

Services Agreement – Google Apps Services

This Services Agreement (the “Agreement”) is entered into by and between Carahsoft Technology Corporation, with offices at 1860 Michael Faraday Dr., Suite 100, Reston, VA 20190 (“Distributor” or “Carahsoft”) and State of Louisiana, with an address at 1201 North 3rd Street, Baton Rouge, L.A. 70802 (“Customer” or “State”). This Agreement will be effective as of the date countersigned below (the “Effective Date”). This Agreement governs (i) Customer’s access to and use of the Service provided by third party provider Google, Inc., with offices at 1600 Amphitheater Parkway, Mountain View, CA 94043 (“Provider”) and (ii) provision of Services to the State directly or through a designated third party reseller (“Reseller”). As of the effective date of this Agreement, Carahsoft is the sole distributor of the Services to customers and resellers within the United States state and local government market vertical.

1. Services.

- 1.1 Facilities. All facilities used to store and process Customer Data (State’s Data) will adhere to reasonable security standards no less protective than the security standards at facilities where Provider stores and processes its own information of a similar type. Provider has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data, protect against anticipated threats or hazards to the security or integrity of Customer Data, and protect against unauthorized access to or use of Customer Data.
- 1.2 Federal Information Security Management Act (FISMA). The Google Apps Core Services received a FISMA “Authorization to Operate” for a Moderate impact system. Provider will continue to maintain a System Security Plan (SSP) for the Google Apps Core Services, based on NIST 800-53 Rev. 3, or a similarly applicable standard. If Provider does not maintain this SSP as stated, the State’s sole and exclusive remedy will be the State’s ability to terminate the Agreement upon thirty (30) days prior written notice.
- 1.3 Modifications.
 - a. To the Services. Provider may make commercially reasonable changes to the Services, from time to time. If Provider makes a material change to the Services, Provider will inform the State, provided that the State has subscribed to be informed about such change.
 - b. To URL Terms. Provider may make commercially reasonable changes to the URL Terms from time to time. If Provider makes a material change to the URL Terms, the State will be informed by either an email to the Notification Email Address or via the Admin Console, or will be alerted by Carahsoft or Reseller. If the change has a material adverse impact on the State and the State does not agree to the change, the State must so notify Provider via the Help Center within thirty (30) days after receiving notice of the change. If the State notifies Provider as required, or Carahsoft or Reseller notifies Provider on the State’s behalf, then the State will remain governed by the terms in effect immediately prior to the change until the end of the then-current term for the affected Services. If the affected Services are renewed, they will be renewed under Provider’s then current URL Terms.
- 1.4 Customer Domain Name Ownership. Prior to providing the Services, Provider, Carahsoft or Reseller may verify that the State owns or controls the State’s Domain Names. If the State does not own, or control, the State’s Domain Names, then Provider, Carahsoft or Reseller will have no obligation to provide the State with the Services.
- 1.5 Ads. Google will not serve Ads within the Services provided under this Agreement or use Customer Data for Ads purposes.
- 1.6 Google Apps Vault. If the State purchases Google Apps Vault, the following additional terms apply:
 - a. Retention. Provider will have no obligation to retain any archived Customer Data beyond the retention period specified by the State (other than for any legal holds). If the State does not renew Google Apps Vault, Provider will have no obligation to retain any archived Customer Data.
- 1.7 Data Security, Audit, Data Deletion, Data Use.
 - a. Security Measures. Provider will take and implement appropriate technical, administrative and organizational measures designed to protect Customer Data against a Security Incident (“Security Measures”). As of the Effective Date Provider has implemented the Security Measures in Appendix I. Provider may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the security of the Services. The State agrees that Provider has no obligation to protect Customer Data that the State elects to store outside of Provider’s systems (e.g. offline or on-premise storage). In no instances would Customer Data be stored outside of the United States in countries on the Office of Foreign Assets Control (“OFAC”) embargoed countries list unless authorized (via license, exemption or exception) under United States Export Control Laws. Google’s current list of facility locations can be found at the following URL: <http://www.google.com/about/datacenters/inside/locations/index.html> (the facility locations and such URL link may be updated or modified by Google from time to time).
 - b. Provider Staff. Provider will take appropriate steps to ensure compliance with the Security Measures by its employees and contractors to the extent applicable to their scope of performance.
 - c. Security Incident. If Provider becomes aware of a Security Incident, Provider will promptly notify the State of such Security Incident, having regard to the nature of such Security Incident and consistent with FedRAMP requirements described in Google’s System Security Plan. Provider will use commercially reasonable efforts to work with the State in good faith to address any known breach of

Provider's security obligations under the TOS. The State is solely responsible for fulfilling any third party notification obligations. "Security Incident" means (a) any unlawful access to Customer Data stored in the Services or systems, equipment or facilities of Google, or (b) unauthorized access to such Services, systems, equipment or facilities that results in loss, disclosure or alteration of Customer Data.

