

Salesforce.com Software Licensing and Support

Contract #505ENT-M16-VARSOFTWARE-00 ([link](#))

Mandatory: No
Cooperative: Yes (WI municipalities may use this contract)
P-Card: Yes

Contract Term

- The SFDC Service Terms will continue in effect until terminated by either party.
- Each Subscription purchased shall have its own annual term dictated by the time of purchase.

Scope

The Agreement is available for use by Wisconsin state agencies, * UW System, and other entities authorized to use state contracts such as Wisconsin municipalities as cited in Wisconsin statutes s. 16.73. The contract is optional for all Authorized Users.

This Agreement is for the purchase of subscription platform-as-a-service (PaaS) licensing by Salesforce, to provide cloud based application development. Salesforce will be used by agencies throughout the state to support application development and deployment.

DET's Innovation Center is the administrative contact and will provide support to agencies for the use of this agreement:

Ryan Baker
DOA – Innovation Center
608-261-2869
ryan.baker@wisconsin.gov

* UW System/ Education - Special Instructions

Contact: Ruth Ginzberg at 608.890.3961 or Email: rginzberg@uwsa.edu

Contact: Abbey Rossi, Account Executive Salesforce for Higher Education, at abbey.rossi@salesforce.com or 713-338-1039 to discuss license options for higher education institutions, which differ from license purchases per this contract.

Excluded from the Scope



The scope does not include the following:

- Purchase of Salesforce implementation services;
- Purchase of hardware or peripheral devices required to meet the functional or technical requirements; and
- Purchase of any equipment related to software functionality.

Note: **Implementation Services** can be purchased from [505ENT-O17-SALESFORCE-00](#) ([link](#)).

Software License Agreement (“SFDC Service Terms”)

Note that the Agreement is made between the State and Carahsoft Technology Corp who is the designated point of sales for Salesforce.

The Authorized User should read the terms and conditions to understand how to remain in compliance with licenses purchased.

Authorized Users will purchase the applicable Salesforce licenses through a reseller on the current mandatory state contract #505ENT-M16-VARSOFTWARE-00. The negotiated terms and conditions around licensure with Salesforce can be found on VendorNet. Municipalities may purchase software licenses from the Salesforce contract or through another manner consistent with their procurement policies.

Pricing

All pricing quoted may be considered the maximum price and may be negotiated further. Pricing cannot exceed the rate card, but can be lower. Each of the four resellers should be contacted with a request for specific product pricing in order to obtain the most competitive rate.

Pricing for renewal terms has been negotiated to a maximum annual increase of 5%.

All prices are firm during a contract term. Pricing can be lowered (or a higher discount) at any time during

the contract without requiring an amendment of the published rates.

Purchase Order (PO) and Invoicing

The PO and invoices shall be itemized.

Contacts for Quotes:

Refer to the [Reseller Contact List](#) posted to VendorNet.

Salesforce Direct Contact:

You may contact Salesforce directly to discuss product features, functionality or any other questions or concerns you may have:

Russell Schomberger

Sr. Account Executive | Salesforce Public Sector
rschomberger@salesforce.com
248-648-0119

Abbey Rossi

Account Executive | Salesforce Higher Education
abbey.rossi@salesforce.com
713-338-1039

Contract Use Questions and Feedback

Direct any questions, comments, complaints, or feedback to the contract manager. User feedback will help to address and correct contractual issues and to prepare for future solicitations.

Contract Manager

Ceotrid Gilbert
DOA – Bureau of Procurement
101 E. Wilson Street, 6th Floor
Madison, WI 53703
608-267-4506
ceotrid.gilbert@wisconsin.gov

SFDC Service Terms

This Contract is between the State of Wisconsin (the "State"), which includes all State of Wisconsin Agencies ("State Agencies") and the University of Wisconsin System and Campuses ("Universities"), as represented by its Department of Administration, located at 101 E Wilson Street, Madison, WI 53702, and Carahsoft Technology Corp ("Contractor" or "Carahsoft").

"Agency" or "State Agency" means an office, department, agency, institution of higher education, association, society or other body in the State of Wisconsin government created or authorized to be created by the State Constitution or any law, which is entitled to expend moneys appropriated by law, including the legislature and the courts, but not including an authority, as defined in Wis. Stat. s. 16.70(2).

"AppExchange" means the online directory of on-demand applications that work with the Service, located at <http://www.appexchange.com> or at any successor websites.

"Personally Identifiable Information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if that element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable: (a) the individual's Social Security number; (b) the individual's driver's license number or state identification number; (c) the number of the individual's financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (d) the individual's DNA profile; or (e) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation, and any other information protected by state or federal law.

"Properly-submitted Invoice" is one that is submitted in accordance with instructions contained on the State's Purchase Order, includes a reference to the proper Purchase Order number, and is submitted to the proper address for processing.

"Reseller" means Carahsoft.

"Service" means the online, Web-based application provided by SFDC via <http://www.salesforce.com> and/or other designated websites, including associated offline components but excluding AppExchange applications.

"Service Fee" means the contracted fees for use of the Service paid to SFDC by the State.

"SFDC" means salesforce.com, inc. and its affiliates.

"State Data" means All data provided by the State shall remain the property of the State. Contractor shall acquire no rights or licenses, including without limitation intellectual property rights or licenses, to use the data for its own purposes by virtue of this Contract or otherwise. Contractor may use the data provided by the State solely for the purposes of carrying out its obligations under this Contract and the administration and management of their respective services. Notwithstanding the above, usage data, storage utilization and similar statistical and consumption data relating to use of the services by the State is not the State's data/information and nothing in this Contract shall be construed as restricting Contractor's rights or interest in such service usage data. State Data as defined herein shall be used solely for the purposes of carrying out its obligations under this Contract and not sold, shared or otherwise provided, directly or indirectly to a third party without the express written permission of the State. All of the State's information stored by or accessed by the Contractor that is the result of any

processing of the State's data shall be the property of the State. The State shall have the ability to access the data except during downtime as may be provided in the SLA.

"**Third-Party Applications**" means online, Web-based applications and offline software products that are provided by third parties, interoperate with the Service, and are identified as third-party applications, including but not limited to those listed on the AppExchange.

"**User Guide**" means the online user guide for the Services, accessible via <http://www.salesforce.com>, as updated from time to time.

"**Users**" means Your employees, representatives, consultants, contractors or agents who are authorized to use the Service and have been supplied user identifications and passwords by You (or by Salesforce.com or Your Reseller at Your request).

"**You**" and "**Your**" and "**State**" means the entity which has contracted to purchase subscriptions to use the Service subject to the conditions of these SFDC Service Terms and may be used interchangeably with "State" herein.

"**Your Data**" means all electronic data or information submitted by You to the Service.

1. **Use of Service.**

- (a) User subscriptions cannot be shared or used by more than one User (but may be reassigned from time to time to new Users who are replacing former Users who have terminated employment with You or otherwise changed job status or function and no longer require use of the Service).
- (b) You (i) are responsible for all activities occurring under Your User accounts; (ii) are responsible for the content of all Your Data; (iii) shall use commercially reasonable efforts to prevent unauthorized access to, or use of, the Service, and shall notify Your Reseller or Salesforce.com promptly of any such unauthorized use You become aware of; and (iv) shall comply with all applicable local, state, federal and foreign laws and regulations in using the Service.
- (c) You shall use the Service solely for Your business purposes (not for the benefit of any third party) and shall not: (i) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share or otherwise commercially exploit or make the Service available to any third party, other than to Users or as otherwise contemplated by these SFDC Service Terms; (ii) send spam or otherwise duplicative or unsolicited messages in violation of applicable laws; (iii) send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material that is harmful to children or violates third party privacy rights; (iv) send or store viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs; (v) interfere with or disrupt the integrity or performance of the Service or the data contained therein; or (vi) attempt to gain unauthorized access to the Service or its related systems or networks.
- (d) You shall not (i) modify, copy or create derivative works based on the Service; (ii) frame or mirror any content forming part of the Service, other than on Your own intranets or otherwise for its own internal business purposes; (iii) reverse engineer the Service; or (iv) access the Service in order to (A) build a competitive product or service, or (B) copy any ideas, features, functions or graphics of the Service.

