing Party's Confidential Information, Recipient will promptly notify Disclosing Party of such unauthorized use or disclosure and will assist Disclosing Party in remedying such unauthorized use or disclosure.
- (D) Recipient is permitted to disclose Confidential Information as required by law, regulation or subpoena, provided that Recipient will, to the extent permitted by law: (i) give Disclosing Party prompt notice of any such requirement, which notice must be sufficient to permit Disclosing Party to seek relief to prevent such disclosure, (ii) cooperate with Disclosing Party to secure confidential treatment of the Confidential Information, and (iii) disclose only that portion of Disclosing Party's Confidential Information that is legally required.
- (E) Confidential Information is and will remain the exclusive property of Disclosing Party. Each Party agrees that it will have no proprietary interest in the other Party's Confidential Information and that nothing contained in this Agreement will be construed to grant either Party any rights, by license or otherwise, to any of the other Party's Confidential Information disclosed pursuant to this Agreement.
- (F) The obligations set forth in this Section will apply to Confidential Information provided, furnished or otherwise disclosed by Disclosing Party to Recipient, whether before or after the Effective Date.

**6.4 Controlling Provisions.** For purposes of this Agreement, and each Statement of Work, the provisions of this Article will have precedence over and supersede any confidentiality or non-disclosure agreement executed by the Parties before the Effective Date.

## 7. DATA PROTECTION

**7.1 Data Protection Legislation.** In performing the Services, SADA will comply with, and will ensure that all SADA personnel comply with, the data protection and privacy legislation, guidelines and industry standards applicable to the Services including, if applicable to the data involved, 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, repealing Directive 95/46/EC (“GDPR”) (such applicable legislation, guidelines and industry standards, “Data Protection Laws”). SADA will not, by any act or omission on SADA’s part, place Customer in breach of any applicable Data Protection Laws. For purposes of this Article, the terms “processing” and “personal data” will have the meanings given in the GDPR. To the extent that the GDPR applies to any personal data processed by SADA, in that the personal data applies to data subjects who are in the European Economic Area (“EEA”) and the processing activities relate to activities identified in Article 3 of the GDPR, the Parties agree that Customer is the “controller” of such data and SADA is acting as a “processor” of such data, as such terms are defined in the GDPR.

**7.2 Processing of Personal Data.** If the Services involve the processing by SADA of personal data on behalf of Customer, SADA will:

- (A) process personal data provided by or on behalf of Customer only as needed to perform its obligations under this Agreement and the applicable Statements of Work and to provide the Services, and will comply with, and only act on, instructions from or on behalf of Customer regarding the processing of that personal data;
- (B) impose a duty of strict confidentiality on any SADA personnel authorized to access or process personal data;
- (C) implement appropriate technical and organizational safeguards to ensure a level of security appropriate to the risk to personal data and protect the personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access; and
- (D) at Customer’s discretion, evidenced by Customer’s written request, delete or return all such personal data to Customer upon termination or expiration of this Agreement, or following the conclusion of the Services related to processing such personal data, and delete any existing copies, unless otherwise required by applicable law.

**7.3 Processing by Subcontractors.** SADA will ensure that any subcontractor engaged by SADA that may access or process personal data provided by or on behalf of Customer only uses such personal data in accordance with the terms of this Agreement and has entered into an agreement with SADA that contains provisions at least as protective of Customer’s personal data as those set forth in this Article. SADA will remain fully liable to Customer for the performance of its subcontractors’ obligations.

**7.4 Breach.** SADA will promptly inform Customer of any suspected or confirmed data protection breaches or unauthorized or unlawful processing, loss or destruction of, or damage to, personal data impacting Customer, any such notice to be provided within 72 hours after SADA becomes aware of such event, which notice will describe the nature of the breach and the measures taken or proposed to be taken to address such breach.

**7.5 Additional Provisions under the GDPR.** In the case of personal data for which Customer is the data controller and the provisions of the GDPR apply to SADA’s processing of such data (if, for example, the processing by SADA (i) is carried out in the context of the activities of an establishment of Customer in the EEA or (ii) the personal data relates to data subjects who are in the EEA and the processing relates to the offering to them of goods or services in the EEA or the monitoring of their behavior in the EEA), SADA will:

- (A) process personal data in relation to which Customer is the data controller only in accordance with specific documented instructions from or on behalf of Customer, including as set forth in this Agreement and any Statements of Work, unless otherwise required by applicable European Union or European Member State law (in which case, SADA will inform Customer of such legal requirement, unless that law prohibits such disclosure on important grounds of public interest);
- (B) obtain prior consent to engage any third party (including subcontractors) to process such personal data on behalf of Customer, ensure that such third-party subcontractor is subject to the provisions set forth in Section 8.3, and inform Customer of any intended changes concerning the addition or replacement of such third parties, giving Customer the opportunity to object to such changes;
- (C) taking into account the nature of the processing, assist Customer, through appropriate technical and organizational measures (insofar as possible), in meeting its obligations under applicable law to respond to requests for exercising the data subject's rights;
- (D) assist Customer in ensuring compliance with any applicable obligations under the GDPR related to security, breach notification, data impact assessments and prior consultation with the supervisory authorities, taking into account the nature of processing and the information available to SADA;
- (E) provide relevant information and assistance, as reasonably requested in writing by Customer, to demonstrate SADA's compliance with its obligations imposed by this Agreement with respect to such personal data, and allow for and cooperate with privacy and security audits, including inspections, conducted by Customer or another auditor designated by Customer (any such audits to be conducted during SADA's normal business hours at upon no less than thirty (30) days' prior written notice); and
- (F) not transfer personal information from a country located in EEA to a country outside the EEA unless Customer has consented to such transfer and such transfer is pursuant to an appropriate data transfer mechanism or agreement that complies with applicable law.

**7.6 Processing by Third Parties.** For purposes of clarification, the provisions of this Article only apply to any processing of personal data by SADA on behalf of Customer. Customer hereby agrees and acknowledges that SADA is not responsible or liable for any processing of personal data that may be done by third parties in connection with any third-party software, applications or other products, even if the Services contemplate Customer's use of such third-party software, applications or other products.

## 8. REPRESENTATIONS, WARRANTIES AND COVENANTS

**8.1 Authorization.** Each Party represents and warrants to the other that: (A) it has the requisite corporate power and authority to enter into this Agreement and to carry out the transactions contemplated by this Agreement; and (B) the execution, delivery and performance of this Agreement and the consummation of the transactions contemplated by this Agreement have been duly authorized by the requisite corporate action on the part of such Party.

**8.2 Performance of Services.** SADA represents, warrants and covenants to Customer that the Services will be performed by qualified personnel with promptness and diligence in a workmanlike manner, consistent with applicable industry standards.

**8.3 Viruses and Disabling Code.** SADA will use commercially reasonable efforts to prevent the coding or introduction of viruses, disabling code or similar items into Customer systems by SADA or its agents; and SADA will, in the event a virus, disabling code or similar item is found to have been introduced into any software deliverables or Customer systems by SADA or its agents, at no additional charge, assist Customer in reducing the effects of the virus, disabling code or similar item.

**8.4 Disclaimer.** OTHER THAN AS PROVIDED IN THIS AGREEMENT, NEITHER PARTY PROVIDES ANY EXPRESS WARRANTIES OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY

IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN ADDITION, SADA MAKES NO EXPRESS OR IMPLIED WARRANTIES RELATING TO THIRD-PARTY PRODUCTS OR SERVICES.

**8.5 Limited Warranty.** If any implied warranties, guarantees or conditions implied by local law cannot be waived, then any such implied warranties are limited in duration to 90 days from delivery of the applicable Service or deliverable.

## 9. INSURANCE

During the term of this Agreement, SADA will keep in force the following insurance coverage with insurers having an A.M. Best rating of A-, VIII or better:

- Workers Compensation as required by statute and Employers' Liability with \$1,000,000 per accident, \$1,000,000 disease policy limit, and \$1,000,000 disease per employee.
- Commercial General Liability with \$1,000,000 per occurrence and \$2,000,000 aggregate.
- Professional Liability/Errors & Omissions with \$5,000,000 per occurrence and \$5,000,000 aggregate, including information security coverage with \$1,000,000 per occurrence/aggregate.
- Employment Practices Liability with \$1,000,000 per occurrence/aggregate.
- Excess Liability or Umbrella Liability with \$6,000,000 per occurrence and \$6,000,000 aggregate.

## 10. INDEMNIFICATION

**10.1 By SADA.** SADA agrees to indemnify, defend, and hold Customer harmless from and against all losses, liabilities, damages, and related costs (including settlement costs and reasonable attorneys' fees) (collectively, "Losses") arising out of a third-party claim that any SADA IP or deliverables infringe or misappropriate any patent, copyright, trade secret or trademark of a third party. Notwithstanding the foregoing, in no event will SADA have any obligations or liability under this Section arising from: (A) use of any deliverable in a modified form or in combination with materials not furnished or approved by SADA, (B) use by Customer or its agents of any deliverable in a manner not reasonably consistent with the applicable specifications, requirements or instructions for such item, (C) compliance with Customer's design or request for customized features; or (D) any content, information or data provided by Customer or other third parties.

**10.2 By Customer.** Customer will indemnify, defend and hold SADA harmless from and against all Losses arising out of (A) a third-party claim that Customer IP or other materials provided to SADA by Customer infringe or misappropriate any patent, copyright, trade secret or trademark of a third party; (B) any deficiency (including penalties and interest) relating to taxes that are the responsibility of Customer; or (C) a third-party claim arising out of or relating to SADA's use of any Customer content, provided such use complies with the terms of this Agreement.

**10.3 Infringement.** If any deliverable becomes, or in SADA's reasonable opinion is likely to become, the subject of an infringement or misappropriation claim or proceeding, SADA will, at its expense: (A) secure the right to continue using the deliverable; (B) replace or modify the deliverable to make it non-infringing, provided that any such replacement or modification will not degrade the performance or quality of the deliverable; or (C) if SADA cannot accomplish either of the foregoing using commercially reasonable efforts, and only in such event, SADA will remove the deliverable and any related charges will be equitably adjusted to reflect such removal.

**10.4 General.** The Party seeking indemnification (the "Indemnitee") will promptly notify the other Party of the claim and cooperate with the indemnifying Party in defending the claim. The indemnifying Party will have full control and authority over the defense, provided that: (A) any settlement requiring the Indemnitee to admit liability, pay any money, or take (or refrain from taking) any action, will require the Indemnitee's

prior written consent, such consent not to be unreasonably withheld or delayed; and (B) the Indemnitee may join in the defense of a claim with its own counsel at its own expense. THE INDEMNITIES PROVIDED IN THIS ARTICLE ARE THE ONLY REMEDY UNDER THIS AGREEMENT FOR VIOLATION OF A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS.

## 11. LIABILITY

### 11.1 Limitation of Liability.

- (A) IN NO EVENT WILL EITHER PARTY BE HELD LIABLE UNDER THIS AGREEMENT FOR SPECIAL, INDIRECT, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF DATA, BUSINESS INTERRUPTION OR LOST PROFITS), WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHERWISE, EVEN IF SUCH PARTY IS AWARE OF OR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.
- (B) EXCEPT AS PROVIDED IN SECTION 12.2, NEITHER PARTY MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE AGGREGATE AMOUNT PAID OR PAYABLE TO SADA BY CUSTOMER UNDER THE APPLICABLE STATEMENT(S) OF WORK GIVING RISE TO SUCH LOSS (EXCLUDING ANY LICENSE FEES PAID FOR THIRD-PARTY PRODUCTS).
- (C) No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either Party more than one year after the Loss occurred, except that an action for non-payment may be brought within one year of the date of last payment.

**11.2 Exceptions to Limitation of Liability.** The limitations set forth in Section 12.1(B) will not apply to: (A) damages occasioned by a Party's breach of its obligations with respect to the other Party's intellectual property rights, (B) Losses that are the subject of indemnification obligations under this Agreement, or (C) Losses determined to be the direct result of a Party's gross negligence or intentional or willful misconduct.

## 12. FORCE MAJEURE

No Party will be liable for any default or delay in the performance of its obligations under this Agreement if and to the extent such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or other acts of God, riots, civil disorders, acts of terrorism, or any other similar cause beyond the reasonable control of such Party. Any Party so delayed in its performance will promptly notify the Party to whom performance is due by telephone (to be confirmed in writing within five days of the inception of such delay) and describe at a reasonable level of detail the circumstances causing such delay.

## 13. DISPUTE RESOLUTION AND GOVERNING LAW

All claims, disputes or controversies arising out of or relating to this Agreement, including disputes relating to the interpretation of any provision of this Agreement or any Party's performance or breach hereunder, will be resolved as set forth in this Article. All negotiations pursuant to this Article will be confidential and will be treated as compromise and settlement negotiations for purposes of the applicable rules of evidence.

**13.1 Dispute Resolution and Arbitration.** In the event of a claim, controversy or dispute, the Parties will consult and negotiate with each other and, recognizing their mutual interests, attempt to reach a satisfactory solution. If the Parties cannot reach settlement within a period of 60 days, then either Party may, upon notice to the other Party, request that the unresolved dispute be settled by binding arbitration conducted in Los Angeles, California by the American Arbitration Association ("AAA") in accordance with its Commercial Arbitration Rules (the "AAA Rules"), provided that notwithstanding any contrary provision within the AAA Rules, the arbitrator must determine the rights and obligations of the parties according to the substantive laws of the state of California. The Parties will select an arbitrator, who will be an attorney with at least 10 years' experience in commercial and contract law, provided that if the amount in dispute is



greater than \$500,000, the dispute will be heard by a panel of three arbitrators, with each party selecting one arbitrator and the AAA selecting the third arbitrator. If the Parties are unable to agree on an arbitrator(s), the arbitrator(s) will be selected according to AAA Rules. Each Party will bear its own expenses and will share equally the fees of the arbitrator(s), provided that the arbitrator(s) will have the discretion to award the prevailing Party all or part of its attorneys' fees and costs, including the costs of the arbitrator(s), if the arbitrator(s) find that the position taken by the other Party on material issues was without substantial foundation. The arbitrator(s) will not have the power to add to, subtract from or modify any of the terms or conditions of this Agreement. The arbitrator(s) rendering judgment upon disputes between the Parties will deliver a written opinion within 15 business days following conclusion of the hearing, setting forth findings of fact, conclusions of law and the rationale for the decision. Any award, which may include legal and equitable relief, will be final and binding and judgment may be enforced by any court of competent jurisdiction.

**13.2 Equitable Relief.** Notwithstanding the foregoing, if a Party determines, in good faith, that a breach or threatened breach of the terms of this Agreement by the other Party would result in irreparable harm, such that a temporary restraining order or other form of injunctive relief is the only appropriate and adequate remedy, such Party may proceed directly to court and may obtain such relief without bond (if permitted by law). The Parties further acknowledge and agree either Party may proceed directly to court if the other Party breaches or threatens to breach its obligations under Article 5 (Proprietary Rights), Article 7 (Confidentiality), or Article 8 (Data Protection). If a court of competent jurisdiction should find that a Party has breached or threatened to breach its obligations under either such Article, both Parties agree that, without any additional findings of irreparable injury or other conditions to injunctive relief, the breaching Party will not oppose the entry of an appropriate order compelling performance by the breaching Party and restraining such Party from any further breaches or threatened breaches.

**13.3 Governing Law; Jurisdiction and Venue.** This Agreement will be governed by and construed in accordance with the laws of the state of California, without regard to its choice of law principles. For any litigation that may arise under Section 14.2 of this Agreement or to enforce an award in accordance with Section 14.1, the Parties irrevocably and unconditionally submit to the non-exclusive jurisdiction and venue (and waive any claim of *forum non conveniens*) of the United States District Court for the Central District of California located in Los Angeles or the Los Angeles Superior Court. The Parties further consent to the jurisdiction of any court located within a district that encompasses assets of a Party against which judgment has been rendered for the enforcement of such judgment or award against the assets of such Party.

**13.4 No Limitation on Rights.** Each Party agrees that the provisions contained in this Article do not limit either Party's right to terminate this Agreement as provided in Article 3.

## 14. GENERAL PROVISIONS

**14.1 Notices.** All notices, requests, consents, approvals, acknowledgements and waivers under this Agreement (other than routine operational communications) will be in writing and will be deemed duly given when (A) delivered personally, (B) one day after being given to an overnight courier with a reliable system for tracking delivery (charges prepaid), (C) when sent by electronic mail with a copy sent by another means specified in this Section, or (D) six days after the day of mailing, when mailed by United States mail, registered or certified mail, return receipt requested, postage prepaid and addressed as follows:

If to Customer: State of West Virginia

Attention: Justin T. McAllister, Chief Financial Officer  
Email: justin.t.mcallister@wv.gov  
Phone: 304-957-8184

If to SADA: SADA Systems, Inc.  
5250 Lankershim Blvd., Suite 620  
North Hollywood, CA 91601

Attention: Patrick Monaghan  
Email: [patrick.monaghan@sadasystems.com](mailto:patrick.monaghan@sadasystems.com)  
Fax: (818) 766-0090  
Phone: (818) 766-2400

A Party may change its address or designee for notification purposes by giving the other Party written notice of the new address or designee, and the date upon which it will become effective.

**14.2 Binding Nature and Assignment.** This Agreement is binding on the Parties and their respective successors and assigns. Either Party may assign this Agreement in connection with a merger, change of control, consolidation, or sale or other disposition of all or substantially all of its assets. Any other assignment will be null and void, except with the other Party's prior written consent.

**14.3 Relationship of the Parties.** SADA, in furnishing the Services, is acting as an independent contractor. SADA is not an agent of Customer and has no authority to represent Customer as to any matters, except as expressly authorized in this Agreement or in a Statement of Work.

**14.4 Customer List.** Customer agrees SADA may refer to Customer and use Customer's name in customer lists and other promotional materials.

**14.5 Waiver of Default.** No delay or omission by either Party to exercise any right or power under this Agreement will be construed to be a waiver thereof. A waiver by either Party of any breach or covenant will not be construed to be a waiver of any succeeding breach or of any other covenant.

**14.6 Third Party Beneficiaries and Use of Work.** Neither Party intends this Agreement to benefit or create any right or cause of action in or on behalf of, any person or entity other than the Parties. Customer understands and agrees that Services performed by SADA under this Agreement are intended only for the parties specified in the applicable Statement of Work and may be misleading or inappropriate if used in another context or for another party and agrees not to use any deliverables or documents produced under this Agreement and a Statement of Work for any purpose other than the intended purpose without SADA's prior written consent.

**14.7 Survival.** The provisions of [Section 3.5](#) (Consequences of Termination), [Section 4.2](#) (Non-Solicitation), [Article 5](#) (Proprietary Rights), [Article 7](#) (Confidentiality), [Article 8](#) (Data Protection), [Section 9.4](#) (Disclaimer), [Article 11](#) (Indemnification), [Article 12](#) (Liability), [Article 14](#) (Dispute Resolution and Governing Law) and this Article, as well as any other provision of this Agreement that contemplates performance or observance subsequent to termination or expiration of this Agreement will survive expiration or termination of this Agreement and continue in full force and effect for the period set forth therein, or if no period is set forth therein, indefinitely.

**14.8 Severability.** If any provision of this Agreement is found to be illegal or otherwise unenforceable in any respect, that provision will be deemed to be restated to reflect as nearly as possible the original intent of the Parties in accordance with applicable law. The remainder of this Agreement will remain in full force and effect.