- d. Security Certification. During the Term, Provider will maintain its ISO/IEC 27001:2005 Certification or a comparable certification ("ISO Certification") for the Services. The certificate is available on Provider's website or through the State's Admin Console, or other electronic means.
 - e. Security Audit. During the Term, Provider will maintain its Service Organization Control (SOC) 2 report (or a comparable report) on Provider's systems examining logical security controls, physical security controls, and system availability ("Audit Report") as related to the Services. Google will make the following available for review by Customer (including Customer Affiliates' superintendents who are End Users upon request): (i) the certificate issued in relation to Google's ISO Certification; (ii) the then-current SOC 3 report; (iii) a summary or redacted version of the then-current confidential Audit Report; or (iv) the then-current confidential Audit Report.
 - f. Distribution of Audit Report. Provider will update the Audit Report, at least every eighteen (18) months. A summary of the Audit Report is available on Provider's website or through the State's Admin Console, or other electronic means.
 - g. Customer and End User Deletion. For the term of the Agreement, Provider will provide the State or End Users with the ability to correct, block, export and delete State Data in a manner consistent with the functionality of the Services. Once the State or End User deletes Customer Data and such Customer Data cannot be recovered by the State or End User, such as from the "trash" ("Customer-Deleted Data"), Provider will delete such Customer-Deleted Data from its systems as soon as reasonably practicable and within a maximum period of 180 days.
 - h. Deletion on Termination. On expiry or termination of the Agreement, Provider will delete all Customer-Deleted Data from its systems as soon as reasonably practicable and within a maximum period of 180 days by overwriting the data or destroying the encryption keys.
 - i. Access to Data. Provider will make available to the State the Customer Data in accordance with the terms of the Agreement in a manner consistent with the functionality of the Services, including the applicable SLA and during any Transition Term, if applicable. To the extent the State, in its use and administration of the Services, does not have the ability to amend or delete Customer Data, (as required by applicable law) or migrate Customer Data to another system or service Provider will comply with any reasonable requests by the State to assist in facilitating such actions to the extent Provider is legally permitted to do so and has reasonable access to the Customer Data.
 - j. Data Use. Provider will access and use Customer Data in accordance with the State's instructions. State instructions may be (i) provided by the State via the Admin Console, (ii) initiated by the State and End Users in their use of the Services, (ii) per the written instructions of the State. The State instructs Provider to access and use Customer Data to provide the Services (which includes the detection, prevention and resolution of security and technical issues).
 - k. Use Restrictions. Provider will only access and use Customer Data in accordance with this Agreement and will not access or use Customer Data for any other purpose.
 - l. Decommissioned Disks. If Customer Data is stored on certain disks that have experienced performance issues, errors or hardware failure, such disks may be decommissioned ("Decommissioned Disk"). Such Decommissioned Disk will be sanitized in a manner as stated in NIST SP 800-88r1 before leaving Google's premises either for reuse or destruction.
- 1.8 Use of the Services by Customer Affiliates. The State will collect and maintain countersigned Memorandums of Understanding (MOUs) from each Customer Affiliate governed by the Louisiana Department of Education who uses Services under this Agreement. The State will act as the overarching authority such Customer Affiliates under this Agreement and subsequent Memorandums of Understanding. Provider acknowledges that Customer Affiliate may submit student data directly to the Provider. Provider will treat such data in accordance with Section 7.5 of the Agreement.

2. State Obligations.

- 2.1 Compliance. The State will use the Services in accordance with the Acceptable Use Policy. Provider may make new applications, features or functionality available from time to time through the Services, the use of which may be contingent upon the State's agreement directly or through Carahsoft or Reseller, as applicable to additional terms. In addition, Provider will make other Non-Google Apps Products, separate from the Services, available to the State and its End Users in accordance with the Non-Google Apps Product Terms and the applicable product-specific terms of service. The State can enable or disable the Non-Google Apps Products at any time through the Admin Console. The State agrees that its use of the Domain Service is subject to its compliance with the Domain Service Terms.
- 2.2 Aliases. The State is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for the State's Domain Names but Provider may monitor emails sent to these aliases for the State's Domain Names to allow Provider to identify Services abuse.
- 2.3 State Administration of the Services. The State may specify one or more Administrators through the Admin Console who will have the rights to access Admin Account(s) and to administer the End User Accounts. The State, Carahsoft and Reseller, if applicable, are

responsible for: (a) maintaining the confidentiality of the password and Admin Account(s); (b) designating those individuals who are authorized to access the Admin Account(s); and (c) ensuring that all activities that occur in connection with the Admin Account(s) comply with the Agreement. The State agrees that Provider's responsibilities do not extend to the internal management or administration of the Services for the State and that Provider is merely a data-processor.