2. **Service Provision.** SFDC will use commercially reasonable efforts to make the Services available 24 hours a day, 7 days a week, except for: (a) planned downtime (of which SFDC shall give at least (8) hours' notice via the Services and which SFDC shall schedule to the extent practicable during the weekend hours from 6:00 p.m. Pacific time Friday to 3:00 a.m. Pacific time Monday), or (b) any unavailability caused by circumstances beyond SFDC's reasonable control,

including without limitation, acts of Nature, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving SFDC employees), or internet service provider failures or delays, and (iii) provide the Services only in accordance with applicable laws and government regulations.

3. **Support and Your Data.** Any exchange of data between You and Reseller, including Reseller's access of Your Data through the Service in connection with support matters, is solely between You and Reseller. SFDC shall not be responsible for any disclosure, modification or deletion of Your Data resulting from any such access by Reseller.
4. **Third-Party Products and Services.** Any acquisition by You of third-party products or services, including but not limited to Third-Party Applications and implementation, customization and other consulting services, and any exchange of data between You and any third-party provider, is solely between You and the applicable third-party provider. SFDC does not warrant or Support third-party products or services, whether or not they are designated by SFDC as "certified" or otherwise. SFDC certification requirements can be found at: <http://certification.salesforce.com/>
5. **Integration with Third-Party Applications.** If You install or enable Third-Party Applications for use with the Service, You acknowledge that SFDC may allow providers of those Third-Party Applications to access Your Data as required for the interoperation of such Third Party Applications with the Service. Salesforce.com shall not be responsible for any disclosure, modification or deletion of Your Data resulting from any such access by Third-Party Application providers. In addition, the Service may contain features designed to interoperate with Third-Party Applications (e.g., Google, Facebook or Twitter applications). To use such features, You may be required to obtain access to such Third-Party Applications from their providers. If the provider of any such Third-Party Application ceases to make the Third-Party Application available for interoperation with the corresponding Service features on terms that allow You continued use of such Third-Party Application, SFDC may cease providing such Service features without entitling You to any refund, credit, or other compensation.
6. **Proprietary Rights.** Subject to the limited rights expressly granted hereunder, Salesforce.com reserves all rights, title and interest in and to the Service, including all related intellectual property rights. The Service is deemed Salesforce.com confidential information, and You will not use it or disclose it to any third party except as permitted in these SFDC Service Terms.
7. **Intellectual Property Indemnification.** Carahsoft agrees to defend, indemnify and hold the State its officers, employees, or agents harmless against any liability or claim that the Service was created in part by violation of or violates the trade secrets of a third party or infringes a U.S. patent or copyright, and will pay resulting costs, damages and attorney's fees finally awarded, provided that: (a) the State promptly notifies Carahsoft of any such claim; (b) the State at Carahsoft's expense (except for the value of employees of the State) provides Carahsoft with all information and reasonable assistance necessary to defend or settle such liability or claim; and (c) Carahsoft has sole control of the defense and all related settlement negotiations.

If such liability or claim occurs, or in Carahsoft's opinion is likely to occur, the State agrees to permit Carahsoft, at Carahsoft's option and expense, either to procure for the State the right to continue using the Services or to replace or modify the Services so that it becomes non-infringing and provides, as is reasonably possible under the circumstances, the same capability as before. If it is not commercially reasonable to perform either of the foregoing options, then Carahsoft may terminate access to the Application and refund the Service Fees paid for the then current term.

To the extent permitted by applicable law, and without waiving any defense of sovereign immunity or any rights or limits to liability existing under Wisconsin law applicable to the

State, the State will be responsible for and Carahsoft will not be responsible for any claims made by an unaffiliated third party that:

- (i) any State Data or non-salesforce software salesforce hosts on behalf of the State infringes the third party's patent, copyright, or trademark or makes intentional unlawful use of its Trade Secret; or
- (ii) arise from State or its end user's violation of the terms of this Contract.
 - (ii) Any use of the Service not contemplated hereunder or in the documentation.
 - (iii) Any use of the Service in combination with other third party products.
 - (iv) Modification of the Service by Non-Salesforce or Carahsoft personnel.

8. **Your Data.** The State will own all right, title and interest in the State Data that is related to the Services provided by this Contract. The Contractor shall not access State user accounts or State Data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Contract and/or SLA, or (4) at the State's written request. Contractor shall not collect, access, or use user-specific State Data except as strictly necessary to provide Service to the State. No information regarding a State's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Contract.

9. **Confidential Information.**

(a) Disclosures.

In connection with the Service's performance hereunder, it may be necessary for the State to disclose to the Service Confidential Information. Carahsoft shall not use such information for any purpose other than the limited purposes set forth in this Contract, and all related and necessary actions taken in fulfillment of the obligations thereunder. Carahsoft shall hold all such information in confidence, and shall not disclose such information to any persons other than its directors, officers, employees, and agents who have a business-related need to have access to such information in furtherance of the limited purposes of this Contract and who have been apprised of, and agree to maintain, the confidential nature of such information in accordance with the terms of this Contract. Carahsoft may disclose Confidential Information of the State to the extent compelled by law to do so, provided Carahsoft gives the State prior notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at the State's cost, if the State wishes to contest the disclosure. If Carahsoft is compelled by law to disclose the State's Confidential Information as part of a civil proceeding to which the Carahsoft is a party, and the State is not contesting the disclosure, the State will reimburse Carahsoft for its reasonable cost of compiling and providing secure access to that Confidential Information.

Carahsoft shall institute and maintain such security procedures as are commercially reasonable to maintain the confidentiality of such information while in its possession or control, including transportation, whether physically or electronically.

Carahsoft shall maintain all information associated with this contract for a period of three (3) years from the date of termination of this Contract, and shall thereafter return or destroy said information as directed by the State.

(b) Indemnification in Event of Carahsoft Breach.

Indemnification: In the event of a breach of this Section by Carahsoft, Carahsoft shall indemnify, defend and hold harmless the State of Wisconsin and any of its officers, employees, or agents from any claims

arising from the acts or omissions of Carahsoft, and its Subcontractors, employees and agents including, but not limited to, disallowances or penalties from federal oversight agencies, and any court costs, expenses, and reasonable attorney fees, incurred by the State in the enforcement of this Section.

(c) Promotional Advertising and News Releases.

Reference to or use of the State of Wisconsin, the Great Seal of the State, the Wisconsin Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Contract shall not be made without prior written approval of the State.

10. **Suggestions.** You agree that Salesforce.com shall have a royalty-free, worldwide, transferable, sublicenseable, irrevocable, perpetual license to use or incorporate into the Service any suggestions, enhancement requests, recommendations or other feedback provided by You or Your Users relating to the operation of the Service.
11. **Fees and Payments.** Contracted fees for use of the Service represent a firm commitment: i.e., an order cannot be canceled during the term of the subscriptions, and the number of User subscriptions contracted for cannot be reduced in the middle of a subscription term. Subscription fees are paid annually in advance and nonrefundable.

The State shall pay SFDC's Properly-submitted Invoices within thirty (30) Days of receipt, provided that the Deliverables or Services to be provided to the State have been delivered, rendered, or installed, and accepted as specified in the solicitation document, Statement of Work (Contract) or this Contract.

If the State fails to pay a Properly-submitted Invoice within thirty (30) Days of receipt, it shall pay a late payment penalty as provided in §16.528, Wis. Stats. However, if the State declares a good faith dispute in regard to an invoice pursuant to §16.528 (3)(e), Wis. Stats., it may pay any undisputed portion of said invoice, and will be exempt from the prompt payment requirement for the disputed portion.