**14.9 Entire Agreement; Amendment and Waiver.** This Agreement and each Statement of Work, including any exhibits referred to herein or therein, each of which is incorporated herein for all purposes, constitutes the entire agreement of the Parties with respect to the subject matter hereof and supersedes all prior agreements, whether written or oral, with respect to the subject matter contained in this Agreement. If Customer requires a purchase order in connection with its invoice, Customer's purchase order terms and conditions will not apply to or modify this Agreement. No change, waiver or discharge will be valid unless made in writing and signed by an authorized representative of the Party against which such change, waiver or discharge is sought to be enforced.

**14.10 Counterparts.** This Agreement may be executed in any number of counterparts, all of which taken together will constitute one single agreement between the Parties.

**IN WITNESS WHEREOF**, this Agreement has been executed by the Parties through their duly authorized officers as of the date set forth above.

SADA Systems, Inc.

State of West Virginia

*Patrick J. Monaghan*

*Justin T. McAllister*

Print name: Patrick J. Monaghan

Print name: Justin T. McAllister

Print title: CLO

Print title: Chief Financial Officer

Date: 09/22/20

Date: September 23, 2020

## G Suite Statement of Work

### Exhibit A to Master Professional Services Agreement

This Statement of Work is entered into in connection with the Master Professional Services Agreement (“Agreement”) by and between SADA Systems Inc. (“SADA”) and **The State of West Virginia** (“Customer”) effective as of the last date of execution by either signatory herein (“Effective Date”). The terms and conditions of the Agreement are incorporated herein by reference. Capitalized terms not defined in this Statement of Work will have the same meaning given to them in the Agreement. This Statement of Work describes certain Services and deliverables that will be provided by SADA to Customer pursuant to the terms and conditions of the Agreement.

### Services Descriptions

The following are product and service descriptions for the items listed in the ‘pricing’ section. Only the items included in the pricing table will be considered within scope.

#### **G Suite Core Product Activation - Enterprise**

SADA will advise on and help with the initial setup of the G Suite Admin Panel to the point that the settings & configurations are ready for any of the G Suite launches. Customer will be equipped to configure and maintain application policies and settings within G Suite in order to meet their unique business needs.

#### *SADA Responsibilities and Deliverables*

- Conduct up to ten (10) ninety minute workshops with the Customer’s designated IT Admin(s) to review activation of core G Suite products, knowledge walkthrough, and sharing of best practices for managing the G Suite Admin Panel
- Guidance in the configuration of email routing rules (including split delivery, if required).
- Advise on and finalize setup of spam settings and virus settings with IT Admin(s).
- Conduct up to four (4) sessions up to two (2) hours on best practices to deploy and manage Chrome Browsers.
- Conduct up to four (4) ninety minute working sessions on network concepts and best practices as they relate to G Suite core services.
- Advise on known best practices and watchpoints for disabling core G Suite applications.
- Advise on Multiple Domain Management best practices, if applicable.
  - This would include assistance with multiple domain configuration, verification completion, and review of applicable best practices and watchpoints
- Guidance on DNS records (MX, CNAME, and A record), including custom web address creation for end user ease of use
- Showcase standard G Suite Admin Panel Roles and advise on custom roles needed.
- Provide best practice security recommendations for administration settings
- Manually provision and assign Admin accounts.

#### *Customer Responsibilities*

- Understanding company application and sharing policies, and if applicable, organization understanding of industry compliance standards
- Understanding necessary admin roles needed to manage the environment from an admin and helpdesk levels.
- Configuring and enabling G Suite policies and settings within the Admin Panel to meet business and compliance standards prior to the launch cycle
- Gaining understanding of the G Suite console to the point of being able to take point post-deployment
- Gathering and providing any/all key applications that are intertwined within the legacy mail platform and/or will be required for G Suite
- Communicating application policy updates to users

- Identifying network limitations and, if needed, updating configurations
- Configuring third party applications, such as provisioning, encryption, single sign on, MDM, etc, required for the roll-out of G Suite, unless otherwise noted in the SOW.

### **Google Vault Enterprise Configuration**

Google Vault allows your organization to manage data retention with a centralized, searchable archive so you can locate data quickly in the event of legal discovery. SADA will partner with Customer Admins and Legal Teams to ensure they are equipped with the Vault best practices, watchpoints, and knowledge in order to maintain and utilize Google Vault post deployment.

#### *SADA Systems' deliverables and responsibilities*

- Conduct up to four (4) ninety minute workshops on Vault Management to Customer Admins. These workshops can cover:
  - How to create default and custom retention rules for mail, drive, and groups
  - Understanding Vault Admin Privileges
- Provision custom Vault Admin Roles with required privileges.
- Provision Vault Admin Role assignments to designated Vault admins
- Conduct up to three (3) ninety minute workshops or working sessions on the Vault Admin Panel to Customer legal admins. These workshops can cover the following:
  - General Google Vault overview
  - How to create legal holds
  - How to search and export data
  - How to share Legal Matters
  - Guidance and assistance in creation of Legal Holds or Legal Matters.

#### *Customer responsibilities*

- Provide privilege requirements for Vault Admin Roles
- Provide list of user emails needing Vault Admin Roles;
  - If multiple Vault Admin Roles exist, Specific Role should be designated.
  - If Vault Admin should only have access to a specific region, Region should be designated.
- Create all required Legal Holds within Google Vault
- Provide written sign-off on Admin Roles and Assignments which SADA implemented and confirmation all Legal Holds have been created by Customer legal team. Sign-off must be provided at least three weeks prior to Core IT Go Live or first Go Live.

### **Provisioning & Lifecycle Management**

#### **Conflict Account Overview and Consultation**

A conflict (or unmanaged) account occurs when a user creates a personal Google account using their work email address. Your organization has now signed up for a managed Google Account and when your admin tries to add those users to your organization's account, they'll have the same address for their personal and work accounts. Two accounts can't share the same email address and must be resolved.

The process outlined below is a key step in successfully provisioning users and must be completed prior to provisioning user accounts in the G Suite tenant.

#### *What is the Agreed Upon Process\**

- All mail domains must be added to G Suite and verified
- Discovery - once all domains are added, are there any conflict accounts?
- Inform - Customer is informed on the implications of available options to resolve accounts
- Decision on resolution path
- Communication sent to end users
- If applicable, conflict accounts resolved

Some steps within this process cannot be updated.

- As the conflict account is defined as a personal account, Google will not provide account details, delete accounts, transfer data, or provide account credentials. The end user is responsible for resolving this conflict if customer chooses this resolution path.
- If Customer decides to resolve conflicts by leveraging the Transfer Tool for Unmanaged Users, provided in the G Suite Admin Panel, Google will send an email directly to the end users. This email cannot be modified.

\*This process can have significant impact to project timeline. User provisioning in the G Suite tenant is dependent on the completion of this project, so the customer should be prepared to work directly with end users to ensure an expeditious resolution.

*SADA Systems' deliverables and responsibilities*

- Conduct up to one (1) 90 minute workshop informing Customer about Conflict Accounts and the options in which to resolve these accounts
- Provide guidance customer on how to use the Transfer Tool for Unmanaged (Conflict) Accounts, available in the G Suite Admin Console.
- Provide targeted communications for identified Conflict Account users

*Customer Responsibilities:*

- Confirm active users identified as Conflict Accounts.
- Confirm and sign off on decision for resolution path.
- Ensure required non-core applications are enabled - such as DoubleClick or Analytics to allow continued use.
- Send custom communications informing Conflict Account users of the decided resolution path.
- Send and Manage Transfer Requests from the Transfer Tool, provided within the G Suite Admin Panel, within expected time frame in order to meet Provisioning milestone
- Sign off that all conflict accounts have been resolved
- Prepare Helpdesk for end user questions and issues

This process does not guarantee the resolution of accounts using other Google services such as Double Click or Analytics. End Users may need to work with Google directly to ensure uninterrupted access to these accounts throughout the provisioning process

**Google Cloud Directory Sync (GCDS)**

Google Cloud Directory Sync (GCDS) runs as a utility in Customer server environment to provide one-way synchronization of LDAP data to G Suite. LDAP will continue to be maintained as the source of truth for all items synchronized. GCDS supports sophisticated LDAP rules for custom mapping of users, groups, non-employee contacts, rich user profiles, aliases, and exceptions.

*What is the Agreed Upon Process*

- Configurations will be created against up to 1 Active Directory domain.
- SADA's process will be as follows:
  - GCDS tool will be installed and verified that it is able to connect to the customer's AD / LDAP server and G Suite environment
  - Up to two (2) 90 minute workshops to include:
    - LDAP Environment Discovery
    - GCDS Tool Workshop
  - Configure GCDS
  - Simulation
  - Implementation
  - One 60 minute Handoff Call

*SADA Systems' deliverables and responsibilities*

- Review customer's LDAP Directory structure

- Build configuration of GCDS to sync only necessary LDAP items.
- Provide a simulation to customer for approval prior to any production syncing.
- Configure a scheduled task to continue ongoing syncs, if desired.
- Provide final Configuration documentation

*Customer Responsibilities:*

- Customer will provide SADA with desired LDAP items to be synced
- Customer will review and approve configuration and simulation sync reports prior to implementation to production

Prior to first workshop, the tool should be installed and verified that it is able to connect to the customer's LDAP server and G Suite environment.

**Lifecycle Management**

SADA will provide lifecycle management guidance for customer admins to successfully make informed decisions during deployment and maintain their environment post-deployment.

This can include the following:

*SADA Systems' deliverables and responsibilities*

- Up to two (2) 60 minute workshops on calendar resource management
- Up to two (2) 60 minute sessions on group management. These can include discussions regarding:
  - Default settings for Google Groups - Email Lists (dependant on creation method)
  - Best Practices and Watchpoints
  - Understanding the additional group settings available
  - If changed, updating the process for the creation of groups and are users aware of the new process?
- Up to two (2) 90 minute sessions on user account management. These can include discussions regarding:
  - Requirements for user data to be kept after deactivation
  - Best practices and Watchpoints when deleting user accounts
- Up to two (2) 60 minute sessions on capability of Command Line tool GAM (Google Apps Manager)

*Customer responsibilities*

- Understand current organization lifecycle management requirements
- Update or add to current documentation to reflect new practices within the G Suite tenant
- Training helpdesk admins in new processes

**Authentication**

Customer shall continue to use current SAML SSO solution. SADA shall consult and assist with the G Suite configuration to allow for use of SSO Solution.

**Mobile Device Management - Mobility Strategy**

Google provides a free, robust application for a variety of mobile devices that allows users to access their G Suite email accounts. SADA will assist with the deployment of mobile device solutions for G Suite by providing up to two workshops to cover:

- Google MDM setup and setup options
- Managed Mobile Apps
- Available Policies
  - Basic vs Advance Policies
  - BYOD vs Company Owned Devices Policies
  - Policy comparison with current MDM Policies, if applicable

- Best Practices for Mobile Offboarding
- Questions from the project team regarding the setup process

Our Enterprise Consultants will work with each customer to tailor a plan in order to introduce new MDM changes to users. This plan may include the following:

#### Consulting Hours

SADA will offer coaching throughout the MDM deployment to help ensure end users are aware of upcoming changes and how to log into G Suite from their mobile devices. This coaching will vary based on the needs of the Customer however, it may include the following.

- Communication & Marketing Strategy Meeting(s)
- Recruiting MDM-Trainers (aka Google Guides)

#### Email Templates

We will work with Customer to create a series of customized email templates that can be sent out to users providing the critical 'who, what, when, where, and why' so that users are knowledgeable about when the change will be occurring and how they need to proceed.

#### End User Documentation

We will work with Customer to create a series of customized end user documentation and instructions so that users are knowledgeable about the mobile set up requirements and steps.

#### Customer Support Enablement

While SADA will assist with the deployment of G Suite, it's important to think about who will be supporting your users at Go-Live and the G Suite platform long-term for your end users. SADA will work closely with Customer to equip their support team with the knowledge to manage G Suite tickets/questions during and post-deployment.

#### *SADA Responsibilities and Deliverables*

- Conduct a Support Kickoff for Customer designated Helpdesk users
- Conduct a Demo of Gmail and Calendar for Customer designated Helpdesk users
- Basic discovery of the existing Helpdesk structure
- Conduct up to three (3) sixty minute workshops with the Customer's designated IT Helpdesk users to review settings and policy decisions in place for core G Suite products, knowledge walkthrough, and sharing of best practices for managing the G Suite Admin Panel depending on their level of access and support
- Provide SADA's G Suite Helpdesk Handouts
- Provide SADA's 1-pager support template

#### *Customer responsibilities*

- Identify and communicate internal escalation path to users for G Suite Issues
- Identify proper Helpdesk/support users for G Suite
- Gather and provide support instructions and project decisions for 1-pager support template

#### Data Migration

##### **SADA Premium Migration**

SADA Systems will deploy and configure data migration tool(s) on the Customer's server that will be used



to transfer data to G Suite. The transfer will use available outgoing bandwidth from the location where the existing data/servers are located.

**What is the Agreed Upon Process**

- Up to 22,000 users will be migrated from O365
- Migration will be for Mail, Calendar, Contact, Tasks, One Drive data within a users account (What Migrates)
- Migrations will be against up to 1 single mail tenant.
- Migrations will be conducted in up to 3 "Go Live Phases"
  - A Go Live Phase is a defined list of users to be migrated or mail flow changes to essentially 'activate' that set of users in G Suite.
  - Weekend Support from any SADA team member will be limited to 4 hours per Go Live Phase
- SADA's process will be as follows:
  - Discovery
  - Setup/Validation
  - Test Migrations
  - Go Live Phase
    - Will repeat up to 3 times according with the number of phases agreed upon
  - Stabilizations
    - Will repeat up to 3 times according with the number of phases agreed upon

Discovery	Setup/Validate	Test Migrations	Go live *	Stabilization*
-----------	----------------	-----------------	-----------	----------------

\*repeats up to 3 times according to the number of phases

**SADA Systems' deliverables and responsibilities:**

- Collect the needed materials and insights into the Source System during the Discovery phase.
- Deploy and configure data migration tool(s) on the Customer's server that will be used to transfer data to G Suite.
- Conduct test migrations according to SADA's lead engineer's findings during discovery.
- Run Go Live Migrations by preparing, starting, and monitoring migration machines during the process.
  - If SADA's lead engineer determines older mail is to run prior to launch, this will only be done in 1 bulk run. If more users are requested to be added, they will need to be part of the bulk migration run during Stabilization (see below)
- Stabilize Go Live migrations by investigating any reported 'missing' data that was part of the planned migration.
  - SADA will run 1 single bulk migration of any 'missed' users during the stabilization and will not conduct more than 1 round per Go Live Phase

**Customer Responsibilities:**

- Customer is responsible for providing migration machines with the specifications listed below, unless otherwise mentioned
- Customer is responsible for enabling forwarding on all user accounts that will be migrated to their destination G Suite account, unless otherwise mentioned.
- Based on the discovery phase, SADA will define a Migration Strategy that will fit best for the customer. Customer is responsible for approving the Migration Strategy prior to moving out of Discovery phase.
- Customer is responsible for populating and managing any user list requested by the Project team, according to the format defined by the SADA team. Failure to deliver accurate lists in a timeline manner will impact schedule and will jeopardize the project success.
- If migrating inactive users, customer is responsible for enabling these users in the source in order to migrate data.

Migration from Archive or local storage (such as PST, OST Archives) is not in scope.

**Migration Machine Specifications:**

64 bit Operating system: Windows 7/Windows 8/Windows 10/Windows Server 2008 R2/2012/2016 (Clean build recommended)

NET Framework 3.5 (for SQL Server Express) and 4.5

Recommended system specification::

- 3GHz 8 Core Processor or better
- 200+GB Disk space
- 16+GB Memory

Number of Machines recommended. 22\*

\*Based on the discovery phase this recommendation can increase.

**\*\*Special Note - SADA does not directly support these services listed below)**

**Google Analytics**

Per email from Analytics support, the Google recommended approach is to use the Analytics management API. This approach will require the partner or Customer to write code using the API to export the data relationships prior to migration and re-create them for the migrated users after the migration.

At least two scripts will be needed: an export script and an import script. The export script saves the data relationships prior to migration to some intermediate data store (local files or cloud). The import script reads the intermediate data store and re-creates the data relationships for the re-created users after the migration

**Google DoubleClick (specifically DoubleClick for Publishers (DFP))**

Per email from DoubleClick support, the Google recommended approach is to have support fix the GAIA IDs after the merge. Specifically:

1. Coordinate with DoubleClick support through a ticket before the merge to minimize the time when users will not have access to DoubleClick data.
2. Delete the users, delete the domain, and wait for the domain to be purged.
3. Re-create the domain and users and migrate the G Suite data as described in the G Suite to G Suite migration documentation.
4. Provide DoubleClick support with the list of users to fix.

**Calendar Resources Migration**

SADA will deploy and configure the migration tool which will be used to transfer the contents of calendar resources to G Suite. The transfer will use available outgoing bandwidth from the location where the existing data/servers are located. G Suite calendar resources support migration of appointments only.

**What is the Agreed Upon Process**

- Up to 4400 calendar resources will be migrated from O365
- Migrations will be for events/appointments within a calendar resource
- Migrations will be against up to 1 single mail tenant.
- Migrations will be conducted in up to 1 "Go Live Phase"
  - A Go Live Phase is a defined list of users to be migrated or mail flow changes to essentially 'activate' that set of users in G Suite.
- SADA's process will be as follows:
  - Discovery
  - Setup/Validation
  - Global Go Live Phase
  - Stabilization

**SADA Systems' deliverables and responsibilities**

- Conduct Discovery with customer by collecting the needed materials and insights into the Source System

- Deploy and configure data migration tool(s) on the Customer's server that will be used to transfer data to G Suite.
- Create 1 batch run of new calendar resources in Google based upon an agreed upon list from the customer.
- Run 1 Go Live Migration by preparing, starting, and monitoring migration machines during the process.
  - Calendar Resource Migration is set to occur at Global Go Live
  - Before Global Go Live, users are expected to continue working in Source platform for these. Issues created due to incorrect bookings must be resolved by end users
- Stabilize Go Live migrations by investigating any reported 'missing' data that was part of the planned migration.
  - SADA will run 1 single bulk migration of any 'missed' calendar resource bookings during the stabilization. These must be part of the planned migration that were missed.

#### *Customer Responsibilities*

- Customer is responsible for populating and managing any list requested by the Project team, according to the format defined by the SADA team. Failure to deliver accurate lists in a timeline manner will impact schedule and will jeopardize the project success.
  - Customer will need to create a file that maps calendar resource email to the email address in G Suite
  - Customer will need to create a file that maps user emails to email address associated to calendar resource in G Suite for permissions.
- Customer is responsible for reviewing and confirming the Default Calendar Resource settings prior to the Global Launch.

#### **Shared Mailbox Consultation and Migration**

Organizations often have shared accounts which are defined as a single account accessible by multiple users. G Suite provides multiple solutions for such use cases including: a form of Google Group - Collaborative Inbox, a delegated user account, a secondary Calendar, or a Calendar Resource. SADA will provide guidance on the proper mapping of shared accounts to the most appropriate solution in G Suite. SADA will help the customer provision accounts to meet their business needs and migrate active data into the new Google solution.