- 2.4 End User Consent. The State's Administrators may have the ability to access, monitor, use, or disclose data available to End Users within the End User Accounts. The State will obtain and maintain all required consents from End Users to allow: (i) the State's access, monitoring, use and disclosure of this data and Provider providing the State with the ability to do so, and (ii) Provider to provide the Services.
- 2.5 Unauthorized Use. The State will use commercially reasonable efforts to prevent unauthorized use of the Services, and to terminate any unauthorized use. The State, Carahsoft or Reseller will promptly notify Provider of any unauthorized use of, or access to, the Services of which it becomes aware.
3. Requesting End User Accounts; Services Term. Requesting End User Accounts, as well as initial and renewal terms for the Services, are to be decided upon between the State and Carahsoft or Reseller, if applicable.
4. Payment. The State can purchase Services from either Carahsoft or an authorized Reseller. The State will pay Carahsoft or Reseller, if applicable, for the Services.
5. Technical Support Services.
 - 5.1 By the State. The State, Carahsoft or Reseller will, at its own expense, respond to questions and complaints from End Users or third parties relating to the State's or End Users' use of the Services. The State, Carahsoft or Reseller will use commercially reasonable efforts to resolve support issues before escalating them to Provider.
 - 5.2 By Provider. If the State, Carahsoft or Reseller cannot resolve a support issue consistent with the above, then the State, Carahsoft or Reseller (as applicable based on the agreement between Provider and Carahsoft) may escalate the issue to Provider in accordance with the TSS Guidelines. Provider will provide TSS to the State, Carahsoft or Reseller (as applicable) in accordance with the TSS Guidelines.
6. Suspension.
 - 6.1 Of End User Accounts by Carahsoft or Provider. If Carahsoft or Provider becomes aware of an End User's violation of the Agreement, then they may specifically request that the State Suspend the applicable End User Account. If Customer fails to comply with this request to Suspend an End User Account, then Carahsoft or Provider may do so. The duration of any Suspension by Carahsoft or Provider will be until the applicable End User has cured the breach which caused the Suspension.
 - 6.2 Emergency Security Issues. Notwithstanding the foregoing, if there is an Emergency Security Issue, then Carahsoft or Provider may automatically Suspend the offending use. Suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the Emergency Security Issue. If Carahsoft or Provider Suspends an End User Account for any reason without prior notice to the State, at the State's request, the party that has suspended the account will provide the State with the reason for the Suspension as soon as is reasonably possible.
7. Confidential Information.
 - 7.1 Obligations. Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates, employees and agents in violation of this Section.
 - 7.2 Exceptions. Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.
 - 7.3 Required Disclosure. Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.
 - 7.4 Third Party Requests. The State is responsible for responding to Third Party Requests. The party which receives the Third Party Request, Carahsoft or Provider as applicable, will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify the State of its receipt of a Third Party Request in a manner permitted by law; (b) comply with the State's reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide the State with the information or tools required for the State to respond to the Third Party Request. The State will first use the Admin Tool to access the required information, and will contact Carahsoft or Provider only if it is insufficient for the State's needs.
 - 7.5 FERPA. The parties acknowledge that (a) the State's Data may include personally identifiable information from education records that are subject to FERPA ("FERPA Records"); and (b) to the extent that the State's Data includes FERPA Records, Provider will be considered a

"School Official" (as that term is used in FERPA and its implementing regulations) and will comply with FERPA. Provider acknowledges and agrees that (a) it will not disclose FERPA Records to any other party without the prior consent of the "Parent" or "Eligible Student" (as such terms are defined in FERPA), or as otherwise may be permitted under FERPA or as provided for in this Agreement, and (b) (2) may only use FERPA Records for legitimate educational interests under this Agreement.

8. Intellectual Property Rights: Brand Features.

- 8.1 Intellectual Property Rights. Except as expressly set forth herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, the State owns all Intellectual Property Rights in State's Data, and Provider owns all Intellectual Property Rights in the Services.
- 8.2 Display of Brand Features. Carahsoft or Provider may display only those State Brand Features authorized by the State (such authorization is provided by the State uploading its Brand Features into the Services), and only within designated areas of the Service Pages. The State may specify the nature of this use using the Admin Console. Provider may also display Provider Brand Features on the Service Pages to indicate that the Services are provided by Provider. Neither party may display or use the other party's Brand Features beyond what is allowed in this Agreement without the other party's prior written consent.
- 8.3 Brand Features Limitation. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights in those Brand Features. A party may revoke the other party's right to use its Brand Features pursuant to this Agreement with written notice to the other and a reasonable period to stop the use.

9. Restrictions on Use. Unless Provider specifically agrees in writing, the State will not, and will use commercially reasonable efforts to make sure a third party does not: (a) sell, resell, lease, or the functional equivalent, the Services to a third party (unless expressly authorized in this Agreement); (b) attempt to reverse engineer the Services or any component; (c) attempt to create a substitute or similar service through use of, or access to, the Services; (d) use the Services for High Risk Activities; or (e) use the Services to store or transfer any State Data that is controlled for export under the International Traffic in Arms Regulations (ITAR). The State is solely responsible for any applicable compliance with HIPAA.