Upon expiration of the initial term, the Service Fee for each annual renewal term may not increase by more than three percent (3%) in the first three renewal terms and by no more than five percent (5%) for the fourth and fifth renewal terms. For the avoidance of doubt, Service Fees for each renewal term must be communicated by Carahsoft to the State at least ninety (60) days prior to expiration of the then current term and may not be increased for twelve (12) months following such Service Fee going into effect.

12. **Termination.** You may not cancel or terminate an executed subscription order. Salesforce.com reserves the right to terminate Your use of the Service due to a breach of these SFDC Service Terms by You or any User, after providing the State with (30) Days written notice of the State's right to cure a failure of the State to perform under these terms.

The State may terminate this Contract after providing SFDC with thirty (30) Days written notice of SFDCs' right to cure a failure to perform under the terms of this Contract.

In addition:

- (a) The State reserves the right to cancel this Contract in whole or in part without penalty, and without prior notice, if Carahsoft:
 - Files a petition in bankruptcy, becomes insolvent, or otherwise takes action to dissolve as a legal entity
 - Makes an assignment for the benefit of creditors

- Fails to maintain and keep in force all required insurance, permits and licenses as provided in this Contract;
- (b) The State reserves the right to cancel this Contract in whole or in part without penalty, with 30 days' notice, if Carahsoft:
- Fails to follow the sales and use tax certification requirements of s. 77.66 of the Wisconsin Statutes;
 - Incurs a delinquent Wisconsin tax liability;
 - Fails to submit a non-discrimination or affirmative action plan as required herein.
 - Fails to follow the non-discrimination or affirmative action requirements of subch. II, Chapter 111 of the Wisconsin Statutes (Wisconsin's Fair Employment Law); or
 - Becomes a state or federally debarred contractor.
13. **Warranty of Good Title.** Carahsoft represents and warrants that: (1) it has all of the necessary rights to grant the Services under these Service Terms; and (2) the Services and Application shall be provided free from any security interest or other lien or encumbrance of which Carahsoft at the time of contracting has no knowledge.
14. **Warranty.** Carahsoft warrants that it will provide the Service in a manner consistent with general industry standards reasonably applicable to the provision thereof; (ii) owns or otherwise has sufficient rights to the Service and the SFDC Technology to grant the rights and licenses granted herein; and (ii) the Service and SFDC Technology do not infringe any intellectual property rights of any third party. This warranty does not apply to any damage resulting from unauthorized use or negligence on the part of State.
15. **Limitation of Liability.**
- Exclusion of Consequential Damages.** IN NO EVENT SHALL SALESFORCE.COM OR CARAHSOFT HAVE ANY LIABILITY TO YOU OR ANY USER FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OR DAMAGES BASED ON LOST PROFITS, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT EITHER YOU OR SALESFORCE.COM HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- Limitation of Direct Damages.** Except for its obligations to indemnify the State under Section 7, or for any breach of its nondisclosure obligations (Section 9), the aggregate and cumulative liability of Carahsoft and Carahsoft representing its suppliers for damages hereunder shall not exceed the amount of one and a half (1.5) times the fees due by the State for the previous twelve (12) months under this Contract. Except for its obligations to indemnify Carahsoft under Section 7, or any breach of its obligations to comply with the License (Section 1), its payment obligations (Section 11), and its non-disclosure obligations (Section 9), the State's aggregate and cumulative liability for damages hereunder shall in no event exceed the amount of one and a half (1.5) times the fees due by the State for the previous twelve (12) months under this Contract.
16. **Further Contact.** Salesforce.com may contact you regarding new Salesforce.com service features and offerings.

17. **Third Party Beneficiary.** SFDC shall be a third party beneficiary to the agreement between You and Reseller solely as it relates to these SFDC Service Terms.

18. **Miscellaneous.**

- a) **STATE TAX EXEMPTION.** The State is exempt from payment of Wisconsin sales or use tax on all purchases.
- b) **ANTITRUST ASSIGNMENT.** By entering into this Contract, the Contractor conveys, sells, assigns and transfers to the State all rights, title and interest in and to all causes of action, claims and demands of whatever nature it may now have or hereafter acquire under the antitrust laws of the United States and the State, relating specifically to that proportionate amount of the particular Deliverables or Services purchased or acquired by the State under this Contract in so far as such obligations and rights do not conflict with the terms of this agreement.
- c) **CONTRACTOR COMPLIANCE AND RESPONSIBILITY FOR ACTIONS.** The Contractor shall at all times comply with and observe all federal, state, and local laws, ordinances, and regulations that are in effect during the term of this Contract that may affect the Contractor's work or obligations hereunder.

The Contractor shall be solely responsible for its actions and those of its agents, employees, or Subcontractors. Neither the Contractor nor any of the foregoing parties has authority to act or speak on behalf of the State.

- d) **APPLICABLE LAW.** The laws of the State of Wisconsin shall govern this Contract without reference to its conflict of law principles. All claims under, or otherwise with respect to, this Contract shall be brought and maintained in the state and federal courts located in Dane County, Madison, USA, and the parties hereby expressly consent (and waive any right to otherwise object) to the exclusive venue and jurisdiction of such courts.
- e) **CONTRACTOR'S INSURANCE RESPONSIBILITY.** The Contractor shall maintain the following insurance coverage:

Worker's compensation insurance, as required under Chapter 102 of the Wisconsin Statutes, for all of the Contractor's employees and Contracted Personnel engaged in the work performed under this Contract;

Commercial liability, bodily injury and property damage insurance against any claim(s) that may occur in carrying out the terms of this Contract, with a minimum coverage of one million dollars (\$1,000,000) liability for bodily injury and property damage including products liability and completed operations; and

Motor vehicle insurance for all owned, non-owned and hired vehicles that are used in carrying out the terms of this Contract, with a minimum coverage of one million dollars (\$1,000,000) per occurrence combined single limit for automobile liability and property damage.

Certificate of Insurance, showing up-to-date coverage, shall be on file in the Agency before the Contract may commence. (if applicable)

The State reserves the right to require higher or lower insurance limits, where warranted.

- f) **RECORDS, RECORDKEEPING AND RECORD RETENTION.** Pursuant to §19.36 (3) of the Wisconsin Statutes, all records of the Contractor that are produced or collected under this Contract are subject to disclosure pursuant to a public records request. The Contractor shall establish and maintain adequate records of all documentation developed or compiled and expenditures incurred under this Contract. All expenditure records shall be kept in accordance with Generally Accepted Accounting Procedures (GAAP). All procedures shall be in accordance

with federal, State and local laws or ordinances. The Contractor, following final payment, shall retain all records produced or collected under this Contract for three (3) years.