#### *What is the Agreed Upon Process*

- Up to 3800 shared accounts will be migrated in total from O365.
- Migration of data will vary based on final destination decided.
  - Only mail data can be migrated to a Collaborative Inbox
  - Mail, Calendar, and Contact data can be migrated to a delegated account
- Migrations will be against up to 1 source domains.
- Migrations will be against up to 1 mail systems.
- Migrations will be conducted in up to 1 "Go Live Phases"
  - A Go Live Phase is a defined list of users to be migrated or mail flow changes to essentially 'activate' that set of users in G Suite.
  - Weekend Support from any SADA team member will be limited to 4 hours per Go Live Phase
- SADA's process will be as follows:
  - Discovery
  - Inventory & Classification
  - Setup/Validation
  - Go Live Phase
  - Stabilization

#### *SADA Systems' deliverables and responsibilities*

- Conduct up to one (1) ninety minute Shared Account workshops to describe possible G Suite solutions for current Shared Mailboxes.
- Provide a template for the Customer team to inventory critical settings for shared accounts

- Provide guidance, watchpoints, and best practices for mapping legacy accounts to G Suite solutions
- Work with the Customer to identify up to four (4) accounts to provision and test in order to validate mapped Google Solution. Customer must validate and sign off on final solution mapping for all accounts no later than 3 weeks prior to the Global Go Live.
- Provide guidance on provisioning best practices.
- Perform one time provisioning of all groups and/or delegated accounts and access rights based on the completed template provided by the customer per Go Live Phase
- SADA will configure a migration tool hosted on the migration machine(s) provided by the customer
- If required, SADA will migrate any missed or re-mapped shared mailboxes one time during the Global Go Live stabilization period.
- Prior to closing our project, SADA will equip the customer with the skills and knowledge necessary for the continued maintenance of Google Groups

#### *Customer Responsibilities*

- Providing list of all shared accounts including access information, use cases, and account settings (as applicable) in a timely manner
- With guidance from SADA, Customer is responsible for determining appropriate destination and permissions for each account in G Suite
- Finalizing the Group mapping list three weeks before the final Go Live. If the customer decides to perform validation tests for business critical solutions, the customer is responsible for ensuring they have enough time to identify test accounts, collect feedback, and make changes to the mapping list before this deadline. If this deadline is missed, SADA cannot guarantee the accounts will be provisioned or provisioned with the correct settings or access rights prior to Go Live.

#### **Google Vault Archive Migration**

SADA will partner with the customer to ensure their archive data is migrated to G Suite in a desired format and in a timely manner. As a best practice, the archive migration will be completed after all users are already 'live' and working in Gmail. Customer's users will still have access to the archive data on the legacy platform during the migration if needed.

This approach reduces delays and dependencies upon the primary deployment of G Suite to the Customer's users. Take note, archive migrations can take longer than active mail migrations so it's important to ensure access is permitted through the duration.

#### *What is the Agreed Upon Process*

- 22,000 user archives and litigation hold data will be migrated from O365 Online Archives
- Migrations will be directly to either a single destination - either G Suite Vault or to user accounts.
  - This decision must be made for all archives, meaning all archives migrate to G Suite Vault or all archives move to the user's mailbox.
  - If choosing to move data to a user's mailbox, the data will be visible to users and searchable in Vault. Whereas migrating archives directly to Vault makes them only searchable in Vault.
- Migrations will be for mail within the archive
- Migrations will be against up to 1 archive source.
- Migrations will be conducted in up to 1 "Go Live Phase"
  - A Go Live Phase is a defined list of users to be migrated or mail flow changes to essentially 'activate' that set of users in G Suite.
- SADA's process will be as follows:
  - Discovery
  - Setup/Validation
  - Global Go Live Phase

#### *SADA's deliverables and responsibilities*

- Conduct Discovery with customer by collecting the needed materials and insights into the SOURCE System

- Deploy and configure data migration tool(s) on the Customer's server that will be used to transfer data to G Suite.
- Run 1 Go Live Migration by preparing, starting, and monitoring migration machines during the process.
  - Archive migration is set to occur after Global Go Live stabilization

**Customer Responsibilities**

- Customer is responsible for the creation, management, and cleanliness of any and all user lists associated with the migration effort - failure in this area may impact the schedule.
- Customer is responsible for backing up any source data and/or meeting any internal policies set around data integrity.
  - Mail Migrations are not 100% therefore customers must ensure they have suitable means of meeting policies outside of relying solely on migration efforts.
- Customer needs to decide if data to be migrated directly in to mailbox or Google Vault
- Customer must address any corrupted archive data that fails to migrate over
- Customer must decrypt any encrypted Archives or PSTs
- Customer must keep the source system active throughout the entire migration process
- Customer must ensure all users are active in G Suite during the process

**SADA Premium File Migration - User Drives**

SADA Systems will deploy and configure migration tools on the Customer's server that will be used to transfer data to G Suite Team Drive. The transfer will use available outgoing bandwidth from the location where the existing data/servers are located. SADA will consult with Customer on G Suite Team Drive application options and best practices for shared file data. SADA then provides guidance on the mapping of file storage data to the most appropriate solution in G Suite Team Drive. SADA will help the customer provision G Suite Team Drives to meet their business needs and migrate active data into the new G Suite solution.

The supported source platforms of this service are:

**On-Premises Platforms:**

- Network File Systems/SAN/NAS

**What is the Agreed Upon Process**

- Migration of 22,000 user drive data and folders to G Suite My Drive
- Migration will be for files within a shared drive file storage
- Migrations will be conducted in up to 3 "Go Live Phases"
  - A Go Live Phase is a defined list of shared drives to be cutover to a G Suite Team Drive to essentially 'activate' that set of shared drives in their new G Suite Team Drive.
  - Weekend Support from any SADA team member will be limited to 4 hours per Go Live Phase
- SADA's process will be as follows:
  - Discovery
  - Setup/Validation
  - Test Migrations
  - Go Live Phase
    - Will repeat up to 3 times according with the number of phases agreed upon
  - Stabilizations
    - Will repeat up to 3 times according with the number of phases agreed upon

Discovery	Setup/Validate	Test Migrations	Go live *	Stabilization*
-----------	----------------	-----------------	-----------	----------------

\*repeats up to 3 times according to the number of phases

**SADA Systems' deliverables and responsibilities:**

- Collect the needed materials and insights into the Source System during the Discovery phase.
- Based on list populated by Customer, SADA will provision all necessary Team Drives up to one time per Go Live upon list being finalized and locked.
- If needed, SADA will bulk import permissions to Team Drives should the source permissions be deemed invalid or out of date by the Customer.
  - Permissions shall be set in bulk up to one time per Go Live upon this list being finalized and locked
- Deploy and configure data migration tool(s) on the Customer's server that will be used to transfer data to G Suite.
- Conduct test migrations according to SADA's lead engineer's findings during discovery.
- Run Go Live Migrations by preparing, starting, and monitoring migration machines during the process.
  - If SADA's lead engineer determines data should be run prior to launch, this will only be done in 1 bulk run. If more data repositories are requested to be added, they will need to be part of the bulk migration run during Stabilization (see below). A delta migration shall be run at the Go Live cutover.
- Stabilize Go Live migrations by investigating any reported 'missing' data that was part of the planned migration.
  - SADA will run 1 single bulk migration of any 'missed' document repositories during the stabilization and will not conduct more than 1 round per Go Live Phase. This shall include the creation and setting of permissions as necessary.

**Customer Responsibilities:**

- Customer is responsible for providing migration machines
- Based on the discovery phase, SADA will define a Migration Strategy that will fit best for the customer. Customer is responsible for approving the Migration Strategy prior to moving out of Discovery phase.
- Customer is responsible for populating and managing any repository list requested by the Project team, according to the format defined by the SADA team. Failure to deliver accurate lists in a timeline manner will impact schedule and will jeopardize the project success.
- If deemed necessary due to out of date permissions within the Source tenant, Customer is responsible for populating and managing any permissions list requested by the Project team.

**\*Google Drive Limits:**

- Size: Up to 1,024,000 characters, regardless of the number of pages or font size. A document that is converted to Google Docs can be up to 50 MB.
- Size: Up to 5 TB for files uploaded but not converted to Google Docs, Sheets, or Slides.
- 500 files limited per folder.
- maximum file path characters name length is 218
- Permission propagation will take additional time if file structure is four or more levels

NOTE: Your network performance may be impacted during data migration periods. This impact is the result of the bandwidth demands of data migration and the impact should be mentioned in all communications sent to users regarding the transition.

**Migration Machine Specifications:**

64 bit Operating system: Windows 7/Windows 8/Windows 10/Windows Server 2008 R2/2012/2016 (Clean build recommended)

NET Framework 3.5 (for SQL Server Express) and 4.5

Recommended system specification::

- 3GHz 8 Core Processor or better

- 200+GB Disk space
- 16+GB Memory

Number of Machines recommended. 22\*

\*Based on the discovery phase this recommendation can increase.

**SADA Premium File Migration - Shared Drives**

SADA Systems will deploy and configure migration tools on the Customer's server that will be used to transfer data to G Suite Team Drive. The transfer will use available outgoing bandwidth from the location where the existing data/servers are located. SADA will consult with Customer on G Suite Team Drive application options and best practices for shared file data. SADA then provides guidance on the mapping of file storage data to the most appropriate solution in G Suite Team Drive. SADA will help the customer provision G Suite Team Drives to meet their business needs and migrate active data into the new G Suite solution.

The supported source platforms of this service are:

**On-Premises Platforms:**

- Network File Systems/SAN/NAS

*What is the Agreed Upon Process*

- Migration of up to 1 Petabyte of shared drive data and folders to G Suite Shared Drives from up to 200 File Servers
- Migration will be for files within a shared drive file storage
- Migrations will be conducted in up to 2 "Go Live Phases"
  - A Go Live Phase is a defined list of shared drives to be cutover to a G Suite Team Drive to essentially 'activate' that set of shared drives in their new G Suite Team Drive.
  - Weekend Support from any SADA team member will be limited to 4 hours per Go Live Phase
- SADA's process will be as follows:
  - Discovery
  - Setup/Validation
  - Test Migrations
  - Go Live Phase
    - Will repeat up to 2 times according with the number of phases agreed upon
  - Stabilizations
    - Will repeat up to 2 times according with the number of phases agreed upon

Discovery	Setup/Validate	Test Migrations	Go live *	Stabilization*
-----------	----------------	-----------------	-----------	----------------

\*repeats up to 2 times according to the number of phases

*SADA Systems' deliverables and responsibilities:*

- Collect the needed materials and insights into the Source System during the Discovery phase.
- Based on list populated by Customer, SADA will provision all necessary Team Drives up to one time per Go Live upon list being finalized and locked.
- If needed, SADA will bulk import permissions to Team Drives should the source permissions be deemed invalid or out of date by the Customer.
  - Permissions shall be set in bulk up to one time per Go Live upon this list being finalized and locked
- Deploy and configure data migration tool(s) on the Customer's server that will be used to transfer data to G Suite.
- Conduct test migrations according to SADA's lead engineer's findings during discovery.
- Run Go Live Migrations by preparing, starting, and monitoring migration machines during the

process.

- If SADA's lead engineer determines data should be run prior to launch, this will only be done in 1 bulk run. If more data repositories are requested to be added, they will need to be part of the bulk migration run during Stabilization (see below). A delta migration shall be run at the Go Live cutover.
- Stabilize Go Live migrations by investigating any reported 'missing' data that was part of the planned migration.
  - SADA will run 1 single bulk migration of any 'missed' document repositories during the stabilization and will not conduct more than 1 round per Go Live Phase. This shall include the creation and setting of permissions as necessary.

**Customer Responsibilities:**

- Customer is responsible for providing migration machines
- Based on the discovery phase, SADA will define a Migration Strategy that will fit best for the customer. Customer is responsible for approving the Migration Strategy prior to moving out of Discovery phase.
- Customer is responsible for populating and managing any repository list requested by the Project team, according to the format defined by the SADA team. Failure to deliver accurate lists in a timeline manner will impact schedule and will jeopardize the project success.
- If deemed necessary due to out of date permissions within the Source tenant, Customer is responsible for populating and managing any permissions list requested by the Project team.

**\*Google Drive Limits:**

- Size: Up to 1,024,000 characters, regardless of the number of pages or font size. A document that is converted to Google Docs can be up to 50 MB.
- Size: Up to 5 TB for files uploaded but not converted to Google Docs, Sheets, or Slides.
- 400,000 files limited per Google Shared Drive.
- maximum file path characters name length is 218
- Permission propagation will take additional time if file structure is four or more levels

NOTE: Your network performance may be impacted during data migration periods. This impact is the result of the bandwidth demands of data migration and the impact should be mentioned in all communications sent to users regarding the transition.

**Migration Machine Specifications:**

64 bit Operating system: Windows 7/Windows 8/Windows 10/Windows Server 2008 R2/2012/2016 (Clean build recommended)

NET Framework 3.5 (for SQL Server Express) and 4.5

Recommended system specification::

- 3GHz 8 Core Processor or better
- 200+GB Disk space
- 16+GB Memory

Number of Machines recommended. 50\*

\*Based on the discovery phase this recommendation can increase.

**Sharepoint Consultation and File Migration**

SADA Systems will deploy and configure migration tools on the Customer's server(s) that will be used to transfer Sharepoint repository data to Google Drive. The transfer will use available outgoing bandwidth from the location where the existing data/servers are located. SADA will consult with Customer on Google Drive application options and best practices for shared file data. SADA then provides guidance on the mapping of Sharepoint data to the most appropriate solution in G Suite. SADA will help the customer



provision G Suite Shared Drives to meet their business needs and migrate active data into the new G Suite solution.

*Priorities of a Sharepoint Migration*

1. Overview of G Suite Native Mapping Options
2. Inventory of SharePoint Sites and Content
3. Mapping of SharePoint Content
4. Migration of Sharepoint Repository to Google Drive
5. Consultation on Workflows and Site Builds

*Description of Priorities*

1. Overview of G Suite Native Mapping Options  
SADA will provide an overview of mapping options in G Suite that are available as potential replacements to G Suite. This overview will include a review of the options, their capabilities and potential limitations, general use cases, and training on workflows and navigation in the most common mapping options.
2. Inventory of SharePoint Sites and Content  
SADA will work with client resources to inventory all SharePoint Sites into a single master sheet. This information will be collected to assist in mapping existing SharePoint sites to new tools. The process will entail
  - o Assistance in creating a survey process to establish use cases per site.
  - o Direction in information required from source system
  - o Assistance in updating and completing the inventory sheet
  - o Review of inventoried solutions to estimate complexity of mapping process
3. Mapping of SharePoint Content  
SADA engineer and project manager will work with the client project team to analyze SharePoint site use cases and recommend the most appropriate tool per site. The outcome of this process will be a mapping spreadsheet illustrating the recommended mapping option per site. This work effort will include:
  - o Analysis of the inventory sheet by SADA for potential mapping options
  - o Workshops with business leads and site owners to discover additional requirements on high-impact sites; including:
    - Workflows currently in use
    - Any UI/display requirements for data
    - Location and use of files in document libraries
    - Analysis and mapping of metadata associated with list-based files
  - o Summarization of mapping option selected and specific steps to map SharePoint requirements to a G Suite solution
4. Migration of Sharepoint Repository Data  
The supported source platforms of this service are:

**Platforms in Scope:**

- SharePoint Online
- Sharepoint 2013 OnPremise

*What is the Agreed Upon Process*

- Migration of up to 150 Sharepoint Document Repositories and Folders to Google Drive
  - 136 Sharepoint Online
  - 11 Sharepoint 2013
- Migrations will be conducted in up to 2 “Go Live Phases”
  - o A Go Live Phase is a defined list of shared drives to be cutover to a G Suite Team Drive to essentially ‘activate’ that set of shared drives in their new G Suite Team Drive.
  - o Weekend Support from any SADA team member will be limited to 4 hours per Go Live Phase
- SADA’s process will be as follows:

- Discovery
- Setup/Validation
- Test Migrations
- Go Live Phase
  - Will repeat up to 2 times according with the number of phases agreed upon
- Stabilizations
  - Will repeat up to 2 times according with the number of phases agreed upon

Discovery	Setup/Validate	Test Migrations	Go Live *	Stabilization*
-----------	----------------	-----------------	-----------	----------------

\*repeats up to 2 times according to the number of phases

5. Consultation on Workflows and Site Builds

SADA shall provide up to 50 hours of consultation surrounding building google sites and new custom workflows within Google. These hours may be used for the following:

- Google Sites workshops with end users reconstructing team sites.
- Building Google Sites templates for use
- Google Apps Script training sessions
- Google Apps Script working sessions with power users reconstructing workflows

*SADA Systems' deliverables and responsibilities:*

- Collect the needed materials and insights into the Source System during the Discovery phase.
- Based on list populated by Customer, SADA will provision all necessary Team Drives up to one time per Go Live upon list being finalized and locked.
- If needed, SADA will bulk import permissions to Team Drives should the source permissions be deemed invalid or out of date by the Customer.
- Permissions shall be set in bulk up to one time per Go Live upon this list being finalized and locked
- Deploy and configure data migration tool(s) on the Customer's server that will be used to transfer data to G Suite.
- Conduct test migrations according to SADA's lead engineer's findings during discovery.
- Run Go Live Migrations by preparing, starting, and monitoring migration machines during the process.
- If SADA's lead engineer determines data should be run prior to launch, this will only be done in 1 bulk run. If more data repositories are requested to be added, they will need to be part of the bulk migration run during Stabilization (see below). A delta migration shall be run at the Go Live cutover.
- Stabilize Go Live migrations by investigating any reported 'missing' data that was part of the planned migration.
- SADA will run 1 single bulk migration of any 'missed' document repositories during the stabilization and will not conduct more than 1 round per Go Live Phase. This shall include the creation and setting of permissions as necessary.

*Customer Responsibilities:*

- Customer is responsible for providing migration machines
- Based on the discovery phase, SADA will define a Migration Strategy that will fit best for the customer. Customer is responsible for approving the Migration Strategy prior to moving out of Discovery phase.
- Customer is responsible for populating and managing any repository list requested by the Project team, according to the format defined by the SADA team. Failure to deliver accurate lists in a timeline manner will impact schedule and will jeopardize the project success.
- If deemed necessary due to out of date permissions within the Source tenant, Customer is responsible for populating and managing any permissions list requested by the Project team.

**\*Google Drive Limits:**

- Size: Up to 1,024,000 characters, regardless of the number of pages or font size. A document that is converted to Google Docs can be up to 50 MB.
- Size: Up to 5 TB for files uploaded but not converted to Google Docs, Sheets, or Slides.
- 400,000 item limit per Google Shared Drive
- maximum file path characters name length is 218
- Permission propagation will take additional time if file structure is four or more levels

NOTE: Your network performance may be impacted during data migration periods. This impact is the result of the bandwidth demands of data migration and the impact should be mentioned in all communications sent to users regarding the transition.

**Migration Machine Specifications:**

64 bit Operating system: Windows 7/Windows 8/Windows 10/Windows Server 2008 R2/2012/2016 (Clean build recommended)  
 NET Framework 3.5 (for SQL Server Express) and 4.5

Recommended system specification::

- 3GHz 8 Core Processor or better
- 200+GB Disk space
- 16+GB Memory

Number of Machines recommended. 2\*

\*Based on the discovery phase this recommendation can increase.