10. Publicity. The State agrees that Carahsoft or Provider may include the State's name or Brand Features in a list of Carahsoft or Provider customers. The State also agrees that Carahsoft or Provider may verbally reference the State as a customer of the products or services that are the subject of this Agreement. Google will not use the State's name or Brand Features in the context of an actual or implied endorsement of the Services. This section is subject to Section 8.3.

11. Government Purposes. The Services were developed solely at private expense and are commercial computer software and related documentation within the meaning of the applicable civilian and military Federal acquisition regulations and any supplements thereto. If the user of the Services is an agency, department, employee, or other entity of the United States Government, under FAR 12.212 and DFARS 227.7202, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Services, including technical data or manuals, is governed by the terms and conditions contained in this Agreement, which is materially consistent with Provider's standard commercial license agreement.

12. Representations, Warranties and Disclaimers.

- 12.1 Representations and Warranties. Each party represents that it has full power and authority to enter into the Agreement. Each party warrants that it will comply with all laws and regulations applicable to its provision, or use, of the Services, as applicable (including applicable security breach notification law). Carahsoft warrants that they will provide the Services in accordance with the applicable Provider SLA. Customer acknowledges and agrees that it is solely responsible for compliance with the Children's Online Privacy Protection Act of 1998, including, but not limited to, obtaining parental consent concerning collection of students' personal information used in connection with the provisioning and use of the Services by the State and End Users. The State represents and warrants that it is a state entity.
- 12.2 Disclaimers. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, NEITHER PARTY MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. NEITHER PROVIDER NOR CARAHSOFT MAKE ANY REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE SERVICES. THE STATE ACKNOWLEDGES THAT THE SERVICES ARE NOT A TELEPHONY SERVICE AND THAT THE SERVICES ARE NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY SERVICES CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS.

13. Term and Termination.

- 13.1 Term. This Agreement will remain in effect for the Term.
- 13.2 Termination for Breach. Either party may suspend performance or terminate this Agreement, or Carahsoft (through Provider) may cease providing the Services, if: (i) the other party is in material breach of the Agreement and fails to cure that breach within thirty (30) days after receipt of written notice or (ii) the other party is in material breach of this Agreement more than two times notwithstanding any cure of such breaches.

13.3 Effects of Termination. If this Agreement terminates, then: (i) the rights granted by one party to the other will cease immediately (except as set forth in this Section); and (ii) upon request each party will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other party.

14. Indemnification.

14.1 By the State. Unless prohibited by applicable law and without waiving sovereign immunity, Customer will indemnify, defend, and hold harmless Carahsoft from and against all liabilities, damages, and costs arising out of a third party claim: (i) regarding the content or substance of State's Data or State's Domain Names; (ii) that the State's Brand Features infringe or misappropriate any patent, copyright, trade secret or trademark of a third party; or (iii) regarding the State's use of the Services in violation of the Acceptable Use Policy.

14.2 By Carahsoft. Carahsoft will indemnify, defend, and hold harmless the State from and against all liabilities, damages, and costs arising out of a third party claim that Provider's technology used to provide the Services or any Carahsoft's Brand Feature infringe or misappropriate any patent, copyright, trade secret or trademark of such third party. Notwithstanding the foregoing, in no event shall Carahsoft have any obligations or liability under this Section arising from: (i) use of any Services or Provider Brand Features in a modified form or in combination with materials not furnished by Carahsoft, and (ii) any content, information or data provided by the State, End Users or other third parties with whom the State or their End Users interact with via the Services or as related to the Services.

14.3 Possible Infringement.

a. Repair, Replace, or Modify. If Carahsoft reasonably believes the Services infringe a third party's Intellectual Property Rights, then Carahsoft will: (a) obtain the right for the State, at its expense, to continue using the Services; (b) provide a non-infringing functionally equivalent replacement; or (c) modify the Services so that they no longer infringe.

b. Suspension or Termination. If Customer is not offered one of the options in Section 14.3a, then Carahsoft may suspend or terminate the State's use of the impacted Services. If Carahsoft terminates the impacted Services, then Carahsoft will notify the State.

14.4 General. The party seeking indemnification will promptly notify the other party of the claim and cooperate with the other party in defending the claim. The indemnifying party has full control and authority over the defense, except that: (a) any settlement requiring the party seeking indemnification to admit liability or to pay any money will require that party's prior written consent, such consent not to be unreasonably withheld or delayed; and (b) the other party may join in the defense with its own counsel at its own expense. THE INDEMNITIES ABOVE ARE A PARTY'S ONLY REMEDY UNDER THIS AGREEMENT FOR VIOLATION BY THE OTHER PARTY OF A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS.

15. Limitation of Liability.

15.1 Limitation on Indirect Liability. NEITHER PARTY WILL BE LIABLE UNDER THIS AGREEMENT FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.

15.2 Limitation on Amount of Liability. NEITHER PARTY MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE GREATER OF (A) TWICE THE AMOUNT PAID BY CUSTOMER TO CARAHSOFT, OR RESELLER, IF APPLICABLE, FOR THE SERVICES DURING THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO LIABILITY OR (B) ONE HUNDRED THOUSAND DOLLARS (USD\$100,000).