- g) **EXAMINATION OF RECORDS.** The State may during normal business hours, upon Two Weeks' notice, have access to and the right to examine, audit, excerpt, transcribe, and copy, on Contractor's premises, any of the Contractor's records and computer data storage media involving transactions directly pertinent to this Contract. If the material is on computer data storage media, the Contractor shall provide copies of the data storage media or a computer printout of such if the State so requests. Any charges for copies of books, documents, papers, records, computer data storage media or computer printouts provided by the Contractor shall not exceed the actual cost to the Contractor and shall be charged to the State. This provision shall survive the termination, cancellation, or expiration of this Contract.
- h) **DISPUTE RESOLUTION.** In the event of any dispute or disagreement between the parties under this Contract, whether with respect to the interpretation of any provision of this Contract, or with respect to the performance of either party hereto, each party shall appoint a representative to meet for the purpose of endeavoring to resolve such dispute or negotiate for an adjustment to such provision. No legal action of any kind, except for the seeking of equitable relief in the case of the public's health, safety or welfare, may begin in regard to the dispute until this dispute resolution procedure has been elevated to the Contractor's highest executive authority and the equivalent executive authority within the State contracting agency, and either of the representatives in good faith concludes, after a good faith attempt to resolve the dispute, that amicable resolution through continued negotiation of the matter at issue does not appear likely.
- i) **BREACH NOT WAIVER.** A failure to exercise any right, or a delay in exercising any right, power or remedy hereunder on the part of either party shall not operate as a waiver thereof. Any express waiver shall be in writing and shall not affect any event or Default other than the event or Default specified in such waiver. A waiver of any covenant, term or condition contained herein shall not be construed as a waiver of any subsequent breach of the same covenant, term or condition. The making of any payment to the Contractor under this Contract shall not constitute a waiver of Default, evidence of proper Contractor performance, or Acceptance of any defective item or work furnished by the Contractor.
- j) **ASSIGNMENT.** No right or duty in whole or in part of the contractor under this contract may be assigned or delegated without the prior written consent of the State of Wisconsin. Even in the event of an approved assignment, if the State encounters a degradation in service or an unwarranted price increase as a result of the assignment, the State may terminate the Contract without penalty, for a pro rata refund.
- k) **USER OVERAGES.** If at any point during the Term, the State activates additional User(s) totaling more than the number specified in the Quote, the additional User(s) will be treated as new Users. The new User(s) will be billed to the State upon its activation on a prorated basis for the time remaining in the Term. Such additional Users shall also be added to a Renewal Term, if applicable.
- l) **USERS ORDERED UNDER PRIOR AGREEMENTS.** It is expressly agreed that any Users ordered pursuant to any other agreement with SFDC shall now be subject to the terms of this Contract.
- m) **NO SERVICE BUREAU.** The State will not use Services in a service bureau capacity except where charges are a cost recovery mechanism related to the States' internal chargeback procedures.

This Contract and the documents incorporated by reference into the Contract constitute the entire agreement of the parties and supersede all prior communications, representations or agreements between the parties, whether oral or written. This Contract may not be modified or amended except by mutual agreement of both parties in writing.

IN WITNESS WHEREOF, this Contract has been duly executed by authorized signatories of the State and SFDC on the dates set forth below.

CARASOFT TECHNOLOGY CORP.

Digitally signed by
Patrick Gallagher
DN: cn=Patrick
Gallagher,
o=Carahsoft
Technology Corp., ou,
email=patrick.gallag
her@carahsoft.com,
c=US
Date: 2016.03.09
16:50:29 -05'00'

Signature
Printed Name
Title
Date

Patrick
Gallag
her

STATE OF WISCONSIN

Signature
Printed Name
Title
Date

DAVID CAGIGAL
CIO
3/16/2016

Attachment 1

Government Cloud Terms

Success Plan Description: Government Cloud Premier + Success Plan provides for products the support described in the Premier + Success Plan (http://www.salesforce.com/assets/pdf/misc/salesforce_premierplans.pdf) ("Premier + Plan"), as amended by the following;

Support Personnel: Government Cloud Premier + Success Plan support will be provided by Qualified US Citizens, subject to these terms. "Qualified US Citizens" are individuals who (1) are United States citizens; (2) are physically located within the United States while performing the support; and (3) have completed a background check as a condition of their employment with Salesforce. Research and development personnel and personnel that provide Administration Services under Government Cloud Premier + Success Plan support, that have logical access to Customer Data, and infrastructure support personnel that provide Government Cloud Premier + Success Plan support that have physical access to the Salesforce Government Cloud infrastructure, will be Qualified US Citizens. All other personnel, including, Customer Success Managers, Success Account Managers, Customer Success Technologists and any other personnel engaged in customer success roles and providing customer success services (collectively referred to as "Success Representatives"), will not be Qualified US Citizens and will not have access to Customer Data unless Customer provides such personnel a User ID or otherwise enables the sharing of Customer Data with such personnel.

Telephone Support: Telephone support is available in English only, and twenty-four hours a day, seven days a week.

Submitting a Case: Users may submit a case in the following ways, (1) In the Services by logging in, clicking "Help & Training," clicking "Contact Support," and clicking "Open a Case," then providing the requested information and clicking "Submit" ("On-Line Case Submission"). Cases submitted via this route shall be automatically routed to a team of Qualified US Citizens. (2) By telephone call to Customer Support as described in the Premier + Plan. Calls for support received via telephone shall be initially responded to by individuals who are not Qualified US Citizens and who may be located outside the United States. These individuals will route cases to a team of Qualified US Citizens. These individuals will access the following information about Users in order to route the calls to Qualified US Citizens: first and last name, email address, username, phone number, and physical business address. To submit a case for Severity Level 1 issues, Customer must call Customer Support. (3) Cases submitted via Chat will not be responded to by Qualified US Citizens and will not be subject to the applicable response time described in the Target Initial Response Time table of the Premier + Plan.

The available products on the Salesforce Government Cloud may change at Salesforce's sole discretion and without advance notice. Customer acknowledges that

Government Cloud products may not be fully compatible with non-Government Cloud Products resulting in decreased functionality. Any products on this Quote that do not include the term "Gov Cloud" in the product name are not Government Cloud products and are not hosted on the Salesforce Government Cloud.

Customers on SFDC commercial instance migrating to Government Cloud:

Customer's data is scheduled to begin migration on an agreed upon date on which the Org is scheduled to migrate from its current infrastructure to the Salesforce Government Cloud infrastructure. Customer acknowledges and agrees that the migration from its current infrastructure to the Salesforce Government Cloud infrastructure requires a planned service downtime. During this planned service downtime, the customer's Salesforce.com org will be completely unavailable for use, the duration of the planned service downtime may range from a few hours for small orgs to up to 48 hours or more for larger orgs depending on a number of factors, include the amount of file storage and data storage the customer is using. Additionally, Customer acknowledges and agrees to the following conditions for this Quote and any add on Quotes executed prior to the completion of the migration process: 1) Customer shall receive the Government Cloud Premier+ Success plan, but may not receive all of the plan's features; 2) Customer's data shall reside on standard commercial infrastructure; and 3) the standard commercial infrastructure may include commercial customer data. Upon completion of migration, Customer data for products ordered under this Quote shall reside in the Salesforce Government Cloud infrastructure, unless otherwise specified in this Quote or any add on Quotes.

Exhibit 1

PREMIER SUCCESS PLAN AND PREMIER+ SUCCESS PLAN for Sales Cloud, Service Cloud, Force.com Platform and Salesforce Chatter*

General. If purchased, the Premier Success Plan or Premier+ Success Plan will be provided to Customer's Users in accordance with this description. Users can submit cases over the Web or by telephone. SFDC will use commercially reasonable efforts to promptly respond to each case, and will use commercially reasonable efforts to promptly resolve each case. Actual resolution time will depend on the nature of the case and the resolution. A resolution may consist of a fix, workaround or other solution in SFDC's reasonable determination.

Designated Contacts. "Designated Contacts" are Users Customer identifies as primary liaisons between Customer and SFDC for technical support. Customer shall identify between one (1) and four (4) Designated Contacts. Customer may be charged an additional fee for Designated Contacts in excess of four (4) at any given time. Customer shall notify SFDC whenever Designated Contact responsibilities are transferred to another individual.

Customers' Designated Contacts shall be responsible for:

1. overseeing Customer's support case activity,
2. developing and deploying troubleshooting processes within Customer's organization, and
3. resolving password reset, username and lockout issues for Customer.

Customer shall ensure that Designated Contacts:

- A. have completed, at a minimum, the basic Services administration course currently titled "Administration Essentials," which is included at no additional charge as part of online training,
- B. have completed any supplemental training appropriate for the Designated Contact's specific role or Customer's usage of the Services,
- C. are knowledgeable about the applicable Services in order to help resolve, and to assist SFDC in analyzing and resolving, technical issues, and
- D. have a basic understanding of any problem that is the subject of a case, and the ability to reproduce the problem in order to assist SFDC in diagnosing and triaging it.