**Adoption, Consulting, Change Management and Training**

SADA recognizes the critical role training, change management, and overall user adoption plays in a successful project rollout. Our Enterprise Consultants will work closely with each Customer to tailor a comprehensive plan in order to drive user adoption. This plan will include the following:

- Change and Transformation Plan:  
 SADA will work with the Customer to create a comprehensive Change and Transformation Plan for the purpose of having a roadmap to guide all rollout initiatives, activities, communications, etc. This document includes a calendar of events/activities (such as those determined from the G Suite Ambassadors Program, etc.) as well as who will execute (Executive Sponsor, IT, Managers, etc.) and via which vehicle (newsletters, lunch and learn, information booth, etc).
- Custom G Suite Learning and Resource Center:  
 SADA will provide an initial G Suite Learning & Resource Center which utilizes Google Sites technology and can serve as the central repository of information for your end users. Essential training information, tips and tricks, and relevant project information are provided to support the weeks surrounding a G Suite transition. Users will have access to information in a variety of formats including documentation and short training videos.
- Build G Suite Ambassadors Program:  
 SADA will work with the Customer to understand the fundamental value of creating a G Suite Ambassadors program in addition to coaching the Customer through selecting the right team of G Suite Ambassadors, setting roles and expectations, as well as properly onboarding and engaging the G Suite Ambassadors throughout the project lifecycle and beyond.
- Customized Communication Templates:  
 SADA will work with the Customer to highlight the fundamental value of having a communication plan. SADA will work with the Customer to customize SADA's standard communication templates

that can be sent out to their users providing the critical ‘who, what, when, where, and why’ so that users are knowledgeable about when the change will be occurring and how they need to proceed. These communications will be built into the Change and Transformation Plan and sent by the Customer to the appropriate audience.

- Customized End User Documentation Templates:  
SADA will work with the Customer to customize SADA’s standard end user documentation templates including job aids. Documents can be sent out to users and posted on the G Suite Learning and Resource Center providing the critical steps and how-to tips. Documentation aids in preparation and use of G Suite tools.
- Success and Measurement Strategy:  
SADA will work with the Customer to understand the fundamental value of having a Success and Measurement Strategy. We will coach the Customer team through setting attainable and measurable success goals in addition to how those goals will be measured. The data obtained from this strategy can be provided to stakeholders to get a data-driven ROI.
- Adoption Consulting:  
SADA will offer coaching throughout the entire project to help drive successful adoption. This coaching will vary based on the needs of the Customer, however, it may include any of the following.
  - Weekly status meetings
  - Follow up items
  - Change management consulting
- Training:  
SADA allocates the following training:  
46 remote webinars  
26 days (consecutive) onsite training (one trip per Go Live)

Recommended allocations for a 2 rollout project where the first rollout focuses on Email, Calendar, Contacts, and Shared Resource migration and the second rollout focuses on Drive, Shared Drives, and SharePoint migration.

- Rollout 1
  - 20 remote webinars
  - 14 days (consecutive) onsite training (one trip per Go Live)
- Rollout 2
  - 26 remote webinars
  - 12 days (consecutive) onsite training (one trip per Go Live)

*End user Training:*

These sessions may be used towards the services that SADA is deploying and generally include Gmail, Calendar, Drive or other aspects of G Suite as determined by the Customer and/or SADA Trainer. SADA will consult with the Customer to develop a virtual and on site training strategy that meets both budget and logistical needs. Targeted sessions are available for Executive/Administrative Assistants who will have delegated access to a mailbox and/or calendar.

*VIP White Glove:*

Allocated training time may be used to provide white glove support to VIPs and/or their Assistants. This may be 1:1 support or group support. Training sessions are tailored to their unique workflows and needs.

*Train-the-Trainer:*

SADA offers Train the Trainer courses in the form of on site or online webinar-style training sessions, or a combination of both. SADA trainers work with staff to learn the material, and may also offer an outline of the content that can help in preparing the new trainers for their role.

*The availability of onsite resources will be based on both the SADA Travel Policy and travel guidelines related to COVID-19 in place at the time of scheduling, along with Customer and SADA employee discretion. Should we conclude that onsite resources are not available, a change order will be created to convert the remaining onsite days to remote sessions.*

*The Customer will be required to provide in advance its policy related to COVID-19 to ensure alignment with SADA's policy. In the event of policy misalignment, SADA may elect to convert, with client's written authorization, any onsite days with remote webinars.*

- **Training Considerations:**

- **Webinars:**

- All webinars have a minimum of five (5) participants and a maximum of 250 participants.
    - All webinar sessions shall be conducted between the hours of 5:00AM and 6:00PM PT (Pacific Time), Monday through Friday (with the exception of national holidays).
    - Webinars are up to 90 minutes per session, however 60 minute sessions are considered best practice.
    - Upon Customer request, SADA may record webinars. All SADA training is considered intellectual property and should remain limited to the Customer staff only (with no public sharing of the materials in any way).
    - The Customer may choose to convert live webinars into clean recordings. Two (2) webinars will be billed, per clean recording to account for recording, editing, etc.
    - The Customer is responsible for hosting all remote webinars if they choose to use their own platform, tracking registration and attendance.
      - One (1) Customer resource is required to open and moderate each remote webinar in the above platform.

- **Onsite Training Sessions:**

- Onsite training is scheduled for up to eight (8) hours per day during normal business hours of the location where the training occurs. Training will not exceed more than eight (8) hours in a single day, nor will it exceed 5 days in a week.

- Training schedules will be constructed to allow 15 minutes between sessions and a minimum 60 minute lunch break.
        - Recommended onsite training strategy is 3 sessions (up to 90 minutes each) and one "open office" session (up to 105 minutes) for Q&A for all staff.
          - No more than 4 onsite training sessions per day
        - SADA will provide a single resource for onsite training. The Customer may request an additional resource, but it will be at SADA's discretion based on availability and may be subject to additional cost.
        - Onsite training will be done between 8AM - 5PM local time.

- **Additional Change Management Considerations**

- All training must be scheduled three (3) weeks prior to 'Go Live(s)', and completed within four (4) weeks of final 'Go Live' date.
      - Any modifications or cancellations to training sessions (i.e. rescheduling date, or time of training session) must be finalized ten (10) business days prior to the originally scheduled session when travel is required. If travel is not associated with the scheduled session, modifications or cancellations may be made up to five (5) business days prior to the originally scheduled session. Additionally, if no participants log into the webinar after fifteen (15) minutes of the scheduled start time the session will be billed toward the project and deducted from the remaining webinar count.
      - All sessions are conducted in English only.

- All SADA's deliverables will be in the English language. The Customer is responsible to secure translation services, and responsible for the accuracy of all translated items. SADA cannot vet the accuracy of any translated material from the English language to any other language.

### **Ongoing Adoption**

SADA will provide specific deliverables to create a strategy for a successful long term G Suite adoption, starting on the date of Customer's Global Go-Live. This includes a 1-day Executive Envisioning workshop to define ongoing adoption and digital transformation initiatives. The Customer will identify a Lead as their designated contact to work with SADA's Enterprise Consultant. The session shall be held no later than 1 month following the latest Customer Go-Live, and prior to the project close.

Furthermore, SADA will also provide a set of templated communications and tips and tricks for the Customer's Change Management team to customize and leverage over the next 3 months to maximize user adoption.

### Executive Envisioning Workshop

The Executive Envisioning Workshop aims at bringing together people from diverse parts of the business in order for them to discuss pain points and opportunities that others may not be aware of and envision how ongoing adoption of G Suite solutions can alleviate these challenges. Through these types of discussions, our goal is to identify the Customer's vision for Google, outline challenges and how we will measure success from our ongoing efforts. The Customer will be responsible for coordinating the appropriate Executives to attend this workshop.

#### **Deliverables:**

- 60 min. Pre-workshop Information and Planning Meeting
- Workshop invitation template
- Pre-workshop Participant Assessment
- Debrief Document
- High-Level Use Cases
- Draft Vision Statement

### **Project Management**

SADA's assigned Project Manager, along with Customer assigned Project Manager, will be overall responsible for leading the contracted scope of work to completion. Based on established roles and responsibilities, the project management activities will include defining and managing the following core deliverables and activities:

#### *SADA Responsibilities and Deliverables*

- Lead Project Kickoff
- Manage Scope & deliverables
- Define Project Decision Tree and Escalation Process
- Own and maintain the project plan and schedule
- Provide status reporting on a bi-weekly basis
- Ongoing management of Decisions, Risks, Issues, and Change Requests
- Manage budget and identify any changes needed
- Coordinate SADA tasks to completion

#### *Customer Responsibilities*

- Define a client team member that will own client related Project Management activities.
- Attend meetings & coordinate customer tasks to completion in accordance with project timeline/deadlines
- Align internal processes, approvals, and departments (i.e. compliance / internal audit)
- Provide estimates on customer tasks and report on completion progress
- Ensure all additional customer required activities are managed in the project plan
- Identify, and facilitate project escalations and customer risks collaboratively working to resolve

- challenges
- Manage customer resource allocation
- Communicate any internal (customer) changes, outages, decisions or other impacts to project activities

In addition, SADA's Project Management team will serve as an advocate for best practices throughout the Project life cycle for in scope work.

### **Scheduling Tool**

SADA Project Manager will be utilizing Smartsheet to build and manage the project plan. If a Client user needs access to manage the schedule along with the SADA Project Manager, the Client will be responsible to furnish a license to Client users.

In the event the Client would like for SADA Project Manager or SADA team members to use a different tool, Client agrees to furnish SADA resources with the necessary licenses and access rights to the Client preferred tool.

### **Project Kickoff**

Once the SOW has been signed, within the first week, a SADA Project Manager is assigned along with technical and adoption leads, as it pertains to in-scope services.

The assigned Project Manager will contact Customer to schedule an 'Introduction Call', during which the Customer is provided with the 'Environment Sheet' as a prerequisite for the project 'Kick-off', as well as, confirming the resources and roles that are needed from the Customer's end. Without the 'Environment Sheet' being reviewed, completed and sent back to SADA for review, and without all the Customer resources being identified and made available to engage on the project, a project Kick-off date cannot be confirmed by SADA delivery team.

A remote project kickoff is typically 90 minutes, it establishes a mutual understanding of the project before development or deployment work officially begins. Standard agenda:

- Team member introductions from both SADA and Customer project teams.
- Project roles and responsibilities are clearly defined.
- Project expectations, timeline, and deliverables are set.
- Review of all documentation, prerequisites, and objectives for the project.
- Project requirements, objectives, and goals are refined or revised as needed.
- Next steps and project milestones are clearly defined.

Project Kick off required attendees from Customer project team:

- Project Manager
- Technical Lead
- Executive Sponsor
- Change Management Lead

### **Go-Lives**

According to SADA and Google's Methodology, there are 3 Go-Lives: Core IT, Early Adopters, and Global.

Go-Live dates are set and confirmed post Kick-off, and post a schedule confirmation between both SADA and Customer Project Managers, or the equivalent. When Go-Lives are confirmed, SADA resources are allocated for the specific dates booked.

The customer can request to change an established Go-Live date, at least 2 weeks in advance of Go Live date, but SADA cannot guarantee the next desired date can be accommodated based on resources

availability. In the event where SADA cannot honor the newly desired date, SADA will provide Customer with the next available date the SADA team can execute on the Go-Live activities.

If knowledge transfer is needed between SADA resources in order to accommodate the Customer desired date changes by bringing in different resources, knowledge transfer hours will be billed to the Customer.

Changing Go-Live dates that impact the term expiration date of the SOW can also be accommodated, at cost. Associated cost is to be assessed by SADA and communicated to Customer upon request. Moving a confirmed Go Live date requires a Change Request, and the SADA Project Manager will process a Change Request for said extension and notates the associated cost.



## Pricing and Payment Terms

The applicable charges for Services to be performed under this Statement of work can be found on the corresponding pricing document provided to the State by SHI International Corp. Anything not specified in that document and the above Service Descriptions is not within scope, including the following: (a) the acquisition and implementation of necessary hardware or software required to complete this Project, (b) deployment or support of desktop software, (c) direct end-user assistance of any type, (d) installation or configuration of an internal SMTP relay, (e) migration of PST data, centrally archived data, or encrypted mail, and (f) the removal, uninstallation, retirement, or decommissioning of any elements within the existing messaging platform.

Additional inactive mailbox, shared mailbox, and public folder migrations above the totals listed in the service descriptions above will be subject to a to be determined fee. The State will be invoiced at the following milestones:

Project Scope (items outside of these scoping variables are not included in this SOW)	
Source Data Platform	Office 365, Windows File Shares, Sharepoint Data Repositories
Number of Secondary or Sub Domains	Up to 5
Max Number of Accounts for Data Migration	22,000
Total Data Migration Size Not to Exceed (GB)	Mail: 100 TB , File Shares : 1 PB of data
Migration Type(s) - (Items marked YES are included within the Project Scope)	

	YES	NO
Mail	X	
Calendar	X	
Contacts	X	
Public Folders	X	
Files	X	
Sharepoint Sites Data	X	
Google Drive		X
Shared Mailboxes	X	
Google Groups		X

**Delivery of Services by SADA:**

1. Customer acknowledges that SADA will provide development and deployment services not to exceed the Term for this SOW, 360 days starting from the project kickoff date. If SADA receives no communication from Customer for a 30 day period, SADA will close the project and bill for services rendered.
2. Any contingent Deployment Voucher Discount shown in the Pricing section of this document will be paid to SADA by Google in the form of a credit if Customer attains 50% usage on G Suite, as determined by the G Suite Admin Control Panel report covering any 30-day period during the first year of Customer's G Suite service. If Customer does not meet this 50% usage threshold within first year of service, an amount equal to this Deployment Voucher Discount will be invoiced to Customer at the conclusion of such 12-month period and Customer will be responsible for paying SADA such amount in accordance with the terms of the Customer Agreement.
3. Customer agrees to the Project Scope data listed in the section above.
4. Customer will provide a single resource who can make decisions to ensure progress can be made on the project without interruptions or delays.
5. Customer acknowledges that project work by SADA cannot begin until all necessary 'deliverables' including hardware, software, and remote access credentials have been provided and verified as working. A detailed list will be provided by SADA upon approval of this SOW.
6. Customer will provide adequate facilities and resources for services rendered by SADA's employees while they are on-site for work authorized by the Customer.
7. Customer agrees to provide direct and unattended VPN network access to complete deployment of tools & services.
8. Customer agrees to the terms and conditions of the Master Professional Services Agreement.

**Hours and Availability**

General project delivery will be from 9 am - 9 pm Eastern, Monday - Friday, excluding national holidays. All SADA support will be provided remotely unless specifically stated as 'on-site.'

**Customer confirms the accuracy of the data and accept the terms and conditions in this section, "Customer Information & Project Scope".**

**Additional Project Information**

**SADA Information**

Role	Name	Responsibilities
Executive Sponsor	Tony Safoian, President/CEO	Executive escalation and support
Sr. Business Development Manager	Mike Kulinski	Responsible for business relations between Customer and SADA. Manages communication on licensing and contractual matters. Serves as Account Manager for Customer upon completion of SOW, offering updates on new releases, Google roadmap, and exploring further opportunities for collaboration.

Project Manager	Assigned upon receipt of all required agreements and deliverables	Drives all workstreams. Coordinates all SADA resources and guides the overall deployment strategy and execution. Shares G Suite best practices. Manages project scope.
Lead Engineer(s)	Assigned upon receipt of all required agreements and deliverables	Technical project lead. Liaison between Customer and Google Support. Provides deep product, application, and integration expertise.
Enterprise Consultants	Assigned upon receipt of all required agreements and deliverables	End-user change management and training lead. Build and execute strategies around end-user communications, training, ambassadors program and ongoing adoption success. Customized end-user communications and curriculum for G Suite training to smooth transition within the organization(s).

The SADA team may include additional resources with specialized skills in additional roles, as necessary to meet project objectives.

**Risks, Issues and Mitigation.**

A **risk** is defined as a potential issue that has not yet occurred. Risks shall be identified as early as possible and categorized according to impact (Low, Med, High, Critical occurrence). SADA will guide the development of a risk mitigation strategy.

An **issue** is a risk that has occurred and presents a challenge to the project. Issues shall be prioritized (Low, Med, High, Critical) and assigned for resolution to the integrated project team.

Risks and issues shall be tracked in an agreed-upon method by both the Customer and SADA, and escalation paths will be specified at project start.

**Project Wrap/Spin Down.**

When the SADA tools and services stated in this statement of work have been implemented and have been demonstrated to work in accordance with the designs set forth in this statement of work, SADA will observe a reasonable period of stabilization and then notify the Customer of project close intentions. Upon presenting this notification to the Customer, the Customer has five (5) working days to notify SADA of any remaining concerns and/or disputed items and what would be required to remove these objections. Project close includes a conference call discussing final items and future support; this call will be followed by SADA sending an official project closed notification to the identified project point of contact for the Customer. All projects are to be closed within four (4) weeks after Global Go Live.

**IN WITNESS WHEREOF**, this Statement of Work has been executed by the Parties through their duly authorized officers as of the date set forth above.

Signatures

**SADA Systems, Inc.**

*Patrick J. Monaghan*

Name: Patrick J. Monaghan

Title: Chief Legal Officer

Date: 09/22/20

**State of West Virginia**

*Justin T. McAllister*

Name: Justin T. McAllister

Title: Chief Financial Officer

Date: September 23, 2020

NASPO ValuePoint  
**PARTICIPATING ADDENDUM**

**CLOUD SOLUTIONS 2016-2026**  
Led by the State of Utah



---

**EXHIBIT C**

# **Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements**

## **1.0 INTRODUCTION**

The Executive Branch has adopted privacy and information security policies to protect confidential and personally identifiable information (hereinafter all referred to as Confidential Information). This Notice sets forth the vendor's responsibilities for safeguarding this information.

## **2.0 DEFINITIONS**

- 2.1 Breach** shall mean the acquisition, access, use or disclosure of Confidential Information which compromises the security or privacy of such information.
- 2.2 Confidential Information**, shall include, but is not limited to, trade secrets, personally identifiable information, protected health information, financial information, financial account number, credit card numbers, debit card numbers, driver's license numbers, State ID numbers, social security numbers, employee home addresses, employee marital status, employee maiden name, etc.
- 2.3 Security Incident** means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information.

## **3.0 BACKGROUND**

Agencies maintain Confidential Information, including, but not limited to, trade secrets, personally identifiable information, protected health information, financial information, financial account numbers, credit card numbers, debit card numbers, driver's license numbers, State ID numbers, social security numbers, employee home addresses, etc. Federal laws, including, but not limited to, the Health Insurance Portability and Accountability Act, the Privacy Act of 1974, Fair Credit Reporting Act and State laws require that certain information be safeguarded. In some situations, Agencies delegate, through contract provisions, functions to vendors that involve the vendor's collection, use and/or disclosure of Confidential Information. WV State government must take appropriate steps to ensure its compliance with those laws and desires to protect its citizens' and employees' privacy, and therefore, must require that its vendors also obey those laws.