15.3 Exceptions to Limitations. These limitations of liability apply to the fullest extent permitted by applicable law but do not apply to breaches of confidentiality obligations, violations of a party's Intellectual Property Rights by the other party, or indemnification obligations.

16. Miscellaneous.

16.1 Notices. Unless specified otherwise herein, (a) all notices must be in writing and addressed to the attention of the other party's legal department and primary point of contact and (b) notice will be deemed given: (i) when verified by written receipt if sent by personal courier, overnight courier, or when received if sent by mail without verification of receipt; or (ii) when verified by automated receipt or electronic logs if sent by facsimile or email.

16.2 Carahsoft may use its authorized resellers to submit quotes to the State of Louisiana and its Affiliates and others authorized by the State to purchase under this Agreement.

16.3 Assignment. Neither party may assign or transfer any part of this Agreement without the written consent of the other party, except to an Affiliate, but only if: (a) the assignee agrees in writing to be bound by the terms of this Agreement; and (b) the assigning party remains liable for obligations incurred under the Agreement prior to the assignment. Any other attempt to transfer or assign is void.

16.4 Change of Control. Upon a change of control (for example, through a stock purchase or sale, merger, or other form of corporate transaction): (a) the party experiencing the change of control will provide written notice to the other party within thirty (30) days after the change of control; and (b) the other party may immediately terminate this Agreement any time between the change of control and thirty days after it receives the written notice in subsection (a).

- 16.5 Force Majeure. Neither party, nor Provider, will be liable for inadequate performance to the extent caused by a condition (for example, natural disaster, act of war or terrorism, riot, labor condition, governmental action, and Internet disturbance) that was beyond the party's reasonable control.
- 16.6 No Waiver. Failure to enforce any provision of this Agreement will not constitute a waiver.
- 16.7 Severability. If any provision of this Agreement is found unenforceable, the balance of the Agreement will remain in full force and effect.
- 16.8 No Agency. Carahsoft, the State, Provider and Reseller, if applicable, are independent contractors and this Agreement does not create an agency, partnership or joint venture.
- 16.9 No Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement.
- 16.10 Equitable Relief. Nothing in this Agreement will limit either party's ability to seek equitable relief.
- 16.11 Venue. The parties agree to venue in accordance with LA Rev Stat § 39:1691.
- 16.12 Amendments. Any amendment must be in writing and expressly state that it is amending this Agreement.
- 16.13 Survival. The following sections will survive expiration or termination of this Agreement: Section 7, 8.1, 13, 14, 15 and 16.
- 16.14 Entire Agreement. This Agreement, and all documents referenced herein, is the parties' entire agreement relating to its subject and supersedes any prior or contemporaneous agreements on that subject. If Customer is presented with a similar agreement on the same subject matter upon its log in to use the Services, this Agreement supersedes and replaces that agreement. The terms located at a URL and referenced in this Agreement are hereby incorporated by this reference.
- 16.15 Interpretation of Conflicting Terms. If there is a conflict between the documents that make up this Agreement, the documents will control in the following order: the Agreement, and the terms located at any URL.
- 16.16 Counterparts. The parties may enter into this Agreement in counterparts, including facsimile, PDF or other electronic copies, which taken together will constitute one instrument.

17. Definitions.

- "Acceptable Use Policy" means the acceptable use policy for the Services available at http://www.google.com/a/help/intl/en/admins/use_policy.html or such other URL as Provider through Carahsoft or Reseller if applicable, may provide.
- "Admin Account(s)" means the administrative account(s) provided to the State by Provider, or to Carahsoft by the State, for the purpose of administering the Services. The use of the Admin Account(s) requires a password, which Provider, through Carahsoft or Reseller, if applicable, will provide to the State.
- "Admin Console" means the online tool provided by Provider to Customer for use in reporting and certain other administration functions.
- "Administrators" mean the Customer-designated technical personnel who administer the Services to End Users on the State's behalf.
- "Ads" means online advertisements, excluding advertisements provided by any advertising products that are not part of the Services (for example, Google AdSense) that Customer chooses to use in connection with the Services, displayed by Provider to End Users.
- "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party. For the purposes of this TOS, Customer Affiliates includes all government agencies related to or governed by the State, the State of Louisiana Board of Regents, all State of Louisiana public universities and community colleges, and the State of Louisiana Department of Education and all public K-12 grade school districts.
- "Brand Features" means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.
- "Confidential Information" means information disclosed by a party to the other party under this Agreement that is marked as confidential or would normally be considered confidential under the circumstances. The State's Data is Confidential Information.
- "Customer Data or State's Data" means data, including email, provided, generated, transmitted or displayed via the Services by the State, or Carahsoft on behalf of the State.
- "Customer Domain Names or State's Domain Names" mean the domain names owned or controlled by the State, which will be used in connection with the Services.
- "Domain Service" means a service provided by Provider to the State purely for the State's convenience, where the State may, through a Provider-provided interface, register domain names through, or transfer domain names to, Registrar Partners (as defined in the Domain Service Terms).