Telephone Support. Telephone support in English is available twenty-four hours a day, seven days a week. Telephone support in French, German, Italian and Spanish is available from 8:00 a.m. to 6:00 p.m. GMT, excluding weekends and holidays. Telephone support in Japanese is available twenty-four hours a day, seven days a week for Severity Level 1 and Level 2 issues (as those Severity Levels are described below), and from 9:00 a.m. to 6:00 p.m. JST on weekdays, excluding December 31 –January 3, for Severity Level 3 and 4 issues. Customer may inquire regarding support in other languages. Calls will normally be answered by a triage agent, who will document the case and route it to the appropriate support team for response to Customer.

Main toll-free Customer Support telephone numbers are as follows. A complete list is available on the Help & Training website at <https://help.salesforce.com/apex/HTViewSolution?id=000001000>:

- United States: +1-866-614-7375
- Ireland: +353-1-440-3590
- Australia: 1-800-789-984
- Japan: 0066 33 812474

Submitting a Case. Users may submit a case in any of the following ways:

1. In the Services by logging in, clicking "Help & Training," clicking "Contact Support," and clicking "Open a Case," then providing the requested information and clicking "Submit." Premier and Premier+ cases are priority-routed to the appropriate support teams.
2. By telephone call to Customer Support as described above. *For Severity Level 1 issues, Customer must call Customer Support.*

Users will be asked to provide their company name and contact information, and each case will be assigned a unique case number.

* A full list of included and excluded products is attached hereto as Appendix B.

For assistance with User password resets, Users should use the “Forgot your password?” link on the login page or contact a Designated Contact or Customer system administrator. For assistance with Salesforce usernames and lockouts, Users should contact a Designated Contact or Customer system administrator. For security reasons, SFDC does not provide contact information for Designated Contacts system administrators.

Severity Levels. Issues will be categorized and handled according to an assigned severity level. The case severity level is selected by the User at time of case submission, and will be updated by SFDC as follows:

Severity Level	Description
Level 1 – Critical	Critical production issue affecting all Users, including system unavailability and data integrity issues with no workaround available.
Level 2 – Urgent	Major functionality is impacted or performance is significantly degraded. Issue is persistent and affects many Users and/or major functionality. No reasonable workaround is available. Also includes time-sensitive requests such as requests for feature activation or a data export.
Level 3 – High	System performance issue or bug affecting some but not all Users. Short-term workaround is available, but not scalable.
Level 4 – Medium	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting a small number of users. Reasonable workaround available. Resolution required as soon as reasonably practicable.

Target Initial Response Time. SFDC will use commercially reasonable efforts to respond to each case within the applicable response time described in the table below, depending on the severity level set on the case.

Target Initial Response Time by Case Severity	
Severity Level	Target Initial Response Time
1	1 hour ¹
2	2 hours ¹
3	4 business hours ²
4 and administration cases for Premier+	8 business hours ²

¹ Severity Level 1 and 2 target initial response times are 24x7, including weekends and holidays. Severity Level 1 cases must be submitted via telephone as described above. Severity Level 1 and 2 target initial response times do not apply to cases submitted via email.

² Severity Level 3 and 4 target initial response times include local business hours only and exclude weekends and holidays, and do not apply to cases submitted via e-mail.

Reproducible errors that cannot promptly be resolved will be escalated to higher support tiers for further investigation and analysis.

Cooperation. SFDC must be able to reproduce errors in order to resolve them. Customer agrees to cooperate and work closely with SFDC to reproduce errors, including conducting diagnostic or troubleshooting activities as requested and appropriate. Also, subject to Customer's approval on a case-by-case basis, Users may be asked to provide remote access to their SFDC application and/or desktop system for troubleshooting purposes.

Escalation Matrix. The table below outlines the escalation contacts available to Customer, as necessary.

Level	Title
1 st level	On-Call Support Manager
2 nd Level	VP, Global Technical Support, Customers for Life
3 rd Level	SVP, Customers for Life
4 th Level	EVP, Customers for Life

Recorded Online Training. The Premier Success Plan and Premier+ Success Plan include unlimited access to self-paced, recorded online courses. Courses, content and language availability are limited, and are subject to change without notice in SFDC's sole discretion. Course materials are confidential information of SFDC and may not be copied or modified, or disclosed or distributed to anyone other than Customers' Users entitled to receive Premier Success Plan or Premier+ Success Plan, except as described under "Customizable Training Templates" below. Online content may be accessed only via websites designated by SFDC.

Customizable Training Templates. The Premier Success Plan and Premier+ Success Plan include unlimited access to downloadable, customizable training course templates ("Customizable Training Templates"). Customer may modify Customizable Training Templates to address Customer's requirements for internal training on the Services. Customer shall not modify or use the Customizable Training Templates for training of anyone other than Users.

SFDC may update Customizable Training Templates from time to time, and recommends that Customer regularly check for updates to the Customizable Training Templates that Customer is using.

Customizable Training Templates are confidential information of SFDC and may not be copied, or disclosed or distributed to anyone other than Customers' Users entitled to receive Premier Success Plan or Premier+ Success Plan. Customer shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of all of its modifications to the Customizable Training Templates, shall use commercially reasonable efforts to prevent unauthorized access to or use of the Customizable Training Templates, and shall notify SFDC promptly of any such unauthorized access or use. SFDC retains ownership of all intellectual property rights in the Customizable Training Templates, and reserves all rights in Customizable Training Templates not expressly granted to the Customer. Subject to the above, SFDC acquires no right, title or interest from Customer hereunder in or to any modifications made by Customer to Customizable Training Templates, including any intellectual property rights in such modifications.

The number and availability of Customizable Training Templates, content and language availability are limited, and are subject to change without notice in SFDC's sole discretion. The quantity and scope of Customizable Training Templates may differ for Premier and Premier+ customers. Customizable Training Templates may be downloaded only via websites designated by SFDC.

Success Programs. Premier Success Plan and Premier+ Success Plan customers may participate in Success Programs. Success Programs include unlimited access to Premier Webinars, Premier Chatter Groups and Premier Content. Premier Webinars, Premier Content and language availability are limited, and are subject to change without notice in SFDC's sole discretion. Online content may be accessed only via websites designated by SFDC.

Success Program materials are confidential information of SFDC and may not be copied or modified, or disclosed or distributed to anyone other than Customers' Users entitled to receive Premier Success Plan or Premier+ Success Plan, except as described under "Customizable Training Templates" above. The Success Programs do not include implementation services, response time commitments for question asked in Chatter Groups or any warranty on content posted in Chatter Groups. SFDC retains ownership of all intellectual property rights posted and provided in the Success Programs and reserves all rights in the content not expressly granted to the Customer.

Developer Support. Developer Support is included in the Premier and Premier+ Success Plans. Developer Support consists of SFDC reviewing Customer-written Apex and Visualforce code and offering suggestions to help with issues encountered during development, as further described in the table below. Developer Support does not include creation of code, including SOQL queries, or pre-release regression testing. Developer Support scope is limited to the review of Apex and Visualforce code containing 200 code lines or less. Developer Support is available only in English.

Developer Support Categories/Types	Included in Premier and Premier+ Developer Support
Force.com Code (Apex) and Force.com Pages (Visualforce)	
Functional description of objects, methods and properties	√
Explanation of governor limits	√
Apex query performance and troubleshooting	√
Salesforce error message troubleshooting and analysis	√
Force.com Apex and Visualforce best practices	√
Analysis and debugging of Force.com Apex and Visualforce (up to 200 lines)	√
Visual Workflow	√
Force.com Web Services API	
Clarification of API documentation	√
API performance troubleshooting	√
Salesforce API error message troubleshooting and analysis	√
Salesforce API best practices	√
Salesforce.com-supported Developer Toolkits (AJAX Toolkit, Force.com Migration Toolkit, Force.com IDE, etc.)	
Salesforce error message troubleshooting	√
Toolkit best practices	√

Success Representative. The Premier Success Plan and Premier+ Success Plan include an assigned Success Representative if Customer has in effect subscriptions with an annual value of at least \$1 million USD.