Utilization of safeguards can greatly minimize potential exposure to sensitive information, and vendors are expected to adhere to industry standard best practices in the management of data collected by, or on behalf of, the State, and in the vendor's possession for a business purpose. Even when sound practices and safeguards are in use, exposures can occur as the result of a

**Notice of State of West Virginia**  
**Confidentiality Policies and Information Security Accountability Requirements**

theft, loss, or compromise of data, or systems containing data. At these times, vendors must be accountable for the loss of data in their possession by ***immediately reporting*** the incident surrounding the loss, and by absorbing any cost associated with the appropriate response actions deemed by the State to be reasonable and necessary. Additional vendor funding may be needed for required activities, such as: rapid notification to affected persons, and provision of a call center to handle inquiries. Notification and call handling will use a State-specified method, format, language, and personnel staffing level.

**4.0 POLICY**

- 4.1** All vendors for the Executive Branch of West Virginia State government shall sign both the RFP or RFQ, as applicable, and the Purchase Order which contain the confidentiality statement, incident response accountability acknowledgement, and adopt this policy by reference.
- 4.2** Vendors must contact the Privacy Officer of the Agency with which they are contracting to obtain Agency-specific privacy policies, procedures and rules, when applicable.
- 4.3** For vendors' information, Agencies generally require at least the following minimum standards of care in the handling of their Confidential Information:
  - 4.3.1** Confidential Information shall only be used or disclosed for the purposes designated in the underlying contract and at no time shall it be disclosed or used for a personal, non-work or non-contract related reason, unless specifically authorized in writing by the Agency.
  - 4.3.2** In all circumstances, vendors shall have no ownership rights or interests in any data or information, including Confidential Information. All data collected by the vendor on behalf of the Agency, or received by the vendor from the Agency, is owned by the Agency. There are no exceptions to this provision.
  - 4.3.3** In no circumstance shall a vendor use Confidential Information, or data, in any way detrimental to the Agency or to any individual whose records reside in the vendor's control. This prohibition shall not be construed to curtail a vendor's whistleblower rights under Federal and State law. If, in the process of making a good faith report under the provisions of W. Va. Code § 6C-1-1 et seq. or the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), (Pub. L. No. 104-191) as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the Federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA") or any other relevant whistleblower law, a vendor finds it necessary to

## **Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements**

disclose Confidential Information to an appropriate authority in accordance with those statutes, the disclosure will not be treated as a Breach of the Agency's security, privacy or confidentiality policies, as long as the confidential nature of the information is explicitly conveyed to the authorized recipient.

- 4.3.4 The State may periodically monitor and/or audit use of the information systems and other record-keeping systems at a vendor location or a State location in an effort to ensure compliance with this policy. In addition, the State may audit, and require strengthening of, vendor policies and/or practices as they impact security of State data within the vendor's possession.
- 4.3.5 Any collection, use or disclosure of information that is determined by the Agency to be contrary to the confidentiality statement, law or Agency policy may result in termination of the underlying contract.
- 4.3.6 The confidentiality and incident response accountability statement contained within the RFP or RFQ, as applicable, and the Purchase Order shall survive termination of the underlying contract.
- 4.4 If there is an incident that involves theft, loss, or compromise of State Confidential Information, the following reporting and/or actions must be taken by the vendor, on its own behalf, or on behalf of its subcontractor:
  - 4.4.1 If the event involves a theft, or is incidental to another crime, appropriate law enforcement officials shall be notified and a police report generated to document the circumstances of the crime, with a goal to establish whether the crime involved a motive to obtain the sensitive data. A copy of the police report will be forwarded in accordance with 4.4.2.3.
  - 4.4.2 Notification of Breach.
    - 4.4.2.1 Upon the **discovery** of Breach of security of Confidential Information, if the Confidential Information was, or is reasonably believed to have been, acquired by an unauthorized person, the vendor shall notify the individuals identified in 4.4.2.3 immediately by telephone call plus e-mail, web form or fax; or,
    - 4.4.2.2 Within 24 hours by e-mail or fax of any **suspected** Security Incident, intrusion or unauthorized use or disclosure of Confidential Information, in violation of the underlying contract and this Notice, of **potential** loss of confidential data affecting the underlying contract.
    - 4.4.2.3 Notification required by the above two sections shall be provided to:



**Notice of State of West Virginia  
Confidentiality Policies and Information Security Accountability Requirements**

- (1) the Agency contract manager whose contact information may be found at [www.state.wv.us/admin/purchase/vrc/agencyli.htm](http://www.state.wv.us/admin/purchase/vrc/agencyli.htm) and,  
(2) unless otherwise directed by the Agency in writing, the Office of Technology at [incident@wv.gov](mailto:incident@wv.gov).

- 4.4.2.4** The vendor shall immediately investigate such actual or suspected Security Incident, Breach, or unauthorized use or disclosure of Confidential Information. Within 72 hours of the discovery, if an actual Breach has occurred, the vendor shall notify the individuals identified in 4.4.2.3 of the following: (a) What data elements were involved and the extent of the data involved in the Breach (e.g. number of records or affected individual's data); (b) The identity of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or Confidential Information; (c) A description of where the Confidential Information is believed to have been improperly transmitted, sent, or utilized; (d) A description of the probable causes of the improper use or disclosure; and (e) Whether any Federal or State laws requiring individual notifications of Breaches are triggered.
- 4.4.2.5** Agency will coordinate with the vendor to determine additional specific actions that will be required of the vendor for mitigation of the Breach, which may include notification to the individual or other authorities.
- 4.4.2.6** All associated costs shall be borne by the vendor. This may include, but not be limited to costs associated with notifying affected individuals.
- 4.5** The State may require that a vendor provide evidence of adequate background checks, including a nationwide record search, for individuals who are entrusted by the vendor to work with State information.
- 4.6** The State requires that any vendor taking possession of State data have comprehensive policies and practices to adequately safeguard that information, and further that the sensitivity of the information is clearly identified and documented in writing, with signed acknowledgement by the vendor that the sensitivity is understood, before it is conveyed to the vendor. Vendor policy should articulate all safeguards in place for the State information, including provisions for destruction of all data, including backup copies of the data, at the end of the vendor's legitimate need to possess the data. All State-owned media containing State information will be returned to the State when no longer legitimately needed by the vendor.
- 4.7** All vendor owned devices that contain or transport any State Confidential Information must be encrypted using the AES algorithm, and an industry

**Notice of State of West Virginia  
Confidentiality Policies and Information Security Accountability Requirements**

standard methodology. This includes desktop and laptop computers (whole drive encryption – not file encryption), personal digital assistants (PDA), smart phones, thumb or flash-type drives, CDs, diskettes, backup tapes, etc.

NASPO ValuePoint  
**PARTICIPATING ADDENDUM**

**CLOUD SOLUTIONS 2016-2026**  
Led by the State of Utah



---

**EXHIBIT D**

## GOOGLE TERMS AND ORDER OF PRECEDENCE AGREEMENT

THIS GOOGLE TERMS AND ORDER OF PRECEDENCE AGREEMENT, (hereinafter "Terms Agreement") by and between Google LLC (hereinafter "Google") and State of West Virginia (hereinafter "State"), (both referred to as "Parties"), is intended to identify the various documents that comprise the terms agreement between the parties that will govern the purchase of G-Suite products under the State's contract with SHI International Corp. ("SHI") identified as CMA 0212 G-SUITE20.

**NOW THEREFORE**, the Parties hereto hereby agree as follows:

1. **Order of Precedence:** The Terms Agreement is comprised of the documents listed in this section. The terms and conditions contained in the various documents shall be interpreted according to the priority given to the document in this section. In that way, any terms and conditions contained in the first priority document shall prevail over conflicting terms in the second priority document, and so on.

### **Terms Agreement Documents:**

- a. **Google Terms and Order of Precedent Agreement** (this document) – First Priority
- b. **WV-96 Agreement Addendum** (Attached as Exhibit A) – Second Priority
- c. **Google Business Associate Addendum** (As Amended and Attached as Exhibit B) – Third Priority
- d. **Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements** (Attached as Exhibit D) – Fourth Priority
- e. **Google Public Sector Terms of Service – G Suite and Other Google Documents** (Attached as Exhibit E) – Fifth Priority\*

\* The various Google documents will be given the order of priority of sixth or lower as indicated in the various documents.

### **2. Modifications:**

#### **a. Google Documents:**

- i. **Weblinks:** The Parties agree that any clickthrough or weblinked terms are inapplicable to this Terms Agreement unless the weblinked document containing the terms is expressly listed herein. The current versions of Google URL Terms are attached to the Terms Agreement as Attachment A.
- ii. **Additional Product Terms:** The Parties agree that additional products referred to in the Additional Product Terms will not be utilized by the State until such time as those products, and the terms associated therewith have been reviewed and incorporated into the Agreement by change order.
- iii. **G Suite Terms:** Section 6. Marketing and Publicity of the G Suite Terms is removed in its entirety as the State is prohibited by law from endorsing a vendor.

3. **Additional Terms:** The Parties Agree that the following terms and conditions are added to this Terms Agreement.

- a. **PRIVACY, SECURITY, AND CONFIDENTIALITY:** The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in Exhibit D.
- b. **ANTITRUST:** In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.
- c. **BACKGROUND CHECK:** The State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check.

IN WITNESS WHEREOF, the Parties have entered into this Terms Agreement as of the date of the last signature below.

STATE OF WEST VIRGINIA  
Office of Technology

By: Justin T. McAllister  
Name: Justin T. McAllister  
Its: Chief Financial Officer  
Date: September 21, 2020

GOOGLE

By: Philip Schindler 2020.09.16  
Name: Philip Schindler 15:23:01  
Its: Authorized Signatory -07'00'  
Date: \_\_\_\_\_

STATE OF WEST VIRGINIA  
Attorney General's Office

As to Form Only  
By: John S. Gray  
Name: JOHN S. GRAY  
Its: Deputy Attorney General  
Date: September 25, 2020

STATE OF WEST VIRGINIA  
Purchasing Division

By: Frank W. Hales  
Name: Frank W. Hales  
Its: Assistant Director  
Date: 9/25/20



**GOOGLE TERMS AND ORDER OF PRECEDENT AGREEMENT**

**EXHIBIT A**

**STATE OF WEST VIRGINIA  
ADDENDUM TO VENDOR'S STANDARD CONTRACTUAL FORMS**

State Agency, Board, or Commission (the "State"): West Virginia Office of Technology

Vendor: Google

Contract/Lease Number ("Contract"):

Commodity/Service: Google G-Suite

The State and the Vendor are entering into the Contract identified above. The Vendor desires to incorporate one or more forms it created into the Contract. Vendor's form(s), however, include(s) one or more contractual terms and conditions that the State cannot or will not accept. In consideration for the State's incorporating Vendor's form(s) into the Contract, the Vendor enters into this Addendum which specifically eliminates or alters the legal enforceability of certain terms and conditions contained in Vendor's form(s). Therefore, on the date shown below each signature line, the parties agree to the following contractual terms and conditions in this Addendum are dominate over any competing terms made a part of the Contract:

1. **ORDER OF PRECEDENCE:** This Addendum modifies and supersedes anything contained on Vendor's form(s) whether or not they are submitted before or after the signing of this Addendum. **IN THE EVENT OF ANY CONFLICT BETWEEN VENDOR'S FORM(S) AND THIS ADDENDUM, THIS ADDENDUM SHALL CONTROL.**
2. **PAYMENT** – Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software licenses, subscriptions, or maintenance may be paid annually in advance.  
Any language imposing any interest or charges due to late payment is deleted.
3. **FISCAL YEAR FUNDING** – Performance of this Contract is contingent upon funds being appropriated by the WV Legislature or otherwise being available for this Contract. In the event funds are not appropriated or otherwise available, the Contract becomes of no effect and is null and void after June 30 of the current fiscal year. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.
4. **RIGHT TO TERMINATE** – The State reserves the right to terminate this Contract upon thirty (30) days written notice to the Vendor. If this right is exercised, the State agrees to pay the Vendor only for all undisputed services rendered or goods received before the termination's effective date. All provisions are deleted that seek to require the State to (1) compensate Vendor, in whole or in part, for lost profit, (2) pay a termination fee, or (3) pay liquidated damages if the Contract is terminated early.  
Any language seeking to accelerate payments in the event of Contract termination, default, or non-funding is hereby deleted.
5. **DISPUTES** – Any language binding the State to any arbitration or to the decision of any arbitration board, commission, panel or other entity is deleted; as is any requirement to waive a jury trial.  
Any language requiring or permitting disputes under this Contract to be resolved in the courts of any state other than the State of West Virginia is deleted. All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.  
Any language requiring the State to agree to, or be subject to, any form of equitable relief not authorized by the Constitution or laws of State of West Virginia is deleted.
6. **FEEES OR COSTS:** Any language obligating the State to pay costs of collection, court costs, or attorney's fees, unless ordered by a court of competent jurisdiction is deleted.
7. **GOVERNING LAW** – Any language requiring the application of the law of any state other than the State of West Virginia in interpreting or enforcing the Contract is deleted. The Contract shall be governed by the laws of the State of West Virginia.
8. **RISK SHIFTING** – Any provision requiring the State to bear the costs of all or a majority of business/legal risks associated with this Contract, to indemnify the Vendor, or hold the Vendor or a third party harmless for any act or omission is hereby deleted.
9. **LIMITING LIABILITY** – Any language limiting the Vendor's liability for direct damages to person or property is deleted.
10. **TAXES** – Any provisions requiring the State to pay Federal, State or local taxes or file tax returns or reports on behalf of Vendor are deleted. The State will, upon request, provide a tax exempt certificate to confirm its tax exempt status.
11. **NO WAIVER** – Any provision requiring the State to waive any rights, claims or defenses is hereby deleted.



- 12. **STATUTE OF LIMITATIONS** – Any clauses limiting the time in which the State may bring suit against the Vendor or any other third party are deleted.
- 13. **ASSIGNMENT** – The Vendor agrees not to assign the Contract to any person or entity without the State’s prior written consent, which will not be unreasonably delayed or denied. The State reserves the right to assign this Contract to another State agency, board or commission upon thirty (30) days written notice to the Vendor. These restrictions do not apply to the payments made by the State. Any assignment will not become effective and binding upon the State until the State is notified of the assignment, and the State and Vendor execute a change order to the Contract.
- 14. **RENEWAL** – Any language that seeks to automatically renew, modify, or extend the Contract beyond the initial term or automatically continue the Contract period from term to term is deleted. The Contract may be renewed or continued only upon mutual written agreement of the Parties.
- 15. **INSURANCE** – Any provision requiring the State to maintain any type of insurance for either its or the Vendor’s benefit is deleted.
- 16. **RIGHT TO REPOSSESSION NOTICE** – Any provision for repossession of equipment without notice is hereby deleted. However, the State does recognize a right of repossession with notice.
- 17. **DELIVERY** – All deliveries under the Contract will be FOB destination unless the State expressly and knowingly agrees otherwise. Any contrary delivery terms are hereby deleted.
- 18. **CONFIDENTIALITY** – Any provisions regarding confidential treatment or non-disclosure of the terms and conditions of the Contract are hereby deleted. State contracts are public records under the West Virginia Freedom of Information Act (“FOIA”) (W. Va. Code §29B-a-1, et seq.) and public procurement laws. This Contract and other public records may be disclosed without notice to the vendor at the State’s sole discretion.
- 19. **THIRD-PARTY SOFTWARE** – If this Contract contemplates or requires the use of third-party software, the vendor represents that none of the mandatory click-through, unsigned, or web-linked terms and conditions presented or required before using such third-party software conflict with any term of this Addendum or that it has the authority to modify such third-party software’s terms and conditions to be subordinate to this Addendum. The Vendor shall indemnify and defend the State against all claims resulting from an assertion that such third-party terms and conditions are not in accord with, or subordinate to, this Addendum.
- 20. **AMENDMENTS** – The parties agree that all amendments, modifications, alterations or changes to the Contract shall be by mutual agreement, in writing, and signed by both parties. Any language to the contrary is deleted.

Any provisions regarding confidentiality or non-disclosure related to contract performance are only effective to the extent they are consistent with FOIA and incorporated into the Contract through a separately approved and signed non-disclosure agreement.

Notwithstanding the foregoing, this Addendum can only be amended by (1) identifying the alterations to this form by using *Italics* to identify language being added and ~~strikethrough~~ for language being deleted (do not use track-changes) and (2) having the Office of the West Virginia Attorney General’s authorized representative expressly agree to and knowingly approve those alterations.

State: WV Office of Technology  
By: *Justin T. McAllister*  
Printed Name: Justin T. McAllister  
Title: Chief Financial Officer  
Date: September 21, 2020

Vendor: \_\_\_\_\_ 2020.09.16  
By: \_\_\_\_\_ *Philipp Schindler* 15:23:37  
Printed Name Philipp Schindler  
Authorized Signatory =07'00'  
Title: \_\_\_\_\_  
Date: \_\_\_\_\_





**GOOGLE TERMS AND ORDER OF PRECEDENT AGREEMENT**

**EXHIBIT B**

## HIPAA Business Associate Addendum

This HIPAA Business Associate Addendum ("**BAA**") is entered into between Google LLC ("**Google**") and the customer agreeing to the terms below ("**Customer**"), and supplements, amends and is incorporated into the Services Agreement(s) (defined below) solely with respect to Covered Services (defined below). This BAA will be effective as of the last signature date below (the "**BAA Effective Date**").

Customer must have an existing Services Agreement in place for this BAA to be valid and effective. Together with the Services Agreement, this BAA will govern each party's respective obligations regarding Protected Health Information (defined below).

You represent and warrant that (i) you have the full legal authority to bind Customer to this BAA, (ii) you have read and understand this BAA, and (iii) you agree, on behalf of Customer, to the terms of this BAA. If you do not have legal authority to bind Customer, or do not agree to these terms, please do not sign or click to accept the terms of this BAA.

**1. Definitions.** Any capitalized terms used but not otherwise defined in this BAA will have the meaning given to them in HIPAA and the HITECH Act.

"**Business Associate**" has the definition given to it under HIPAA.

"**Breach**" has the definition given to it under HIPAA. A Breach will not include an acquisition, access, use, or disclosure of PHI with respect to which Google has determined in accordance with 45 C.F.R. § 164.402 that there is a low probability that the PHI has been compromised.

"**Customer**" means the State of West Virginia or any agency, comprising a sub-part of the State of West Virginia.

"**Covered Entity**" has the definition given to it under HIPAA.

"**Covered Services**" means the Google products and services specifically stated as "Included Functionality" at [http://cloud.google.com/terms/identity/hipaa\\_functionality.html](http://cloud.google.com/terms/identity/hipaa_functionality.html).

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996 and the rules and the regulations thereunder, as amended.

"**HIPAA Implementation Guide**" means the informational guide that Google makes available describing how the Covered Services may be configured by Customer in connection with Customer's HIPAA compliance efforts. The HIPAA Implementation Guide for the Covered Services is available for review at the following URL: [https://static.googleusercontent.com/media/gsuite.google.com/en//terms/2015/1/hipaa\\_implementation\\_guide.pdf](https://static.googleusercontent.com/media/gsuite.google.com/en//terms/2015/1/hipaa_implementation_guide.pdf).

"**HITECH Act**" means the Health Information Technology for Economic and Clinical Health Act enacted in the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and the regulations thereunder, as amended.

**“Protected Health Information” or “PHI”** has the definition given to it under HIPAA and for purposes of this BAA is limited to PHI within Customer Data to which Google has access through the Covered Services in connection with Customer’s permitted use of Covered Services.