“Domain Service Terms” means the terms at: http://www.google.com/a/help/intl/en/admins/domain_service_terms.html, or other such URL as may be provided by Provider.

“Emergency Security Issue” means either: (a) the State’s use of the Services in violation of the Acceptable Use Policy, which could disrupt: (i) the Services; (ii) other customers’ use of the Services; or (iii) the Provider network or servers used to provide the Services; or (b) unauthorized third party access to the Services.

“End Users” means the individuals State permits to use the Services.

“End User Account” means a Provider-hosted account established by the State through the Services for an End User.

“FERPA” means the Family Educational Rights and Privacy Act (20 U.S.C. 1232g) and the Family Educational Rights and Privacy Act Regulations (34 CFR Part 99), as amended or otherwise modified from time to time.

“Google Apps Core Services” means the following components of the Services: Gmail, Google Calendar, Google Contacts, Google Docs, Google Sheets, Google Slides, Google Groups, Google Talk, Google Hangouts, Google Sites, Google Drive, as well as the supporting general support system. These Google Apps Core Services are more fully described here: http://www.google.com/a/help/intl/en/users/user_features.html

“Help Center” means the Provider help center accessible at <http://www.google.com/support/> or other such URL as Provider may provide.

“High Risk Activities” means uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Services could lead to death, personal injury, or environmental damage.

“HIPAA” means the Health Insurance Portability and Accountability Act of 1996, as may be amended from time to time, and any regulations issued thereunder.

“Intellectual Property Rights” means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, moral rights law, and other similar rights.

“Non-Google Apps Products” means Provider products which are not part of the Services, but which may be accessed by End Users using their End User Account login and password. The Non-Google Apps Products are set forth at the following URL: <http://www.google.com/support/a/bin/answer.py?hl=en&answer=181865>, or such other URL as Provider may provide.

“Non-Google Apps Product Terms” means the terms found at the following URL: http://www.google.com/apps/intl/en/terms/additional_services.html, or such other URL as Provider may provide from time to time.

“Notification Email Address” means the email address designated by the State to receive email notifications from Provider. The State may provide a Distributor email address for this purpose if it so chooses. The State may change this email address through the Admin Console.

“Distributor” means the entity the State is paying to provide access to and use of the Services. For the purposes of this Agreement, Distributor refers to Carahsoft Technology Corp.

“SDN List” is the US Treasury Department’s List of Specially Designated Nationals.

“Service Pages” mean the web pages displaying the Services to End Users.

“Services” means, as applicable, the Google Apps for Government Services and Google Apps Vault provided by Provider and used by the State under this Agreement. The Services are as described here: http://www.google.com/a/help/intl/en/users/user_features.html, or other such URL as Provider may provide. For the purposes of this Agreement, the Google Apps for Government Services and Google Apps Vault include the Google Apps Core Services.

“SLA” means the Service Level Agreement located here: http://www.google.com/apps/intl/en/terms/reseller_sla.html, or such other URL as Provider may provide from time to time.

“Suspend” means the immediate disabling of access to the Services, or components of the Services, as applicable, to prevent further use of the Services.

“Term” means the term of the Agreement, which will begin on the Effective Date and will automatically renew on an annual basis unless terminated in writing to Carasoft pursuant to the Agreement, or pursuant to Customer’s agreement with Carahsoft. Under no circumstances will the Term be automatically renewed for more than ten (10) years from the Effective Date.

“Third Party Request” means a request from a third party for records relating to an End User’s use of the Services. Third Party Requests can be a lawful search warrant, court order, subpoena, other valid legal order, or written consent from the End User permitting the disclosure.

“TSS” means the technical support services provided by Provider to the Administrators during the Term pursuant to the TSS Guidelines.

"TSS Guidelines" means Provider's technical support services guidelines then in effect for the Services. TSS Guidelines are at the following URL: <http://www.google.com/a/help/intl/en/admins/tssg.html> or such other URL as Provider may provide.

"URL Terms" means the Acceptable Use Policy, the SLA and the TSS Guidelines.

IN WITNESS WHEREOF, the parties have executed this Agreement by persons duly authorized as of the date signed below.

Carahsoft Technology Corp.

By: Digitally signed by Terry Drinkwine
(Authorized Signature)
DN: cn=Terry Drinkwine, o=Carahsoft
Technology, ou,
Title: email=terry.drinkwine@carahsoft.co
m, c=US
Date: Date: 2016.08.03 08:51:41 -04'00'

Customer: State of Louisiana

By: Richard Howze
(Authorized Signature)
RICHARD HOWZE
(Print Name)
Title: STATE CIO
Date: 8-4-16

Appendix I

Security Measures

As of the Effective Date, Provider abides by the Security Measures set out in this Exhibit. During the Term of the Agreement, the Security Measures may change but Provider agrees that any such change shall not cause a material degradation in the security of the Services.