The role of the Success Representative is to help Customer with Salesforce product adoption, including reviewing Salesforce usage metrics, sharing Salesforce best practice advice and guidance related to Customer’s Salesforce deployment, and helping to escalate technical issues as necessary. Customer is responsible for its evaluation and for any implementation of the Success Representative’s recommendations.

Administration Services. If Customer purchases the Premier+ Success Plan option, SFDC will perform the system administration functions listed in [Appendix A](#) for the Services. SFDC administrators will work in tandem with the Customer’s Designated Contacts to execute tasks listed in Schedule A based on Customer’s design specifications. Customer is responsible for gathering business and functional requirements, design specifications, change management approvals, and documentation of configuration, and for designing and/or delivering training materials.

SFDC will provide a complimentary User subscription to Customer for use by the SFDC administration team. Customer’s Designated Contacts will act as Customer’s sole contacts for submitting administration cases on behalf of Customer. Administration cases are assigned Severity level 4, and are worked during local business hours only.

The Premier+ Success Plan does not include implementation of the Services. The Premier+ Success Plan is for ongoing support and administration of the Services after the Services have been implemented. Administration Services are available only in English.

Excluded Items. Neither the Premier Success Plan nor the Premier+ Success Plan includes:

- Assistance with Salesforce password resets. For password resets, Users should click the “Forgot your password?” link on the login page or contact their system administrator;
- Assistance with Salesforce usernames. For assistance with usernames, Users should contact their system administrator;
- Assistance with Salesforce lockouts due to incorrect login attempts. For assistance with Salesforce lockouts due to incorrect login attempts, Users should contact their system administrator to unlock the account, or wait for the lockout period to expire;
- Assistance with non-SFDC products, services or technologies, including implementation, administration or use of third-party enabling technologies such as databases, computer networks or communications systems;
- Assistance with AppExchange applications, whether authored by SFDC or a third party;
- Assistance with installation or configuration of hardware, including computers, hard drives, networks or printers; or
- Creation or testing of custom code, including SOQL queries, except as provided under Developer Support.

Changes to Premier Success Plan and Premier+ Success Plan. SFDC may modify the Premier Success Plan and Premier+ Success Plan from time to time, provided the level of service under either plan will not materially decrease during a subscription term.

APPENDIX A: ADMINISTRATION SERVICES

Administration services exclude the initial implementation of the Salesforce application, data migrations, data management or manipulation (de-duping, merging, cleansing), transferring data from one org or object to another, flows, AppExchange installs/uninstalls/customization, VLOOKUPS and custom code. Administration cases are assigned Severity level 4, and are worked during local business hours only.

Administration Categories/Tasks	Description of Administration Tasks
Set Up and Customization	
Users	Create, update and deactivate users
Portal Users ¹	Create, update and deactivate portal users
Roles	Create and update roles and role hierarchies
Profiles	Create and update profiles
Public Groups	Create and update public groups
Custom Objects	Create and update custom objects
Standard Objects	Update standard objects
Custom Fields	Create and update custom fields
Page Layouts ²	Create and update page layouts
Record Types	Create and update record types
List Views	Create and update list views
Queues	Create and update queues
Assignment Rules	Create and update assignment rules
Auto-response Rules	Create and update auto-response rules
Escalation Rules	Create and update escalation rules
Support/Lead Settings	Update settings
Manage Teams (Account/Sales/Case)	Create and update teams on user record
Pricebook	Create and update pricebook
Workflow Rules/Tasks/Alerts/ Field Updates	Create and update workflow rules, tasks, alerts, and field updates
Approval Processes	Create and update workflow approval processes
Process Builder	Create and update Process Builder processes
Reports	Assist in creation and modification of reports as necessary
Dashboards	Create and update dashboards as necessary
Analytic Snapshots	Create and update analytic snapshots as necessary
Custom Report Types	Create and update custom report types
Validation Rules	Assist in creation and modification of validation rules as necessary
Formula Fields	Assist in creation and modification of formula fields as necessary
Summary Formula Fields	Assist in creation and modification of summary formula fields as necessary
Translations Workbench	Create and update translations
Forecast Hierarchy	Update forecast hierarchies
Communities	Create and update Communities settings
Territory	
Territory Hierarchy	Create and update territory hierarchies
Territory Rules	Create and update territory rules
User Territory Assignments ¹	Create and update user territory assignments
Communication Templates	
HTML Letterhead Templates ³	Create HTML letterhead templates
Email Templates	Create email templates
Quote Templates	Create and update quote templates
Data	
Mass Transfer Records ¹	Mass transfer records, provided by customer in formatted CSV file
Mass Delete Records ¹	Mass delete records, provided by customer in formatted CSV file
Mass Create Records ¹	Mass create records, provided by customer in formatted CSV file
Mass Update Records ¹	Mass update records, provided by customer in formatted CSV file
Duplicate Management ¹	Assist in creation and modification of duplicate management rules
Security	
Sharing Rules	Create and update sharing rules
Field Accessibility	Create and update field accessibility
Password Policies	Manage password policies
Session Settings	Manage session settings
IP Ranges	Add and update IP ranges
Company	
Currencies	Manage currencies
Fiscal Year	Create and update fiscal year
Business hours	Create and update business hours
Productivity and Collaboration	
Create Content	Create and update Content workspaces
Add Users to Workspaces	Add users to workspaces
Chatter Feed Settings (org wide)	Create and update Chatter feed settings
Chatter Groups ¹	Add users to Chatter groups
Search Settings	Create and update search settings
Ideas Settings	Create and update ideas settings
Answers Settings	Create and update answers settings
Mobile	
Mobile Configurations	Create and update mobile configurations

¹Customer provides data in Salesforce-specified CSV format.

²Excludes custom code.

³Includes creation of templates; HTML email content provided by customer.

Appendix B

SALESFORCE.COM STANDARD, PREMIER, AND PREMIER+ SUCCESS PLANS PRODUCT INCLUSIONS and EXCLUSIONS

Standard, Premier, and Premier+ Success Plans are available for a subset of Salesforce subscription products.

Products **included** in Salesforce.com Standard, Premier, and Premier+ Success Plans*:

- Sales Cloud
- Service Cloud
- Force.com
- Salesforce Chatter
- Salesforce Communities
- Salesforce Knowledge – Only
- Salesforce Database.com
- Salesforce Employee Help Desk- Only
- Salesforce Employee Community – Only
- Salesforce Identity – Only
- Salesforce Site.com
- DRO (Data Residency Option)
- Data.com Prospector and Data.com Clean
- Salesforce Marketing Cloud*
- Employee Community
- Knowledge
- Live Agent
- Site.com Contributor
- Site.com Publisher
- Analytics Cloud

*Salesforce Marketing Cloud Premier is sold separately from other Premier Success products. Also available for purchase with Salesforce Marketing Cloud is a Standard+ offering that is only available to Marketing Cloud customers.

Products **excluded** from Salesforce.com Premier, and Premier+ Success Plans*:

- Work.com**
- Console for Sales Cloud
- Mobile
- All Data.com Services not referenced under the inclusions list above

*Any other product not noted as specifically included in the list above is excluded from Premier and Premier+ Success Plans.

**Premier+ for Work.com is available when sold as part of Performance Edition only

Products **excluded** from Salesforce.com Standard, Premier, and Premier+ Success Plans:

- Heroku
- Remedyforce
- Pardot
- IdentityConnect
- Desk.com
- Remedyforce
- Service Cloud Government Connect



Salesforce Government Cloud

Background

Federal, state, and local government agencies and government contractors trust Salesforce's cloud-computing platform to deliver critical business applications. This is largely because of Salesforce's commitment to security and privacy. Salesforce's vision is to be government's trusted Cloud Service Provider (CSP), based on the values of maintaining the confidentiality, integrity, and availability of customer data. Salesforce's methods to fulfill this vision are built upon an executive commitment to ensure and continuously improve the security of Salesforce's services, and include:

- **Defense-in-depth:** whenever possible, multiple controls and technologies are applied to limit the possibility of any single point of failure.
- **Investment:** in personnel, tools, and technologies to manage, analyze, and improve security effectiveness.
- **Transparency:** trust cannot be maintained without open communications regarding service performance, reliability, and security, and to that end Salesforce strives to be the industry leader in transparency. See trust.salesforce.com for further details.