**“Security Breach”** means any Breach of Unsecured PHI or Security Incident of which Google becomes aware.

**“Security Incident”** has the definition given to it under HIPAA.

**“Services Agreement(s)”** means the written agreement(s) entered into between Google and Customer for provision of the Covered Services, which agreement(s) may be in the form of online terms of service.

**“Subcontractor”** means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

2. **Applicability.** This BAA applies to the extent Customer is acting as a Covered Entity or a Business Associate to create, receive, maintain, or transmit PHI via a Covered Service and to the extent Google, as a result, is deemed under HIPAA to be acting as a Business Associate or Subcontractor of Customer. Customer acknowledges that this BAA does not apply to, or govern, any other Google product, service, or feature that is not a Covered Service.

3. **Use and Disclosure of PHI.**

- (a) Except as otherwise stated in this BAA, Google may use and disclose PHI only as permitted or required by the Services Agreements and/or this BAA or as Required by Law. This means PHI created, received, maintained or transmitted on behalf of the Customer by the Associate. This PHI is governed by this Addendum and is limited to the minimum necessary, to complete the tasks or to provide the services associated with the terms of the original Agreement.
- (b) Google may use and disclose PHI for the proper management and administration of Google’s business and to carry out the legal responsibilities of Google, provided that any disclosure of PHI for such purposes may only occur if: (1) required by applicable law; or (2) Google obtains written reasonable assurances from the person to whom PHI will be disclosed that it will be held in confidence, used only for the purpose for which it was disclosed, and that Google will be notified of any Security Breach.
- (c) Google has no obligations under this BAA with respect to any PHI that Customer creates, receives, maintains, or transmits outside of the Covered Services (including Customer’s use of its offline or on-premise storage tools or third-party applications) and this BAA will not apply to any PHI created, received, maintained or transmitted outside of the Covered Services.

4. **Customer Obligations.**

- a. Customer may only use the Covered Services to create, receive, maintain, or transmit PHI. Customer is solely responsible for managing whether Customer's end users are authorized to share, disclose, create, and/or use PHI within the Covered Services.
- b. Customer will not request that Google or the Covered Services use or disclose PHI in any manner that would not be permissible under HIPAA if done by Customer (if Customer is a Covered Entity) or by the Covered Entity to which Customer is a Business Associate (unless expressly permitted under HIPAA for a Business Associate).
- c. For End Users that use the Covered Services in connection with PHI, Customer will use controls available within the Services, including those detailed in the HIPAA Implementation Guide, to ensure its use of PHI is limited to the Covered Services. Customer acknowledges and agrees that the HIPAA Implementation Guide is provided by Google solely as an informational guide with respect to Customer's configuration options, and that Customer is solely responsible for ensuring that its and its End Users' use of the Covered Services complies with HIPAA and HITECH.
- d. Customer will take appropriate measures to limit its use of PHI to the Covered Services and will limit its use within the Covered Services to the minimum extent necessary for Customer to carry out its authorized use of such PHI.
- e. Customer warrants that it has obtained and will obtain any consents, authorizations and/or other legal permissions required under HIPAA and/or other applicable law for the disclosure of PHI to Google. If there are any changes in, or revocation of, the permission given by an individual for use or disclosure of PHI, Customer is responsible for managing its use of the Covered Services accordingly to update and/or delete such PHI in the Covered Services.

## **5. Associate Obligations.**

- (a) **Stated Purposes Only.** The PHI may not be used by the Associate for any purpose other than as stated in this Addendum or as required or permitted by law.
- (b) **Limited Disclosure.** The PHI is confidential and will not be disclosed by the Associate other than as stated in this Addendum or as required or permitted by law. Associate is prohibited from directly or indirectly receiving any remuneration in exchange for an individual's PHI unless Customer gives written approval and the individual provides a valid authorization. Associate will refrain from marketing activities that would violate HIPAA, including specifically Section 13406 of the HITECH Act. Associate will report to Customer any use or disclosure of the PHI, including any Security Incident not provided for by this Agreement of which it becomes aware.
- (c) **Mitigation.** Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Associate of a use or disclosure of the PHI by Associate in violation of the requirements of this Addendum and report its mitigation activity back to the Customer.

- 6. Appropriate Safeguards.** Google and Customer will each use appropriate safeguards designed to prevent against unauthorized use or disclosure of PHI, and as otherwise required under HIPAA, with respect to the Covered Services. This shall include, but not be limited to:
- a. Limitation of the groups of its workforce and agents, to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Addendum, and the use and disclosure of the minimum PHI necessary or a Limited Data Set;
  - b. Appropriate notification and training of its workforce and agents in order to protect the PHI from unauthorized use and disclosure;
  - c. Maintenance of a comprehensive, reasonable and appropriate written PHI privacy and security program that includes administrative, technical and physical safeguards appropriate to the size, nature, scope and complexity of the Associate's operations, in compliance with the Security Rule;
  - d. In accordance with 45 CFR § 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.

**7. Reporting.**

- (a) Subject to Section 6(d), Google will promptly notify Customer following Google's Discovery of a Security Breach in accordance with HIPAA and in the most expedient time possible under the circumstances, consistent with the legitimate needs of applicable law enforcement and applicable laws, and after taking any measures Google deems necessary to determine the scope of the Security Breach and to restore the reasonable integrity of Google's systems.
- (b) To the extent practicable, Google will use commercially reasonable efforts to mitigate any further harmful effects of a Security Breach caused by Google.
- (c) Google will send any applicable Security Breach notifications to the notification email address provided by Customer in the Services Agreement or via direct communication with the Customer.
- (d) Notwithstanding Section 6(a), this Section 6(d) will be deemed as notice to Customer that Google periodically receives unsuccessful attempts for unauthorized access, use, disclosure, modification or destruction of information, or interference with the general operation of Google's information systems and the Covered Services.
- (e) In following the Security Incident notification procedure set out in the Data Processing Amendment, Google will, to the extent it has such information, provide Customer with details of the Security Incident relating to such Customer

including (i) the dates of the Security Incident; (ii) a description of the Customer resources impacted; (iii) the root cause of the Security Incident; and (iv) steps Google has taken to mitigate the potential risks and steps Google recommends Customer take to address the Security Incident.

Associate will cooperate in good faith with Customer in the investigation of any Security Incident. The parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.

- (f) Customer will coordinate with Associate to determine additional specific actions that will be required of Associate for mitigation of the Breach. Customer shall have the right to control all breach notifications to third parties. Associate will provide reasonable assistance to Customer. Such assistance will include the action outlined in (e) above as well as other assistance to answer questions the Customer has about the nature of the breach as well as remediation actions

If Associate enters into a subcontract relating to the Agreement where the subcontractor or agent receives PHI as described in Section 3.a. of this Addendum, all such subcontracts or downstream agreements shall contain the same incident notification requirements as contained herein.

- (g) Assistance in Litigation or Administrative Proceedings. Associate shall make itself and any subcontractors, workforce or agents assisting Associate in the performance of its obligations under this Agreement, available to the Customer at no cost to the Customer to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Customer, its officers or employees based upon claimed violations of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inaction or actions by Associate, except where Associate or its subcontractor, workforce or agent is a named as an adverse party.

8. **Subcontractors.** Google will take appropriate measures to ensure that any Subcontractors used by Google to perform its obligations under the Services Agreements that require access to PHI on behalf of Google are bound by written obligations that provide the same material level of protection for PHI as this BAA. To the extent Google uses Subcontractors in its performance of obligations hereunder, Google will remain responsible for their performance as if performed by Google.
9. **Access and Amendment.** Customer acknowledges and agrees that Customer is solely responsible for the form and content of PHI maintained by Customer within the Covered Services, including whether Customer maintains such PHI in a Designated Record Set

within the Covered Services. Google will provide Customer with access to Customer's PHI via the Covered Services so that Customer may fulfill its obligations under HIPAA with respect to Individuals' rights of access and amendment within ten (10) days of request by the Customer. Customer is responsible for managing its use of the Covered Services to appropriately respond to such Individual requests.

10. **Accounting of Disclosures.** Google will document disclosures of PHI by Google, its agents or subcontractors and provide an accounting of such disclosures to Customer as and to the extent required of a Business Associate under HIPAA and in accordance with the requirements applicable to a Business Associate under HIPAA. Associate agrees to document disclosures of the PHI and information related to such disclosures as would be required for Agency to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. This should include a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years from the date of disclosure, or longer if required by state law. At a minimum, such documentation shall include:
- the date of disclosure;
  - the name of the entity or person who received the PHI, and if known, the address of the entity or person;
  - a brief description of the PHI disclosed; and
  - a brief statement of purposes of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.

11. **Access to Records.** To the extent required by law, and subject to applicable attorney client privileges, Google will make its internal practices, books, and records concerning the use and disclosure of PHI received from Customer, or created or received by Google on behalf of Customer, available to the Secretary of the U.S. Department of Health and Human Services (the "**Secretary**") for the purpose of the Secretary determining compliance with this BAA. The Associate shall also make these records available to Customer, or Customer's contractor, for periodic audit of Associate's compliance with the Privacy and Security Rules.

12. **Reserved.**

13. **Reserved.**

**14. Expiration and Termination.**

(a) This BAA will terminate on the earlier of (i) a permitted termination in accordance with Section 11(b) below, or (ii) the expiration or termination of all Services Agreements under which Customer has access to a Covered Service.

(b) If either party materially breaches this BAA, the non-breaching party may terminate this BAA on 10 days' written notice to the breaching party unless the breach is cured within the 10-day period. An opportunity to cure by Associate is at the sole discretion of the Customer. If a cure under this Section 11(b) is not reasonably possible, the non-breaching party may immediately terminate this BAA, or if neither termination nor cure is reasonably possible under this Section

11(b), the non-breaching party may report the violation to the Secretary, subject to all applicable legal privileges.

- (c) If this BAA is terminated earlier than the Services Agreements, Customer may continue to use the Services in accordance with the Services Agreements, but must delete any PHI it maintains in the Covered Services and cease to further create, receive, maintain, or transmit such PHI to Google.

**15. Return/Destruction of Information.** On termination of the Services Agreements, Google will return or destroy all PHI received from Customer, at the Customer's option, and retain no copies, or created or received by Google on behalf of Customer; provided, however, that if such return or destruction is not feasible, Google will extend the protections of this BAA to the PHI not returned or destroyed and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. This shall also apply to all agents and subcontractors of Associate. The duty of Associate and its agents and subcontractors to assist the Customer with any HIPAA required accounting of disclosures survives the termination of the underlying Agreement.

**16. General Provisions/Ownership of PHI.**

- a. **Retention of Ownership.** Ownership of the PHI resides with the Customer and is to be returned on demand or destroyed at the Customer's option, at any time, and subject to the restrictions found within Section 4.b. above.
- b. **Secondary PHI.** Any data or PHI generated from the PHI disclosed hereunder which would permit identification of an individual must be held confidential and is also the property of Customer.
- c. **Electronic Transmission.** Except as permitted by law or this Addendum, the PHI or any data generated from the PHI which would permit identification of an individual must not be transmitted to another party by electronic or other means for additional uses or disclosures not authorized by this Addendum or to another contractor, or allied Customer, or affiliate without prior written approval of Customer.
- d. **No Sales.** Reports or data containing the PHI may not be sold without the Customer's or the affected individual's written consent.
- e. **No Third-Party Beneficiaries.** Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than Customer, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.
- f. **Interpretation.** The provisions of the Addendum shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provisions in this Addendum. The interpretation of this Addendum shall be made under the laws of the state of West Virginia.
- g. **Amendment.** The parties agree that to the extent necessary to comply with applicable law they will agree to further amend this Addendum.




h. **Additional Terms and Conditions.** Additional discretionary terms may be included in the release order or change order process.

**17. Miscellaneous.**

- (a) **Survival.** Sections 12 (Return/Destruction of Information) and 13 (Return/Destruction of Information) will survive termination or expiration of this BAA.
- (b) **Counterparts.** The parties may execute this BAA in counterparts, including facsimile, PDF or other electronic copies, which taken together will constitute one instrument.
- (c) **Effects of Addendum.** To the extent this BAA conflicts with the remainder of the Services Agreement(s), this BAA will govern. This BAA is subject to the "Governing Law" section in the Services Agreement(s). Except as expressly modified or amended under this BAA, the terms of the Services Agreement(s) remain in full force and effect.

Signed by the parties' authorized representatives on the dates below.

**Google LLC**

By: \_\_\_\_\_ 2020.09.16  
Print  15:23:53  
Title: \_\_\_\_\_ -07'00'  
Date: \_\_\_\_\_

**Customer:**

By: Justin T. McAllister  
Print Name: Justin T. McAllister  
Title: Chief Financial Officer  
Date: September 21, 2020



**GOOGLE TERMS AND ORDER OF PRECEDENT AGREEMENT**  
**EXHIBIT D**

# **Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements**

## **1.0 INTRODUCTION**

The Executive Branch has adopted privacy and information security policies to protect confidential and personally identifiable information (hereinafter all referred to as Confidential Information). This Notice sets forth the vendor's responsibilities for safeguarding this information.

## **2.1 DEFINITIONS**

- 2.2 Breach** shall mean a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Google.
- 2.3 Confidential Information**, shall include, but is not limited to, trade secrets, personally identifiable information, protected health information, financial information, financial account number, credit card numbers, debit card numbers, driver's license numbers, State ID numbers, social security numbers, employee home addresses, employee marital status, employee maiden name, etc.
- 2.4 Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Security Incidents shall not include Unsuccessful Security incidents as defined in Section 4.5.2.1.

## **3.0 BACKGROUND**

Agencies maintain Confidential Information, including, but not limited to, trade secrets, personally identifiable information, protected health information, financial information, financial account numbers, credit card numbers, debit card numbers, driver's license numbers, State ID numbers, social security numbers, employee home addresses, etc. Federal laws, including, but not limited to, the Health Insurance Portability and Accountability Act, the Privacy Act of 1974, Fair Credit Reporting Act and State laws require that certain information be safeguarded. In some situations, Agencies delegate, through contract provisions, functions to vendors that involve the vendor's collection, use and/or disclosure of Confidential Information. WV State government must take appropriate steps to ensure its compliance with those laws and desires to protect its citizens' and employees' privacy, and therefore, must require that its vendors also obey those laws.

Utilization of safeguards can greatly minimize potential exposure to sensitive information, and vendors are expected to adhere to industry standard best practices in the management of data collected by, or on behalf of, the State, and in the

## **Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements**

vendor's possession for a business purpose. Even when sound practices and safeguards are in use, exposures can occur as the result of a theft, loss, or compromise of data, or systems containing data. Additional vendor funding may be needed for required activities, such as: rapid notification to affected persons, and provision of a call center to handle inquiries.

### **4.1 POLICY**

- 4.2** All vendors for the Executive Branch of West Virginia State government shall sign both the RFP or RFQ, as applicable, and the Purchase Order which contain the confidentiality statement, incident response accountability acknowledgement, and adopt this policy by reference.
- 4.3** Vendors must contact the Privacy Officer of the Agency with which they are contracting to obtain Agency-specific privacy policies, procedures and rules, when applicable.
- 4.4** For vendors' information, Agencies generally require at least the following minimum standards of care in the handling of their Confidential Information:
  - 4.4.1** Confidential Information shall only be used or disclosed for the purposes designated in the underlying contract and at no time shall it be disclosed or used for a personal, non-work or non-contract related reason, unless specifically authorized in writing by the Agency.
  - 4.4.2** In all circumstances, vendors shall have no ownership rights or interests in any data or information, including Confidential Information. All data collected by the vendor on behalf of the Agency, or received by the vendor from the Agency, is owned by the Agency. There are no exceptions to this provision.
  - 4.4.3** In no circumstance shall a vendor use Confidential information, or data, in any way detrimental to the Agency or to any individual whose records reside in the vendor's control. This prohibition shall not be construed to curtail a vendor's whistleblower rights under Federal and State law. If, in the process of making a good faith report under the provisions of W. Va. Code § 6C-1-1 et seq. or the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), (Pub. L. No. 104-191) as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the Federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA") or any other relevant whistleblower law, a vendor finds it necessary to

## **Notice of State of West Virginia Confidentiality Policies and Information Security Accountability Requirements**

disclose Confidential Information to an appropriate authority in accordance with those statutes, the disclosure will not be treated as a Breach of the Agency's security, privacy or confidentiality policies, as long as the confidential nature of the information is explicitly conveyed to the authorized recipient.

- 4.4.4** The State may periodically, through the use of the Google Services, monitor and/or audit use of the information systems and other record-keeping systems contained within the Services.
- 4.4.5** Any collection, use or disclosure of information that is determined by the Agency to be contrary to the confidentiality statement, law or Agency policy may result in termination of the underlying contract.
- 4.4.6** The confidentiality and incident response accountability statement contained within the RFP or RFQ, as applicable, and the Purchase Order shall survive termination of the underlying contract.
- 4.5** If there is an incident that involves theft, loss, or compromise of State Confidential Information, the following reporting and/or actions must be taken by the vendor, on its own behalf, or on behalf of its subcontractor:
  - 4.5.1** If the event involves a theft, or is incidental to another crime, appropriate law enforcement officials shall be notified and a police report generated to document the circumstances of the crime, with a goal to establish whether the crime involved a motive to obtain the sensitive data. A copy of the police report will be forwarded in accordance with 4.4.2.3.
  - 4.5.2** Notification of Breach.

Google will promptly notify Customer following Google's Discovery of a successful Security Incident in the most expedient time possible, consistent with the legitimate needs of applicable law enforcement and applicable laws, and after taking any measures Google deems necessary to determine the scope of the Security Breach and to restore the reasonable integrity of Google's systems.

In following the Security Incident notification procedure set out in the Data Processing Amendment, Google will, to the extent it has such information, provide Customer with details of the Security Incident relating to such Customer including (i) the dates of the Security Incident and discovery of the Security Incident; (ii) a description of the Customer Data impacted; (iii) the root cause of the Security Incident; and (iv) steps Google has taken to mitigate the potential risks and steps Google recommends Customer take to address the security Incident.

## **Notice of State of West Virginia**

### **Confidentiality Policies and Information Security Accountability Requirements**

**4.5.2.1** Vendor will cooperate in good faith with Agency in the investigation of any Security Incident. The parties acknowledge and agree that this Section constitutes notice by Vendor to the Agency of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Agency shall be required. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Vendor's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of confidential information.

**4.5.2.2** Agency will coordinate with the vendor to determine additional specific actions that will be required of the vendor for mitigation of the Breach. Agency shall have the right to control all breach notifications to third parties.

**4.6** The State may require that a vendor provide evidence of adequate background checks, including a nationwide record search, for individuals who are entrusted by the vendor to work with State information.

**4.7** The State requires that any vendor taking possession of State data have comprehensive policies and practices to adequately safeguard that information, and further that the sensitivity of the information is clearly identified and documented in writing, with signed acknowledgement by the vendor that the sensitivity is understood, before it is conveyed to the vendor. Vendor policy should articulate all safeguards in place for the State information, including provisions for destruction of all data, including backup copies of the data, at the end of the vendor's legitimate need to possess the data. All State-owned media containing State information will be returned to the State when no longer legitimately needed by the vendor.

**4.8** All vendor owned devices that contain or transport any State Confidential Information must be encrypted using the AES algorithm, and an industry standard methodology. This includes desktop and laptop computers (whole drive encryption – not file encryption), personal digital assistants (PDA), smart phones, thumb or flash-type drives, CDs, diskettes, backup tapes, etc.