I. Data Center & Network Security.

(a) Data Centers.

Infrastructure. Provider maintains geographically distributed data centers. Provider stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Provider to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. Provider servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Provider employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. Provider replicates data over multiple systems to help to protect against accidental destruction or loss. Subcontractor has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks & Transmission.

Data Transmission. Data centers are connected via encrypted links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Subcontractor transfers data via Internet standard protocols.

External Attack Surface. Provider employs multiple layers of network devices and intrusion detection to protect its external attack surface. Provider considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Provider intrusion detection involves:

1. Tightly controlling the size and make-up of Provider's attack surface through preventative measures;
2. Employing intelligent detection controls at data entry points; and
3. Employing technologies that automatically remedy certain dangerous situations.

Provider makes available security logs in the Admin Console that include failed and successful logins, IP addresses and locations to assist the Customer in investigating security incidents.

Incident Response. Provider monitors a variety of communication channels for security incidents, and Provider's security personnel will react promptly to known incidents.

Encryption Technologies. Provider makes HTTPS encryption (also referred to as SSL or TLS) available.

2. Access and Site Controls.

(a) Site Controls.

On-site Data Center Security Operation. Provider's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. Provider maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Provider's data centers employ an electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 90 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. Provider has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Provider's infrastructure security personnel are responsible for the ongoing monitoring of Provider's security infrastructure, the review of the Services, and for responding to security incidents.

Access Control and Privilege Management. The State's administrators and end users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.

Internal Data Access Processes and Policies – Access Policy. Provider's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Provider aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Provider employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing RSA keys are designed to provide Provider with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Provider requires the use of unique user IDs, strong passwords; two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Provider's internal data access policies and training.

Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Provider uses hardware tokens.

3. Data.

(a) Data Storage, Isolation & Authentication.

Provider stores data in a multi-tenant environment on Google-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. Subcontractor logically isolates data on a per end user basis at the application layer. Provider logically separates the State's data, including data from different end users, from each other, and data for an authenticated end user will not be displayed to another end user (unless the former end user or administrator allows the data to be shared). A central authentication system is used across all Services to increase uniform security of data.

The State will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable the State to determine the product sharing settings applicable to end users for specific purposes. The State may choose to make use of certain logging capability that Provider may make available via the Services, products and APIs. The State agrees that its use of the APIs is subject to the API Terms of Use.

(b) Decommissioned Disks and Disk Erase Policy.

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Provider's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security.

Provider personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Provider conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Provider's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling customer data are required to complete additional requirements appropriate to their role (e.g. certifications). Provider's personnel will not process customer data without authorization.

Amendment to the Services Agreement – Google Apps
Appendix 2: Elementary and Secondary Education Data Sharing Agreement

This Amendment (“Amendment”) replaces Appendix 2: Elementary and Secondary Education Data Sharing Agreement within the Services Agreement – Google Apps Services Agreement entered into between the parties set forth in the signature block on August 4, 2016.

Appendix 2: Elementary and Secondary Education Data Sharing Agreement

WHEREAS, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and its implementing regulations codified at 34 C.F.R 99. 1 et seq. make personally identifiable student information in education records confidential and, subject to certain exceptions, prohibits the disclosure of such information to third parties,

WHEREAS, FERPA and its implementing regulations allow for an educational agency or institution to share personally identifiable student-level data with third party service providers,

WHEREAS, R.S. 17:3914 allows for Local Educational Agencies to contract with a private entity for student and other educational services and release personally identifiable information pursuant to the terms of the a contract,

WHEREAS, the Louisiana Department of Education (hereinafter referred to as “State”) and Carasoft Technology Corp. (hereinafter referred to as “Contractor”) have entered into a contractual arrangement (the “Services Contract”), pursuant to which the Contractor, through Google Inc. (“Google”), a third party service provider, will provide Services (which will have the meaning given to it under the Services Contract) to State and Local Educational Agencies (LEAs).

WHEREFORE, the State and Contractor do enter into this Agreement subject to the terms and conditions as specified herein.

This Data Sharing Agreement (hereinafter referred to as “Agreement”), upon execution, shall supersede and replace all other Data Sharing Agreements that are in existence between the Louisiana Department of Education and the Contractor. Capitalized terms not defined in this Agreement will have the meaning ascribed to them in the Services Contract.

1. Local Educational Agencies Stipulation

The Contractor acknowledges that local educational agencies (LEAs) in Louisiana submit student data directly to the Contractor or Google pursuant to the Services Contract. The Contractor hereby agrees, to be bound, and will ensure that Google is bound, vis-à-vis any and all such Louisiana LEAs that unilaterally sign an addendum to this data sharing agreement, by all of the provisions of this Agreement with respect to any student data provided directly to the Contractor or Google by such Louisiana LEAs pursuant to the Services Contract. Any and all such Louisiana LEAs agree to access and use the Services in accordance with the terms and conditions of the Services Contract

and to be bound by such Services Contract as if each had entered into that Services Contract directly with Contractor.