"Nothing is more important to our company than the privacy of our customers' data."

— Parker Harris, Co-founder, Salesforce

Deployment Model

Salesforce's deployment model is a "public" cloud infrastructure, as defined by NIST 800-145. In the Salesforce Cloud, an agency dynamically provisions computing resources over the Internet on our multi-tenant infrastructure. This is a cost effective deployment model for agencies as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability, resiliency, security, and manageability.

As a Software as a Service (SaaS) and Platform as a Service (PaaS) leader, data security is of utmost importance for Salesforce. Salesforce serves over 100,000 customers and processes over three billion transactions a day. The organizations that use Salesforce include customers in heavily regulated industries such as financial services, healthcare, insurance, and public sector that require strict adherence with security and privacy requirements. Salesforce raises the bar of security to meet the requirements of our customers, specifically customers in heavily regulated industries such as Public Sector, by maintaining numerous security and privacy certifications.



Salesforce Government Cloud

As part of our commitment to our Government Customers, Salesforce has made the investment to create a government specific cloud to address the FedRAMP requirements for cloud computing. In May 2014, Salesforce became the first CSP to attain a **FedRAMP Authority to Operate** for both Software as a Service (SaaS) and Platform as a Service (PaaS), consistent with the FedRAMP moderate baseline controls. The Authority to Operate was granted by the US Department of Health and Human Services for the Salesforce Government Cloud (described in more detailed below).



The Salesforce Government Cloud is a partitioned instance of Salesforce's multi-tenant public cloud infrastructure, specifically for use by U.S federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs). The isolated production infrastructure supporting the Salesforce Government Cloud Customer Data ensures that the physical hardware is separate from hardware supporting other customers. While isolated, the underlying infrastructure supporting the Salesforce Government Cloud is the same trusted architecture model that supports Salesforce's multi-tenant public cloud offering and over a billion customer transactions a day.

Access to systems and permissions, which could permit access to Customer Data inside of the Salesforce Government Cloud, is restricted to Qualified U.S. Citizens. Qualified U.S. Citizens are individuals who are United States citizens, and are physically located within the United States when accessing the Salesforce Government Cloud systems; and have completed a background check as a condition of their employment with Salesforce¹.

¹ This excludes telephone calls for support that may initially be responded to by individuals who may not be Qualified U.S. Citizens and who may be located outside the United States. These individuals will then route cases to a team of Qualified U.S. Citizens.



Government Cloud compared to Public Cloud

 government cloud	 public cloud
Identical core hardware	
Identical core code base	
Multitenant infrastructure shared w/ government ² customers	Multitenant infrastructure shared w/ public customers
FIPS 140-2 validated 128-bit or 256-bit AES encryption in transit (TLSv1, 1.1, 1.2)	128-bit or 256-bit (RC4) encryption in transit (TLSv1.0, 1.1, 1.2)
FIPS 140-2 validated 128-bit AES Encrypted Custom Fields	128-bit AES Encrypted Custom Fields
Support provided by U.S. based, U.S. Citizens	Worldwide follow the sun support
ISO 27001, SOC 2, PCI, HIPAA, and FedRAMP	ISO 27001, SOC 2, PCI, HIPAA
Premiere+ Support included	Premiere+ Support not included

FedRAMP Authority to Operate (ATO)

The Salesforce Government Cloud information system and authorization boundary, is comprised of the Force.com Platform, Salesforce Services (Sales Cloud, Service Cloud, Chatter), and the backend infrastructure (servers, network devices, databases, storage arrays) that support the operations of these products, referred to as the General Support System (GSS).

In order to maintain compliance with FedRAMP³, Salesforce conducts continuous monitoring on the Government Cloud. Continuous monitoring includes ongoing technical vulnerability detection and remediation, remediation of open Compliance related findings, and at least annual independent assessment of a selection of security controls by a third party assessment organization (3PAO).



² U.S federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs)

³ Salesforce's ongoing commitment to compliance with FedRAMP will be focused solely on the Government Cloud environment. Any potential future modifications required to comply with ongoing enhancements to FedRAMP will be addressed in the Government Cloud. All FedRAMP and other Federal Government security related procedures and documentation will be focused on the Government Cloud.



Federal government Agencies can request access to the Salesforce FedRAMP Agency ATO package by submitting a request to the FedRAMP PMO. All other customers can submit a request to Salesforce via the customer's account representative. Each customer will need to review the documentation and assess that organization's compliance requirements. Customers may need to purchase additional Salesforce and/or third party products and services in order to meet their individual requirements.

Products Available



The Enterprise Edition and Unlimited Edition of some Salesforce products are available for use on the Salesforce Government Cloud. For a list of available products on the Salesforce Government Cloud⁴, see: <http://sfdc.co/GovernmentCloudProductsList>.

⁴ From time to time, the list of available products on the Salesforce Government Cloud may change at Salesforce's sole discretion and without any advance notice. Prior to a Government Customer placing an order on the Salesforce Government Cloud, please contact your local Salesforce sales or renewal representative for the most current product availability information on the Salesforce Government Cloud.

Exhibit 2

STATE OF WISCONSIN SECURITY RIDER

The following terms and conditions are specific to cloud computing including but not limited to SaaS, IaaS and PaaS (all XaaS services). These terms shall supplement the SFDC Service Terms. In the event of a conflict between the terms of this Exhibit 2, State of Wisconsin Security Rider and the SFDC Service Terms, Exhibit 2, this State of Wisconsin Security Rider shall control.

1. Definitions:

1.1 **“Authorized Persons”** means the Contractor’s employees, contractors, subcontractors or other agents who need to access the State’s personal data to enable the Contractor to perform the services required.

1.2 **“Contracting Agency”** means the Agency entering into this Contract on behalf of the State.

1.3 **“Contractor”** means the Contractor and its employees, Subcontractors, agents and affiliates who are providing the services agreed to under the contract.

1.4 **“Data Breach”** means the unauthorized access that result in the use, disclosure or theft of the State’s unencrypted personal data.

1.5 **“Deliverables”** means all project materials, including Goods, software licenses, data, and documentation created during the rendering of Services hereunder. Deliverables shall be the property of the State of Wisconsin unless otherwise specified in the Contract.

1.6 **“Disabling Code”** means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the software and/or State’s processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

1.7 **“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.

1.8 **“Inspection”** means an examination of Deliverables or Services provided under this Contract in order to determine their fitness for use.

1.9 **“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 State because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

1.10 **“Personal Data”** means an individual’s last name and the individual’s first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable: (a) the individual’s Social Security number; (b) the individual’s driver’s license number or state identification number; (c) the individual’s date of birth; (d) the number of the individual’s financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual’s financial account; (e) the individual’s DNA profile; or (f) the individual’s unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation, and any other information protected by state or federal law.

1.11 **“Proprietary Information”** means information, including a formula, pattern, compilation, program, device, method, technique or process to which all of the following apply:

- a. The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.
- b. The information is the subject of efforts to maintain its secrecy that are reasonable under the circumstances.

1.12 **“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.

1.13 **“Public Information”** means information that (i) is collected, assembled or maintained under a law or ordinance or in connection with the transaction of official business by a governmental body or for a governmental body; and (ii) the governmental body owns or to which it has a right of access.

1.14 **“State”** means the government of the State of Wisconsin, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the State of Wisconsin.

1.15 **“State Contact”** means the person or persons designated in writing by the State to receive security incident or breach notification.

1.16 **“Security Incident”** means the possible or actual unauthorized to personal data or non-public data the Contractor believes could reasonably result in the use, disclosure or theft of the State’s unencrypted personal data or non-public data within the possession or control of the Contractor. A security incident may or may not turn into a data breach.

1.17 **“Service Level Agreement”** or (“SLA”) means the SFDC Service Terms as agreed to between the State and SFDC that is subject to the terms and conditions in this document that unless otherwise agreed to includes but is not limited to (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed, and (6) any remedies for performance failures.

1.18 **“Statement of Work”** means a mutually executed document describing services to be performed by Contractor and delivered to the State and if any, the relevant terms and conditions associated therein.

1.19 **“Subcontractor”** means an entity that enters into an agreement with the Contractor for the purpose of delivering Deliverables or rendering Services to the State.

1.20 **“Work Center”** means a charitable organization or nonprofit institution which is licensed under s. 104.07 and incorporated in this State or a unit of county government which is operated for the purpose of carrying out a program of rehabilitation for severely handicapped individuals and for providing the individuals with remunerative employment or other occupational rehabilitating activity of an educational or therapeutic nature, and which is engaged in the production of materials, supplies or equipment or the performance of contractual services in connection with which not less than 75% of the total hours of direct labor are performed by severely handicapped individuals.

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

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of this Contract shall become and remain the property of the State.

c. The Contractor shall not use any information collected in connection with the Services issued from this Contract for any purpose other than fulfilling the Services.

d. Government Cloud Encryption Capabilities:

As part of the Salesforce Government Cloud, Salesforce is capable of responding to FIPS 140-2 cryptographic implementations for data being transferred between the State's web browser and Salesforce. Data that resides within Salesforce's protected boundary does not use FIPS 140-2 validated encryption as compensating/mitigating controls are in place to protect data. Additional information is provided below.

Data In Motion

Salesforce employs cryptographic mechanisms to protect information during transmission. All transmissions between the user and Salesforce are encrypted by default with a 2048-bit Public Key. Our service uses International/Global Step Up certificates. We support one-way TLS, in which customers create secure connections before sharing private data.

Secure routing and traffic flow policies ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary.

Data At Rest

NIST SP 800-53 Rev. 4 states in SC-28, "Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system." SC-28 also states, "Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate." All secondary storage media (hard drives, disk drives, and tapes) containing customer data are maintained within Salesforce's secure production data centers until the media has been sanitized and destroyed. Salesforce relies on physical access controls as a compensating control to protect the data.

For primary data storage, Salesforce provides customers with a built-in capability to apply field-level encryption, using 128-bit keys with AES encryption, for a selection of custom fields included in the Force.com Platform and Salesforce Services. Field-level encryption ensures the data associated with designated fields is encrypted in storage. Additional information regarding field-level security can be accessed via the following link:

https://help.salesforce.com/apex/HTViewHelpDoc?id=fields_about_encrypted_fields.htm&language=en.

3. Data Location: The Contractor shall provide its services to the State and its end users solely from data centers in the U.S. Storage of State Data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store State Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access State Data remotely only as required to

provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited or provided in this Contract.

4. Security Incident or Data Breach Notification: Salesforce will promptly notify the State (within 48 hours) in the event Salesforce becomes aware of an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce support, email to the State's administrator and Security Contact (if contact is submitted by State and contact information is kept up to date), and public posting on trust.salesforce.com.

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate State identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate State identified contact within 48 hours or sooner by telephone and email so long as the State has provided a contact, if it has confirmed that there has been a data breach.

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

7. Termination and Suspension of Service:

7.1. In the event of a termination of the Contract, the Contractor shall implement an orderly return of the State's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the State to extract its data and perform the subsequent secure disposal of the State's data per NIST 800-88 Revision 1.

7.2. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the State's data.

7.3. In the event of termination of any services or Contract in entirety, the Contractor shall not take any action to intentionally erase the State's data for a period of:

- 30 days after the effective date of termination, if the termination is in accordance with the contract period or if the termination is for convenience
- 30 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any State Data and shall thereafter, unless legally prohibited, delete all State Data in its systems or otherwise in its possession or under its control per NIST 800-88 Revision 1.

7.4. The State 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 an SLA.

7.5. Upon termination of the Services or the Contract in its entirety, unless legally prohibited, Contractor shall securely dispose of all State Data in all of its forms, in its systems or otherwise in its possession or under its control including but not limited to disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the State. 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 State upon completion.

8. Background Checks:

Contractor will engage in the services of a background screening vendor to conduct background checks including address verification for the last 7 years, a criminal background check at the state, federal and national searches to identify felony and misdemeanor convictions within the last 7 years, global sanctions check, education verification, and employment history. A hiring decision is then made based on the information collected.

The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

9. Access to Security Logs and Reports: The State can directly access reports containing information on latency statistics, user access, user access IP address, user access history and security logs for all State files related to this contract from within the Service.

10. Contract Audit: The Contractor shall allow the State to audit conformance to the Contract terms. The State may perform this audit or contract with a third party at its discretion and at the State's expense.

The State or its authorized representatives will have access to material related to this contract during normal business hours and upon a two week notice, to perform an operational audit of the Contractor's performance of the contract, and related books and records pertaining to any sums to be paid hereunder or facts relative to any claim against the Contractor which may be chargeable to The State or its property. The Contractor shall provide the State and its authorized representatives with such information and assistance as needed to perform the audits.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an un-redacted version of the audit report upon request to a State. The Contractor may remove its proprietary information from the un-redacted version. Salesforce's information security control environment applicable to the Salesforce Services undergoes an independent evaluation in the form of SOC 1 (SSAE 16), SOC 2, or SOC 3 reports. The most recent SSAE16 SOC 1 Report, SOC 2 Report and SSAE16 SOC 1 Bridge (Gap) Letter are available upon request.

12. System Maintenance and Upgrade Notice: The Contractor shall give a minimum forty eight (48) hour advance notice, or as included in the SLA to the State 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. It usually includes a new version number.

Contractor shall make updates and upgrades available to State at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect State's use of or access to the Service, or increase the cost of the Service to the State.

All upgrades, patches, and other system maintenance are provided at no additional cost to the State. In addition, Salesforce releases 3 complimentary upgrades each year, in Winter, Spring, and Summer versions. All Salesforce users are always on the latest version of our platform because everyone gets instant upgrades (typically on an opt-in basis). Each release will be delivered automatically in a transparent manner, and will not break your configurations.

13. Security:

The Salesforce multi-tenant, cloud platform architecture enables us to leverage a common infrastructure and software code base across all of our customers who benefit from access to the most current release of the application, periodic upgrades, more rapid innovation, and the economies of a shared infrastructure.

Salesforce understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.

Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce Force.com platform gives you the peace of mind only a world-class security infrastructure can provide.

Third-party validation

Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we

continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum. Additional audits and certifications include: CSA 'Consensus Assessments Initiative', JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.

Protection at the application level

Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define company-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts.

Protection at the facilities level

Salesforce security standards are stringent and designed with demanding customers in mind, including the world's most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk and to tape, with tape providing a second level of physical protection. Neither disks nor tapes ever leave the data center.

Protection at the network level

Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of State Data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The State shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor. This includes the ability for the State to import data from other Contractors. The State has the ability to export data from the service at any time during the course of the subscription via a .csv file. Contractor shall specify if State is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The

technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar Contract with the Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request.

19. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973. For the most up to date information on Product Accessibility and 508 VPATS please see: http://www.salesforce.com/company/legal/508_accessibility.jsp

20. Subscription Terms: Contractor grants to the State a license to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (as applicable), and use Contractors' documentation.

No terms, including standard click through license or website terms or use or privacy policy, shall apply to the State unless such terms are included in the Contract or otherwise agreed to in writing by both parties.