**GOOGLE TERMS AND ORDER OF PRECEDENT AGREEMENT**

**EXHIBIT E**

## Google Cloud Master General Terms

These Google Cloud Master Terms are comprised of the Google Cloud Master General Terms ("General Terms"), and all Services Schedules and Order Forms that are incorporated by reference into the Google Cloud Master General Terms (collectively, the "Terms").

### Google Cloud Master General Terms

**1. Services.** After the Customer and Reseller and/or Distributor complete and execute an Order Form, (a) Google will provide the Services to Customer in accordance with the Terms, including the SLAs, and (b) Customer may use the Services in accordance with the applicable Services Schedule.

### **2. Customer Obligations.**

**2.1 Consents.** Customer is responsible for any consents and notices required to permit (a) Customer's use and receipt of the Services and (b) Google's accessing, storing, and processing of data provided by Customer (including Customer Data, if applicable) under the Terms.

**2.2 Compliance.** Customer will (a) ensure that Customer and its End Users' use of the Services complies with the Terms, (b) use commercially reasonable efforts to prevent and terminate any unauthorized access or use of the Services, and (c) promptly notify Google of any unauthorized use of, or access to, the Services of which Customer becomes aware.

**2.3 Use Restrictions.** Customer will not, and will not allow End Users to, (a) copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any of the source code of the Services (except to the extent such restriction is expressly prohibited by applicable law); (b) sell, resell, sublicense, transfer, or distribute the Services; or (c) access or use the Services (i) in a manner intended to avoid incurring Fees; (ii) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State; (iii) in a manner that breaches, or causes the breach of, Export Control Laws; or (iv) to transmit, store, or process health information subject to United States HIPAA regulations except as permitted by an executed HIPAA BAA with Google (if approved), or an executed HIPAA BAA with Google's Reseller or Distributor.

### **3. RESERVED.**

### **4. Intellectual Property.**

**4.1 Intellectual Property Rights.** Except as expressly described in the Terms, the Terms do not grant either party any rights, implied or otherwise, to the other's content or Intellectual Property. As between the parties, Customer retains all Intellectual Property Rights in Customer Data and Customer Applications, and Google retains all Intellectual Property Rights in the Services and Software.

**4.2 Feedback.** At its option, Customer may provide feedback and suggestions about the Services to Google ("Feedback"). If Customer provides Feedback, then Google and its Affiliates may use that Feedback without restriction and without obligation to Customer.



## **5. Confidentiality.**

**5.1 Use and Disclosure of Confidential Information.** Subject to the Freedom of Information Act or similar state open records law, the Recipient will only use the Disclosing Party's Confidential Information to exercise its rights and fulfill its obligations under the Terms, and will use reasonable care to protect against the disclosure of the Disclosing Party's Confidential Information. Notwithstanding the foregoing, the Recipient may disclose the Disclosing Party's Confidential Information (a) to its Delegates who have a need to know and who are bound by confidentiality obligations at least as protective as those in this

Section 5 (Confidentiality); (b) with the Disclosing Party's written consent; or (c) regardless of any other provision in the Terms, as strictly necessary to comply with Legal Process, provided the Recipient promptly notifies the Disclosing Party prior to such disclosure unless legally prohibited from doing so. The Recipient will comply with the Disclosing Party's reasonable requests to oppose disclosure of its Confidential Information.

Notwithstanding the foregoing, the Parties understand that the terms of all State contracts, including any agreements with Google, will be disclosed via posting to the internet without notice.

**5.2 Redirect Disclosure Request.** If the Recipient receives Legal Process for the Disclosing Party's Confidential Information, the Recipient will first attempt to redirect the third party to request it from the Disclosing Party directly. To facilitate this request, the Recipient may provide the Disclosing Party's basic contact information to the third party. This Section 5.2 does not apply to West Virginia's obligations under FOIA.

## **6. Reserved.**

## **7. Reserved.**

**8. Disclaimer.** Except as expressly provided for in the Terms, to the fullest extent permitted by applicable law, Google (a) does not make any warranties of any kind, whether express, implied, statutory, or otherwise, including warranties of merchantability, fitness for a particular use, noninfringement, or error-free or uninterrupted use of the Services or Software and (b) makes no representation about content or information accessible through the Services. The Services are not intended to be used for High Risk Activities. Any use of the Services for High Risk Activities by Customer or its End Users will be at Customer's own risk, and Customer will be solely liable for the results of any failure of the Services when used for High Risk Activities.

## **9. Indemnification.**

**9.1 Google Indemnification Obligations.** Google will defend Customer and its Affiliates participating under the Terms ("Customer Indemnified Parties"), and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that the Customer Indemnified Parties' use of Google Indemnified Materials infringes the third party's Intellectual Property Rights.

**9.2 Customer Intellectual Property Infringement.** If Google is damaged or becomes subject to a Third-Party Legal Proceeding as a result of Customer's infringement of any third-party intellectual property, Google will pursue available remedies under applicable federal, state or local law.

**9.3 Indemnification Exclusions.** Sections 9.1 (Google Indemnification Obligations) and 9.2 (Customer Intellectual Property Infringement) will not apply to the extent the underlying allegation arises from (a) Customer's breach of the Terms or (b) a combination of the Google Indemnified Materials or Customer Materials (as applicable) with materials not provided by Google or the Customer under the Terms, unless the combination is required by the Terms.

**9.4 Indemnification Conditions.** Sections 9.1 (Google Indemnification Obligations) is conditioned on the following:

(a) Customer must promptly notify Reseller who will notify Google in writing of any allegation(s) that preceded the Third-Party Legal Proceeding and cooperate reasonably with Google to resolve the allegation(s) and Third-Party Legal Proceeding. If breach of this Section 9.4(a) prejudices the

defense of the Third-Party Legal Proceeding, then Google's obligations under Section 9.1 (Google Indemnification Obligations) will be reduced in proportion to the prejudice.

(b) Unless otherwise prohibited by law, Customer must tender sole control of the indemnified portion of the Third-Party Legal Proceeding to the indemnifying party, subject to the following: (i) the Customer may appoint its own non-controlling counsel, at its own expense; and (ii) any settlement requiring the Customer to admit liability, pay money, or take (or refrain from taking) any action, will require the Customer's prior written consent, not to be unreasonably withheld, conditioned, or delayed.

**9.5 Remedies.**

(a) If Google reasonably believes the Services might infringe a third party's Intellectual Property Rights, then Google may, at its sole option and expense, (i) procure the right for Customer to continue using the Services, (ii) modify the Services to make them non-infringing without materially reducing their functionality, or (iii) replace the Services with a non-infringing, functionally equivalent alternative.

(b) If Google does not believe the remedies in Section 9.5(a) are commercially reasonable, then Google may Suspend or terminate the impacted Services. If Google terminates Services under this Section 9.5 (Remedies), then upon Customer request (i) Google will refund to Customer any unused prepaid Fees that Customer paid to Google for use of the terminated Services, and (ii) if Customer has made financial commitments in an Order Form or addendum to the Terms, then Google will agree to amend such commitments proportional to Customer's spend on the terminated Services in the year preceding the termination of the Services.

**9.6 Sole Rights and Obligations.** Without affecting either party's termination rights, this Section 9 (Indemnification) states the Customer's sole and exclusive remedy under the Terms for any third-party allegations of Intellectual Property Rights infringement covered by this Section 9 (Indemnification).

**10. Liability.**

**10.1 Limited Liabilities.**

**(a) To the extent permitted by applicable law and subject to Section 10.2 (Unlimited Liabilities), neither party will have any Liability arising out of or relating to the Terms for any**

- (i) indirect, consequential, special, incidental, or punitive damages or**
- (ii) lost revenues, profits, savings, or goodwill.**

**(b) Each party's total aggregate Liability for damages arising out of or relating to the Terms is limited to the Fees Customer paid under the applicable Services Schedule during the 12 month period before the event giving rise to Liability.**

**(c) Enhanced Liability: Notwithstanding Section 10.1(b) above, Google will be liable to the Customer for up to an additional \$2,000,000 for costs (including but not limited to notification costs and credit monitoring services) incurred by the Customer arising out of a Data Incident or Breach as described in the HIPAA Business Associate Addendum.**

**10.2 Unlimited Liabilities. Nothing in the Terms excludes or limits either party's Liability for:**

- (a) subject to Section 8 (Disclaimer), death, personal injury, or tangible personal property damage resulting from its negligence or the negligence of its employees or agents;**
- (b) its fraud or fraudulent misrepresentation;**
- (c) its obligations under Section 9 (Indemnification);**
- (d) its infringement of the other party's Intellectual Property Rights;**
- (e) its payment obligations under the Terms; or**
- (f) matters for which liability cannot be excluded or limited under applicable law.**

**11. Term and Termination.**

**11.1 Term. The Terms, unless they expire or terminate in accordance with the Reseller Agreement or Distributor Agreement, will remain in effect for the contract period as described in the applicable Reseller Agreement or Distributor Agreement.**

**11.2 Termination for Convenience. Subject to any financial commitments in an Order Form or addendum to the Terms, Customer may terminate the Terms or an Order Form for convenience prior written notice to Reseller or Distributor.**

**11.3 Reserved.**

**11.4 Effects of Termination.** If the Terms terminate or expire, then all Services Schedules and Order Forms also terminate or expire. If an Order Form terminates or expires, then after that Order Form's termination or expiration effective date, (a) all rights and access to the Services under that Order Form will terminate (including access to Customer Data, if applicable), unless otherwise described in the applicable Services Schedule, and (b) Reseller or Distributor will send Customer a final invoice (if applicable) for payment obligations under that Order Form. Termination or expiration of one Order Form will not affect other Order Forms.

**11.5 Survival.** The following Sections will survive expiration or termination of the Terms: Section 4 (Intellectual Property), Section 5 (Confidentiality), Section 8 (Disclaimer), Section 9 (Indemnification), Section 10 (Liability), Section 11.4 (Effects of Termination), Section 12 (Miscellaneous), Section 13 (Definitions), and any additional sections specified in the applicable Services Schedule.

## **12. Miscellaneous.**

**12.1 Notices.** Google will provide notices under the Terms to Customer by sending an email to the Notification Email Address. Customer will provide notices under the Terms to Google by sending an email to [legal-notices@google.com](mailto:legal-notices@google.com). Notice will be treated as received when the email is sent. Customer is responsible for keeping its Notification Email Address current.

**12.2 Emails.** The parties may use emails to satisfy written approval and consent requirements under the Terms.

**12.3 Reserved.**

**12.4 Reserved.**

**12.5 Force Majeure.** Neither party will be liable for failure or delay in performance of its obligations to the extent caused by circumstances beyond its reasonable control, including acts of God, natural disasters, terrorism, riots, or war.

**12.6 Subcontracting.** Google may subcontract obligations under the Terms but will remain liable to Customer for any subcontracted obligations.

**12.7 No Agency.** The Terms do not create any agency, partnership, or joint venture between the parties.

**12.8 No Waiver.** Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under the Terms.

**12.9 Severability.** If any part of the Terms is invalid, illegal, or unenforceable, the rest of the Terms will remain in effect.

**12.10 No Third-Party Beneficiaries.** The Terms do not confer any rights or benefits to any third party unless it expressly states that it does.

12.11 Equitable Relief. Nothing in the Terms will limit either party's ability to seek equitable relief.

12.12 Reserved.

12.13 Amendments. Except as specifically described otherwise in the Terms, any amendment to the Terms must be in writing, expressly state that it is amending the Terms, and be signed by both parties.

12.14 Independent Development. Nothing in the Terms will be construed to limit or restrict either party from independently developing, providing, or acquiring any materials, services, products, programs, or technology that are similar to the subject of the Terms, provided that the party does not breach its obligations under the Terms in doing so.

12.15 Reserved.

12.16 Conflicting Terms. If there is a conflict among the documents that make up the Terms, then the documents will control in the following order: the applicable Order Form, the applicable Services Schedule, the General Terms, and the URL Terms.

12.17 Reserved.

12.18 Reserved.

12.19 Reserved.

12.20 Headers. Headings and captions used in the Terms are for reference purposes only and will not have any effect on the interpretation of the Terms.

### 13. Definitions.

"Affiliate" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party.

"AUP" means Google's acceptable use policy as defined in the applicable Services Schedule.

"BAA" or "Business Associate Agreement" is an amendment to the Customer's Reseller Agreement or Distributor Agreement covering the handling of Protected Health Information (as defined in HIPAA).

"Brand Features" means each party's trade names, trademarks, logos, domain names, and other distinctive brand features.

"Confidential Information" means information that one party or its Affiliate ("Disclosing Party") discloses to the other party ("Recipient") under the Terms, and that is marked as confidential or would normally be considered confidential information under the circumstances, such as trade secrets or personally identifiable information. Customer Data is Customer's Confidential Information. Confidential Information does not include information that is independently developed by the recipient, is shared with the recipient



by a third party without confidentiality obligations, or is or becomes public through no fault of the recipient.

**"Control"** means control of greater than 50% of the voting rights or equity interests of a party.

**"Customer Application"** has the meaning described in the Services Schedule.

**"Customer Data"** has the meaning described in the Services Schedule (if applicable).

**"Customer Indemnified Materials"** has the meaning described in the applicable Services Schedule.

**"Delegates"** means the Recipient's employees, Affiliates, agents, or professional advisors.

**"Distributor"** means an entity authorized by Google to distribute the Services to a Reseller for resale to federal, state, or local government entities of the United States (or representatives of such entities).

**"Distributor Agreement"** means, if applicable, the separate agreement between Customer and Distributor regarding the Services. The Distributor Agreement is independent of and outside the scope of these Terms.

**"Effective Date"** means the date of the last party's signature of the General Terms (or other applicable ordering document that incorporates the General Terms).

**"End User" or "Customer End User"** means an individual that Customer permits to use the Services or a Customer Application.

**"Export Control Laws"** means all applicable export and re-export control laws and regulations, including (a) the Export Administration Regulations ("**EAR**") maintained by the U.S. Department of Commerce, (b) trade and economic sanctions maintained by the U.S. Treasury Department's Office of Foreign Assets Control, and (c) the International Traffic in Arms Regulations ("**ITAR**") maintained by the U.S. Department of State.

**"Fees"** means the product of the amount of Services used or ordered by Customer multiplied by the Prices, plus any applicable Taxes. Fees will be described in the Customer's Reseller Agreement or Distributor Agreement.

**"Google Indemnified Materials"** has the meaning described in the applicable Services Schedule.

**"High Risk Activities"** means activities where the failure of the Services could lead to death, serious personal injury, or severe environmental or property damage.

**"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996 as it may be amended from time to time, and any regulations issued under it.

**"including"** means including but not limited to.

**"Indemnified Liabilities"** means any (a) settlement amounts approved by the indemnifying party, and (b) damages and costs finally awarded against the indemnified party and its Affiliates by a court of competent jurisdiction.



**“Intellectual Property”** or **“IP”** means anything protectable by an Intellectual Property Right.

**“Intellectual Property Right(s)”** means all patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.

**“Legal Process”** means an information disclosure request made under law, governmental regulation, court order, subpoena, warrant, governmental regulatory or agency request, or other valid legal authority, legal procedure, or similar process.

**“Liability”** means any liability, whether under contract, tort (including negligence), or otherwise, regardless of whether foreseeable or contemplated by the parties.

**“Notification Email Address”** has the meaning described in the applicable Services Schedule.

**“Order Term”** means the period of time starting on the Services Start Date for the Services and continuing for the period indicated on the Order Form unless terminated in accordance with the Agreement.

**“Prices”** has the meaning described in the applicable Reseller Agreement or Distributor Agreement.

**“Reseller Agreement”** means the separate agreement between Customer and Reseller regarding the Services. The Reseller Agreement is independent of and outside the scope of these Terms.

**“Reseller”** means, if applicable, the authorized non-Affiliate third party reseller that sells Google Services through a Distributor to Customer.

**“Service Level Agreement”** or **“SLA”** has the meaning described

in the Services Schedule. **“Services”** has the meaning described

in the applicable Services Schedule.

**“Services Schedule(s)”** means a schedule to the Terms with terms that apply only to the services and software (if applicable) described in that schedule.

**“Services Start Date”** means either the start date described in the Order Form or, if none is specified in the Order Form, the date Google makes the Services available to Customer.

**“Software”** has the meaning described in the Services Schedule (if applicable).

**“Suspend”** or **“Suspension”** means disabling access to or use of the Services or components of the Services.

**“Third-Party Legal Proceeding”** means any formal legal proceeding filed by an unaffiliated third party before a court or government tribunal (including any appellate proceeding).

**“Trademark Guidelines”** means Google’s Brand Terms and Conditions described at <https://www.google.com/permissions/trademark/brand-terms.html>.



**“URL”** means a uniform resource locator address to a site on the internet.

**“URL Terms”** has the meaning described in the Services Schedule.

**“Use Restrictions”** means the restrictions in Section 2.3 (Use Restrictions) of these General Terms and any additional restrictions on the use of Services described in a section entitled “Additional Use Restrictions” in the applicable Services Schedule.



## **Google Cloud Master Terms G Suite Services Schedule**

This G Suite Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Terms. This Services Schedule applies solely to the services described in this Services Schedule. Terms defined in the General Terms apply to this Services Schedule.

### **1. Using the Services.**

- 1.1 **Admin Console.** Google will provide Customer access to the Admin Console through which Customer may manage its use of the Services. Customer may specify one or more Administrators through the Admin Console who will have the right to access Admin Accounts. Customer is responsible for (a) maintaining the confidentiality and security of the End User Accounts and associated passwords and (b) any use of the End User Accounts. Customer agrees that Google's responsibilities do not extend to the internal management or administration of the Services for Customer.
- 1.2 **Additional Use Restrictions.** Unless otherwise permitted in the G Suite Service Specific Terms, Customer will not use, and will not allow End Users to use, the Services to place or receive emergency services calls.
- 1.3 **Requesting Additional End User Accounts During Order Term.** Customer may purchase additional End User Accounts during an Order Term by (a) executing an additional Order Form reflecting the purchase with Google or (b) ordering End User Accounts via the Admin Console. Such additional End User Accounts will have a pro-rated term ending on the last day of the applicable Order Term.

### **2. Data Processing and Security.**

- 2.1 **Data Processing Amendment.** The Data Processing Amendment is incorporated into this Services Schedule once Customer accepts it in the Admin Console. If the processing of Personal Data under the Terms is subject to the GDPR, then Customer will accept the Data Processing Amendment in the Admin Console.

### **3. Additional Payment Terms.**

- 3.1 **Usage and Invoicing.** Customer will pay all Fees for the Services and such payment will be made pursuant to the Reseller Agreement or Distributor Agreement. Google's measurement tools will be used to determine Customer's usage of the Services. Unless otherwise provided in an Order Form or required by law, Fees for Services are nonrefundable.
- 3.2 **Reserved.**

### **4. Updates to Services and Terms.**

#### **4.1 Changes to Services.**

- (a) **Limitations on Changes.** Google may update the Services, provided the updates do not result in a material reduction of the performance or security of the Services.

(b) **Discontinuance.** Google will notify Customer at least 12 months before discontinuing any Core Service (or associated material functionality), and at least 36 months for any Key Service (or associated material functionality), in each case unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.