2. Purpose of the Disclosure

Any Customer Data disclosed to Contractor or Google pursuant to this Agreement and the Services Contract may only be used for the sole purpose of Contractor or Google providing the Services (which includes the detection, prevention and resolution of security and technical issues) and performing its obligations under this Agreement and Services Contract, and for State and the LEAs to access and use the Services.

3. Data

The State and LEAs have the ability to access its Customer Data in the Services in a manner consistent with the functionality of the Services, as well as to amend or delete such data. Specific data elements shared by LEAs will be detailed within a countersigned Memorandum of Understanding as stated in Section 1.8 of the Services Contract, The State and LEAs reserve the right to withhold any data detailed in the Memorandum if determined, in their sole discretion, that disclosure of such data would violate any provision of state or federal law.

4. Confidentiality

Customer Data is confidential information and Contractor will, and will ensure that Google will, protect and treat Customer Data in accordance with Section 7 of the Services Contract. Contractor will, and ensure that Google will, process, store, limit access to, and delete Customer Data in accordance with its Security Measures that are attached as Appendix 1 to the Services Contract.

5. Restrictions on Use

Contractor will, and will ensure that Google will, only access and use Customer Data in accordance with this Agreement and the Services Contract and will not access or use Customer Data for any other purpose.

6. Indemnification

By the LEA. Unless prohibited by applicable law and without waiving sovereign immunity, LEA will indemnify, defend, and hold harmless Carahsoft from and against all liabilities, damages, and costs arising out of a third party claim: (i) regarding the content of the substance of LEA's Customer Data or LEA's Customer Domain Names; (ii) that the LEA's Customer Brand Features infringe or misappropriate any patent, copyright, trade secret or trademark of a third party; or (iii) regarding the LEA's use of the Services in violation of the Acceptable Use Policy.

7. Ownership

Except as expressly set forth in the Services Contract or this Agreement, neither party is granted any rights, implied or otherwise, to the other party's content or State Data or Customer Data or any of the other party's intellectual property. As between the parties, the State owns all Intellectual Property Rights in State's Data. Further, the LEA owns all intellectual property rights of LEA's data.

8. Security Audits

Pursuant to the Services Contract, Contractor will ensure that Google (a) maintains its Service Organization Control (SOC) 2 report (or a comparable report) on Google's systems examining logical security controls, physical security controls, and system availability ("Audit Report") as related to the Services; (b) updates the Audit Report, at least every eighteen (18) months and (c) makes a summary of the Audit Report is available to State or the LEAs.

9. Security Breach

Pursuant to Section 1.7c of the Services Contract, Contractor will ensure that if Google becomes aware of Security Incident (as defined in the Services Contract), the State or LEAs, as applicable, will be promptly notified of such Security Incident, having regard to the nature of such Security Incident and consistent with FedRAMP requirements described in Google's System Security Plan.

Contractor will ensure that Google will also take commercially reasonable steps, in accordance with industry standards, to remedy any Security Incident.

10. Term of Agreement

This Agreement shall begin on the same date as the effective date of the Services Contract and shall remain effective so long as the Services Contract remains in effect. This Agreement will automatically and immediately terminate when the Services Contract terminates or expires.

11. Termination for Convenience

The State may terminate this Agreement at any time by giving Contractor and all LEAs written notice of such termination. An LEA may terminate its participation in this Agreement by giving notice to the Contractor, without effect on the participation by the State or any other LEA.

12. Assignment of Agreement

Contractor shall not assign any interest in this Agreement by assignment, transfer, or novation, without prior written consent of the State, except in conjunction with the assignment of the Services Contract. Nothing in this provision shall preclude the Contractor from subcontracting

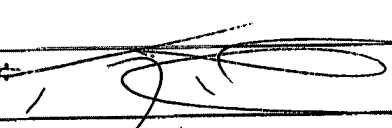
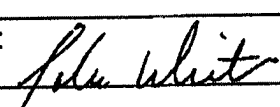
with third parties to perform work contemplated herein; however, the Contractor is responsible for ensuring that any such subcontractor(s) adhere to, and agree to be bound by, all provisions of this Agreement.

13. Venue. The parties agree to venue in accordance with LA Rev Stat § 39:1691.

14. Survival

Contractor's obligation under Clauses 2, 4, 5, 6, 7, 13 and 14 shall survive expiration and/or termination of this Agreement. Contractor's obligations under Clauses 8 and 9 shall survive expiration and/or termination of this Agreement until Contractor has fully complied with its obligation to destroy data as set forth herein.

IN WITNESS WHEREOF, the parties have executed this Agreement as of this 4th day of August, 2016.

Carahsoft Technology Corp	State of Louisiana
Name: Terry Drinkwine	Name: John C. White
Title: VP Sales	Title: State Superintendent of Education
Signature: 	Signature: 
Date: 12/12/16	Date: 12/14/16