(c) **Support.** Google will continue to provide product and security updates, and Technical Support Services, until the conclusion of the applicable notice period under subsection (b) (Discontinuance).

4.2 **Changes to Terms.** Google may update the URL Terms, provided the updates do not (a) result in a material degradation of the overall security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Data Processing Amendment, or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material updates to URL Terms.

4.3 **Permitted Changes.** Sections 4.1 (Changes to Services) and 4.2 (Changes to Terms) do not limit Google's ability to make changes required to comply with applicable law or address a material security risk, or that are applicable to new or pre-general availability Services or functionality.

## **5. Temporary Suspension.**

5.1 **Services Suspension.** Google may Suspend Services if (a) necessary to comply with law or protect the Services or Google's infrastructure supporting the Services or (b) Customer or any End User's use of the Services does not comply with the AUP, and it is not cured following notice from Google. For Suspensions of End User Accounts, Google will provide Customer's Administrator the ability to restore End User Accounts in certain circumstances.

5.2 **Limitations on Services Suspensions.** If Google Suspends Services, then (a) Google will provide Customer notice of the cause for Suspension without undue delay, to the extent legally permitted, and (b) the Suspension will be to the minimum extent and for the shortest duration required to resolve the cause for Suspension.

**6. Technical Support.** Google will provide G Suite Technical Support Services to Customer during the Order Term in accordance with the G Suite Technical Support Services Guidelines.

## **7. Additional Customer Responsibilities.**

7.1 **Customer Domain Name Ownership.** Customer is responsible for obtaining and maintaining any rights necessary for Customer's and Google's use of the Customer Domain Names under the Terms. Before providing the Services, Google may require that Customer verify that Customer owns or controls the Customer Domain Names. If Customer does not own or control the Customer Domain Names, then Google will have no obligation to provide the Services to Customer.

7.2 **Abuse Monitoring.** Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for

Customer Domain Names, but Google may monitor emails sent to these aliases to allow Google to identify Services abuse.

- 8. Using Brand Features Within the Services.** Google will display only those Customer Brand Features that Customer authorizes Google to display by uploading them into the Services. Google will display those Customer Brand Features within designated areas of the web pages displaying the Services to End Users. Customer may specify the nature of this use in the Admin Console. Google may also display Google Brand Features on such web pages to indicate that the Services are provided by Google.
- 9. Additional Products.** Google makes optional Additional Products available to Customer and its End Users. Customer's use of Additional Products is subject to the Additional Product Terms.
- 10. Reseller Orders.** This Section 10 (Reseller Orders) applies if Customer orders the Services from a Reseller under a Reseller Agreement.

  - 10.1 Orders.** If Customer orders Services from Reseller, then (a) fees for the Services will be set between Customer and Reseller, and any payments will be made directly to Reseller under the Reseller Agreement; (b) RESERVED; (c) Customer will receive applicable SLA credits (if any) from Reseller; (d) Google may share Customer Confidential Information with Reseller as a Delegate subject to General Terms Section 5.1 (Use and Disclosure of Confidential Information); and (e) Customer may request additional End User Accounts during the Order Term by contacting Reseller.
  - 10.2 Reseller as Administrator.** At Customer's discretion, Reseller may access Customer's Account or Customer's End User Accounts. As between Google and Customer, Customer is solely responsible for (a) any access by Reseller to Customer's Account or Customer's End User Accounts and (b) defining in the Reseller Agreement any rights or obligations as between Reseller and Customer with respect to the Services.
  - 10.3 Reseller Verification of Domain Names.** Reseller may verify that Customer owns or controls the Customer Domain Names. If Customer does not own or control the Customer Domain Names, then Google will have no obligation to provide the Services to Customer.
  - 10.4 Reseller Technical Support.** Customer acknowledges and agrees that Reseller may disclose End User Personal Data to Google as reasonably required in order for Reseller to handle any support issues that Customer escalates to or via Reseller.
- 11. Termination of Previous Agreements.** If Google and Customer have previously entered into a G Suite Agreement, then that agreement will terminate on the Services Start Date, and the Agreement will govern the provision and use of the Services going forward.
- 12. Additional Definitions.**

"**Additional Products**" means products, services, and applications that are not part of the Services but may be accessible for use in conjunction with the Services.

"**Additional Product Terms**" means the then-current terms at [https://gsuite.google.com/intl/en/terms/additional\\_services.html](https://gsuite.google.com/intl/en/terms/additional_services.html).

**“Admin Account”** means a type of End User Account that Customer (or Reseller, if applicable) may use to administer the Services.

**“Admin Console”** means the online console(s) and tool(s) provided by Google to Customer for administering (a) the Services under this Services Schedule and (b) the services set out in a Complementary Product Services Summary (if applicable).

**“Administrator”** means Customer-designated personnel who administer the Services to End Users on Customer’s behalf, and have the ability to access Customer End User Accounts. Such access includes the ability to access, monitor, use, modify, withhold, or disclose any data available to End Users associated with their End User Accounts.

**“AUP”** means the then-current acceptable use policy for the Services described at <https://cloud.google.com/terms/aup/>.

**“Complementary Product Services Summary”** has the meaning given in the Data Processing Amendment.

**“Core Services”** means the then-current “Core Services for G Suite” as described in the Services Summary at [https://gsuite.google.com/terms/user\\_features.html](https://gsuite.google.com/terms/user_features.html).

**“Customer Data”** means data submitted, stored, sent, or received via the Services by Customer or its End Users.

**“Customer Domain Name”** means a domain name specified in the Order Form to be used in connection with the Services.

**“Customer Materials”** means Customer Data and Customer Brand Features.

**“Data Processing Amendment”** means the then-current terms describing data protection and processing obligations with respect to Customer Data, as described at [https://gsuite.google.com/terms/dpa\\_terms.html](https://gsuite.google.com/terms/dpa_terms.html).

**“End User Account”** means a Google-hosted account established by Customer through the Services for an End User to use the Services.

**“GDPR”** has the meaning given to it in the Data Processing Amendment.

**“Google Indemnified Materials”** means Google’s technology used to provide the Services and Google’s Brand Features.

**“G Suite Service Specific Terms”** means the then-current terms specific to one or more Services described at <https://gsuite.google.com/terms/service-terms/>.

**“G Suite Technical Support Services”** or **“TSS”** means the technical support service provided by Google to Customer under the G Suite Technical Support Services Guidelines.

**“G Suite Technical Support Services Guidelines”** or **“TSS Guidelines”** means the then-current G Suite support service guidelines described at <https://gsuite.google.com/terms/tssg.html>.

**"Key Services"** means Gmail, Google Calendar, Google Docs, Google Sheets, Google Slides, Google Drive, Hangouts Chat, Hangouts Meet, and Google Forms.

**"Notification Email Address"** means the email address(es) designated by Customer in the Admin Console.

**"Other Services"** means the then-current "Other Services for G Suite" as described in the Services Summary at [https://gsuite.google.com/terms/user\\_features.html](https://gsuite.google.com/terms/user_features.html).

**"Personal Data"** has the meaning given to it in the Data Processing Amendment.

**"Prices"** means (a) for orders from a Reseller, the applicable prices agreed in the Reseller Agreement, otherwise (b) the applicable prices described at <https://gsuite.google.com/pricing.html>, unless otherwise agreed in an Order Form or amendment to this Services Schedule.

**"Reseller"** means, if applicable, the authorized unaffiliated third-party reseller that sells the Services to Customer.

**"Reseller Agreement"** means, if applicable, the separate agreement between Customer and Reseller regarding the Services. The Reseller Agreement is independent of and outside the scope of the Agreement.

**"Services"** means the then-current Core Services and Other Services described at [https://gsuite.google.com/terms/user\\_features.html](https://gsuite.google.com/terms/user_features.html).

**"SLA"** means the then-current service level agreement described at <https://gsuite.google.com/terms/sla.html>.

**"URL Terms"** means the AUP, G Suite Data Processing Amendment, G Suite Service Specific Terms, G Suite Technical Support Services Guidelines, and SLAs.

## Google Cloud Master Terms Implementation Services Schedule

This Implementation Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Terms. This Services Schedule applies to implementation and advisory services described in this Services Schedule that are designed to help Customer use Google products and services. Terms defined in the General Terms apply to this Services Schedule.

1. **Services.**
  - 1.1 **Provision of Services.** Google will provide Services, including Deliverables, to Customer, subject to Customer fulfilling its obligations under Section 2.1 (Cooperation).
  - 1.2 **Training Services.** Customer may order Training Services for use in connection with the Services. Training Services are subject to the Training Terms.
  - 1.3 **Invoices and Payment.** Customer will pay all Fees for Services ordered under this Services Schedule. Fees for some Services may be non-cancellable, as specified in the Order Form.
  - 1.4 **Personnel.** Google will determine which Personnel will perform the Services. If Customer requests a change of Personnel and provides a reasonable and legal basis for such request, then Google will use commercially reasonable efforts to replace the assigned Personnel with alternative Personnel.
  - 1.5 **Compliance with Customer's Onsite Policies and Procedures.** Google Personnel performing Services at Customer's facilities will comply with Customer's reasonable onsite policies and procedures made known to Google in writing in advance.
2. **Customer Obligations.**
  - 2.1 **Cooperation.** Time will not be of the essence in performing the Implementation Services. Customer will provide reasonable and timely cooperation in connection with Google's provision of the Services and delivery of the Deliverables. Google will not be liable for a delay caused by Customer's failure to provide Google with the information, materials, consents, or access to Customer facilities, networks, or systems required for Google to perform the Services. If Reseller or Distributor informs Customer of such failure and Customer does not cure the failure within 30 days, then (a) Reseller or Distributor may terminate any incomplete Services and (b) Customer will pay actual costs incurred by Reseller or Distributor for the cancelled Services.
  - 2.2 **No Personal Data.** Customer acknowledges that Google does not need to process Personal Data to perform the Services. Customer will not provide Google with access to Personal Data unless the parties have agreed in a separate agreement on the scope of work and any terms applicable to Google's processing of such Personal Data.
3. **Payments.** If Customer orders Professional Services from a Partner: (a) Customer will pay Partner for the Professional Services; (b) all payment terms are to be decided upon between Customer and Partner; (c) there will not be an Ordering Document between Google and Customer; (d) Google will provide to Partner any refunds or credits that may be due to Customer; and (e) any obligation on the part of Partner to provide any such

refunds or credits to Customer will depend on the terms decided upon between Customer and Partner.

#### **4. Intellectual Property.**

4.1 **Background IP.** Customer owns all rights, title, and interest in Customer's Background IP. Google owns all rights, title, and interest in Google's Background IP. Customer grants Google a license to use Customer's Background IP to perform the Services (with a right to sublicense to Google Affiliates and subcontractors). Except for the license rights under Sections 4.2 (Google Technology) and 4.3 (Deliverables), neither party will acquire any right, title, or interest in the other party's Background IP under this Services Schedule.

4.2 **Google Technology.** Google owns all rights, title, and interest in Google Technology. To the extent Google Technology is incorporated into Deliverables, Google grants Customer a limited, worldwide, non-exclusive, perpetual, non-transferable license (with the right to sublicense to Affiliates) to use the Google Technology in connection with the Deliverables for Customer's internal business purposes. This Services Schedule does not grant Customer any right to use materials, products, or services that are made available to Google customers under a separate agreement, license, or Services Schedule.

4.3 **Deliverables.** Google grants Customer a limited, worldwide, non-exclusive, perpetual, fully-paid, non-transferable license (with the right to sublicense to Affiliates) to use, reproduce, and modify the Deliverables for Customer's internal business purposes.

#### **5. Warranties and Remedies.**

5.1 **Google Warranty.** Google will perform the Services in a professional and workmanlike manner, in accordance with practices used by other service providers performing services similar to the Services. Google will use Personnel with requisite skills, experience, and qualifications to perform the Services.

5.2 **Remedies.** Google's entire liability and Customer's sole remedy for Google's failure to provide Implementation Services or Deliverables that conform with Section 5.1 (Google Warranty) will be for Google to, at its option, (a) use commercially reasonable efforts to re-perform the Services or (b) terminate the Order Form and refund any applicable Fees received for the nonconforming Services. Any claim that Google has breached the warranty as described in Section 5.1 (Google Warranty) must be made within 30 days after Google has performed the Services.

5.3 **Disclaimers.** TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS SECTION 5, GOOGLE DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. GOOGLE MAKES NO REPRESENTATIONS ABOUT ANY GOOGLE PRODUCTS OR ANY CONTENT OR INFORMATION MADE ACCESSIBLE OR AVAILABLE BY OR THROUGH THE PROFESSIONAL SERVICES.

**6. Indemnification.**

6.1 **Indemnification Exclusions.** General Terms Sections 9.1 (Google Indemnification Obligations) will not apply to the extent the underlying allegation arises from (a) modifications to the Google Indemnified Materials or Customer Materials (as applicable) by anyone other than Google or (b) compliance with Customer's instructions, design, or request for customized features.

6.2 **Infringement Remedies.** The remedies described in General Terms Section 9.5 (Remedies) also apply to Deliverables.

7. **Effects of Termination.** If this Services Schedule or an Order Form under this Services Schedule between Customer and Partner expires or terminates, then:

(a) **Effect on Services.** The rights under the Terms granted by one party to the other regarding the Services will cease immediately except as described in this Section 7 (Effects of Termination), and Google will stop work on the Services.

(b) **Reserved.**

(c) **Survival.** The following Sections of this Schedule will survive expiration or termination of this Services Schedule: 4 (Intellectual Property), 6 (Indemnification), 7 (Effects of Termination), and 11 (Additional Definitions).

8. **Reserved.**

9. **Reserved.**

10. **Miscellaneous.**

10.1 **Independent Development.** Nothing in the Terms of Service will be construed to limit or restrict either party from independently developing, providing, or acquiring any materials, services, products, programs or technology that are similar to the subject of the Terms of Service t, provided that the party does not violate its obligations under the Terms of Service.

10.2 **No Third-Party Beneficiaries.** The Terms of Service do not confer any benefits on any third party unless it expressly states that it does.

10.3 **Interpretation of Conflicting Terms.** Unless stated otherwise in the applicable Ordering Document, if there is a conflict between any term of the Terms of Service and a term of an Ordering Document, the Terms of Service will govern.

11. **Additional Definitions.**

**"Background IP"** means all Intellectual Property Rights owned or licensed by a party (a) before the Effective Date of the applicable Order Form or (b) independent of the Services.



**“Customer Indemnified Materials”** means (a) Customer Background IP and any other information, materials, or technology provided to Google by Customer in connection with the Services (in each case, excluding any open source software) and (b) Customer’s Brand Features. Customer Indemnified Materials do not include Google Technology or Deliverables.

**“Deliverables”** means work product created specifically for Customer by Google Personnel as part of the Services and specified as Deliverables in an Order Form.

**“Google Indemnified Materials”** means (a) Deliverables and Google Technology (in each case, excluding any open source software) or (b) Google’s Brand Features. Google Indemnified Materials do not include Customer Background IP.

**“Google Technology”** means (a) Google Background IP; (b) all Intellectual Property and know-how applicable to Google products and services; and (c) tools, code, algorithms, modules, materials, documentation, reports, and technology developed in connection with the Services that have general application to Google’s other customers, including derivatives of and improvements to Google’s Background IP. Google Technology does not include Customer Background IP or Customer Confidential Information.

**“Notification Email Address”** means the email address(es) designated by Customer in the applicable Order Form.

**“Order Form”** means an order form issued by Reseller and/or Distributor and executed by Customer and Google specifying the Services Google will provide to Customer under this Services Schedule.

**“Personal Data”** means personal data that (a) has the meaning given to it in the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (“GDPR”) and (b) would cause Google to be subject to GDPR as a data processor for Customer.

**“Personnel”** means a party’s and its Affiliates’ respective directors, officers, employees, agents, and subcontractors.

**“Prices”** means the amounts agreed to in an Order Form under this Services Schedule.

**“Services”** means the then-current advisory and implementation services described at <https://g.co/cloudpsoterm>s and similar advisory or implementation services designed to help Customer use Google products and services. Services do not include Training Services.

**“Training Services”** means education and certification services related to Google products and services for individual users, as more fully described in an applicable Order Form. Training Services do not include Deliverables.

**“Training Terms”** means the then-current terms applicable to Training Services described at <https://enterprise.google.com/terms/training-services.html>.

# Google Cloud Platform Acceptable Use Policy

Last modified: December 16, 2015 | [Previous Versions](#)

Use of the Services is subject to this Acceptable Use Policy.

Capitalized terms have the meaning stated in the applicable agreement between Customer and Google.

Customer agrees not to, and not to allow third parties to use the Services:

- to violate, or encourage the violation of, the legal rights of others (for example, this may include allowing Customer End Users to infringe or misappropriate the intellectual property rights of others in violation of the Digital Millennium Copyright Act);
- to engage in, promote or encourage illegal activity;
- for any unlawful, invasive, infringing, defamatory or fraudulent purpose (for example, this may include phishing, creating a pyramid scheme or mirroring a website);
- to intentionally distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- to interfere with the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;
- to disable, interfere with or circumvent any aspect of the Services;
- to generate, distribute, publish or facilitate unsolicited mass email, promotions, advertisements or other solicitations ("spam"); or



- to use the Services, or any interfaces provided with the Services, to access any other Google product or service in a manner that violates the terms of service of such other Google product or service.

# Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.3)

The customer agreeing to these terms ("Customer"), and Google LLC, Google Ireland Limited, Google Asia Pacific Pte. Ltd., or any other entity that directly or indirectly controls, is controlled by, or is under common control with Google LLC (as applicable, "Google"), have entered into one or more G Suite Agreement(s) (as defined below) and/or Complementary Product Agreements(s) (as defined below) (each, as amended from time to time, an "Agreement").

- 1. Commencement.
  - This Data Processing Amendment to G Suite and/or Complementary Product Agreement including its appendices (the "Data Processing Amendment") will be effective and replace any previously applicable data processing and security terms as from the Amendment Effective Date (as defined below).
  - This Data Processing Amendment supplements the applicable Agreement. Where that Agreement was entered into offline with Google Ireland Limited, this Data Processing Amendment supersedes the "Privacy" Clause in the Agreement (if applicable).
- 2. Definitions
  - 2.1 Capitalized terms defined in the applicable Agreement apply to this Data Processing Amendment. In addition, in this Data Processing Amendment:
    - "Additional Products" means products, services and applications that are not part of the Services but that may be accessible, via the Admin Console or otherwise, for use with the Services.



- **“Additional Security Controls”** means security resources, features, functionality and/or controls that Customer may use at its option and/or as it determines, including the Admin Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.
- **“Advertising”** means online advertisements displayed by Google to End Users, excluding any advertisements Customer expressly chooses to have Google or any of its Affiliates display in connection with the Services under a separate agreement (for example, Google AdSense advertisements implemented by Customer on a website created by Customer using any Google Sites functionality within the Services).
- **“Affiliate”** means any entity controlling, controlled by, or under common control with a party, where “control” is defined as: (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.
- **“Agreed Liability Cap”** means the maximum monetary or payment-based amount at which a party’s liability is capped under the applicable Agreement.
- **“Alternative Transfer Solution”** means a solution, other than the Model Contract Clauses, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law.
- **“Amendment Effective Date”** means the date on which Customer accepted, or the parties otherwise agreed to, this Data Processing Amendment.
- **“Audited Services”** means:

