



**CONTRACT
BETWEEN THE STATE OF TENNESSEE,
DEPARTMENT OF GENERAL SERVICES, CENTRAL PROCUREMENT OFFICE
AND
ZENDESK, INC.**

This Contract, by and between the State of Tennessee, Department of General Services, Central Procurement Office ("State") and Zendesk, Inc. ("Contractor" or "Zendesk"), is for the provision of Zendesk Software-as-a-Service Customer Service Platform, as further defined in the "SCOPE." State and Contractor may be referred to individually as a "Party" or collectively as the "Parties" to this Contract.

The Contractor is a Corporation
Contractor Place of Incorporation: Delaware
Contractor Edison Registration ID # 0000152766

A. SCOPE:

- A.1. The Contractor shall provide a software-as-a-service cloud based customer support solution as described at www.zendesk.com ("Service") as specified by this Contract.
- A.2. Definitions.
- A.2.1. **Account:** means all Zendesk accounts or instances created by or on behalf of State or its Agents within the Service.
- A.2.2. **Agent:** means an individual authorized to use the Service through State's Account as an agent and/or administrator as identified through a unique login.
- A.2.3. **Application programming interface (API):** specifies how some software components should interact with each other. In practice, many times an API comes in the form of a library that includes specifications for routines, Data structures, object classes, and variables.
- A.2.4. **Cloud Software as a Service (SaaS):** Services related to the delivery of Software-based applications made available by the provider running on a cloud infrastructure through the internet. The State does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- A.2.5. **Reserved.**
- A.2.6. **Data:** means any information, formulae, algorithms, or other content that the State, the State's employees, Agents and End Users upload, create or modify using the Service pursuant to this Contract. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.
- A.2.7. **Data Breach:** means any access, destruction, loss, theft, use, modification or disclosure of Data by an unauthorized party or that is in violation of Contract terms and/or applicable state or federal law.
- A.2.8. **Reserved.**
- A.2.9. **Documentation:** means any written or electronic documentation, images, video, text or sounds specifying the functionalities of the Service provided or made available by Zendesk to State, Agents or End-Users through the Service website or otherwise.
- A.2.10. **End-User:** means any person or entity other than State or Agents with whom State or its Agents



interact using the Service.

- A.2.11. **Electronic discovery:** refers to discovery in civil litigation or government investigations which deals with the exchange of information in electronic format. These Data are subject to local rules and agreed-upon processes, and are often reviewed for privilege and relevance before being turned over to opposing counsel.
- A.2.12. **FISMA:** The Federal Information Security Management Act is a Federal law that aims to strengthen Federal Government information security, including through the requirement for the development of mandatory information security risk management standards.
- A.2.13. **HIPAA:** The Health Insurance Portability and Accountability Act of 1996 is a Federal law that aims to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information.
- A.2.14. **ISO 10002:2004 (ISO, ITIL, and COBIT):** International quality management standard that promotes customer satisfaction. To meet this standard, a system must identify complaints and causes, create solution processes, and analyze customer satisfaction.
- A.2.15. **ISO 27001:** International specification that provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system (ISMS).
- A.2.16. **NIST:** National Institute of Standards and Technology is an organization that develops and issues standards, guidelines, and other publications to assist agencies in implementing FISMA
- A.2.17. **Other Services:** means third party products, applications, services, software, networks, systems, directories, websites, databases and information which the Service links to, or which the State may connect to or enable in conjunction with the Service, including, without limitation, Other Services which may be integrated directly into the Service. Zendesk Voice and Zopim Live Chat shall be provided under this Contract and not included as "Other Services."
- A.2.18. **Personal Data:** means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
- A.2.19. **Processing/To Process:** means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- A.2.20. **Service Plan:** means the Enterprise and Enterprise Elite level service plans being offered to the State and the functionality and services associated therewith (as detailed at www.zendesk.com) for which the State subscribes with respect to each Agent.
- A.2.21. **Subscription Term:** means the period during which the State has agreed to subscribe to the Service with respect to any individual Agent.
- A.2.22. **Zendesk Group:** means Zendesk, Inc., a Delaware Corporation together with all its Affiliates.
- A.3. **Warranties.** Contractor represents and warrants that throughout the Term of this Contract ("Warranty Period"), the Service will conform in all material respects to the Documentation.



Contractor grants a license to the State to use all software provided under this Contract in the course of the State's business and purposes.

- A.4. Periodic Meetings. The State reserves the right, at the State's option, to request periodic meetings with Contractor management staff to discuss topics including, but not limited to, the following: general contract direction, management, and coordination; State of Tennessee technical infrastructure and standards; time keeping and other project progress records. At the State's sole discretion, these meetings shall occur at a State location or via conference call and shall be at no additional cost to the State or the State agencies, except when such meetings are held at a State location or another location other than the location of Contractor, in which case State shall pay all reasonable expenses associated with Contractors' personnel's travel to such location, in accordance with Section C.4.
- A.5. EXCEPT AS STATED OTHERWISE IN THIS AGREEMENT THE SERVICE, ALL SERVER AND NETWORK COMPONENTS ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS, WITHOUT ANY WARRANTIES OF ANY KIND TO THE FULLEST EXTENT PERMITTED BY LAW.
- A.6. Correction of Deficiencies. Any corrections of deficiencies relating to the Contract Scope of Services requirements or deliverables and any investigation necessary to determine the source of such deficiencies shall be completed by the Contractor at no cost to the State.
- A.7. Additional Work – Professional Services. The State may request, at its sole discretion, additional work (professional services) involving the enhancement or modification of a deliverable under the Contract Scope, provided that this Contract is amended, pursuant to Section D.3. Remuneration for any such additional work shall be based on the applicable "contingent," payment rate(s) detailed in Section C.3 of this Contract.

The Contractor shall build all new extensions or packages for Zendesk in accordance with federal and state laws and standards, where they exist.

- (1) The State will request Modifications and Enhancements in writing to define the purpose and scope of the Modification or Enhancement. A Modification and Enhancement Request, or "MER," will include:
 - Requestor name and role
 - Brief description
 - Reason or justification
 - Requirements and specifications
 - Request for a cost estimate, approximate time (hours) and resources necessary to complete the modification or enhancement
 - Requested or mandated delivery date
- (2) The Contractor shall prepare an Estimate for the MER. Said Estimate shall include:
 - Total Fixed Cost to deliver the Modification or Enhancement - the cost shall be based on the Contractor's estimate of the total number of hours required to deliver the Modification or Enhancement and the payment rates specified in Contract Section C.3. The Total Fixed Cost shall represent the maximum amount that the State will compensate the Contractor for the Modification or Enhancement.
 - The estimated delivery date of the Modification or Enhancement.
 - The impact of delivering the Modification or Enhancement on operations and activities.
- (3) The State, at its sole discretion, may accept or reject the Contractor's estimate.



- (i) If the State agrees to the Contractor's estimate, the State shall provide acceptance in writing, which authorizes the Contractor to begin work according to the MER.
- (ii) If the State does not agree to the Contractor's estimate, the State may:
 - Elect not to proceed with the Modification or Enhancement;
 - Negotiate the estimate with the Contractor;
 - Revise the MER to provide additional information to clarify the scope of the request.

The Contractor shall not begin work on any MER without the State's written acceptance of the Contractor's estimate.

The State, at its sole discretion, will determine the prioritization of the MER work.

- (4) The Contractor shall modify the State Zendesk solution according to the MER, and shall thoroughly test the modifications.
 - (i) The Contractor shall prepare and provide to the State documented instructions for deploying the Modification or Enhancement to the State's production environment.
 - (ii) The Contractor shall prepare and provide to the State new or updated system and user documentation related to the Modification or Enhancement.
 - (iii) The Contractor shall work with the designated State project team member to coordinate with Zendesk and other support vendors on any changes that affect those systems.
- (5) The State will test the delivered Modification or Enhancement to ensure that:
 - The Modification or Enhancement completely provides the functions as required by the MER.
 - The Modification or Enhancement has no deficiencies in documentation, or defects in efficiency or performance.

The State, at its sole discretion, will determine acceptance of the Modification or Enhancement, and will indicate its acceptance or non-acceptance to the Contractor in writing within thirty (30) days of installation to the State's environment.

A.8. Contingent Rates. In accordance with section C.3 of this Contract, The State may request and the Contractor may agree to perform additional work (professional services) involving the Enhancement or Modification of deliverables under the Contract Scope of Services, provided that this Contract is amended to require such work.

- i. Remuneration for any such additional work shall be based on the applicable contingent, payment rate(s) detailed below and as approved by the State.

<u>SERVICE</u>	<u>AMOUNT PER HOUR</u>
Developer	\$185
Trainer	\$185



Engagement Manager	\$185
--------------------	-------

- ii. The Contractor shall be compensated for travel, meals, or lodging in accordance with "State Comprehensive Travel Regulations," as outlined in Section C.4.

A.9. Contract Management and Reporting. The Contractor shall designate a Contract Manager to be a single point of contact for all activities and issues related to work under this Statewide Contract. The Contract Manager shall coordinate as necessary with the State to ensure that Contractor activities are managed consistently with overall Contract requirements.

- (i) Risk Management Plan – If available, Contractor shall provide a Risk Management Plan outlining potential risks, mitigation strategies, and risk management processes.
- (ii) Issue Management Plan – If available, Contractor shall provide an Issue Management Plan for documenting, tracking, and reporting issues, including the process for elevating issues for joint management decision by the Contractor and the State.
- (iii) Backup and Recovery Plan – The Contractor shall create a Backup and Recovery Plan that supports multiple environments, failover environments and Disaster Recovery. In order to prevent loss of data, the Contractor shall develop and implement recovery procedures, including the process for restoring data to its original or prior form.
- (iv) Contingency of Operations Plan. The Contractor shall develop and submit a Contingency of Operations Plan to specify planning for the remediation of specific software and/or operations in the event of critical impact resulting from natural, accidental or intentional events. The Contingency Operations Plan shall document the Contractor's plans and procedures to maintain State support and shall include, but not be limited to the following:
 - Description of the Contractor's emergency management procedures and policy
 - How the Contractor will communicate with the State during emergencies
 - List of primary and alternate Contractor points of contact, each with primary and alternate telephone numbers and e-mail addresses
 - Procedures for safeguarding sensitive and/or classified State information (if applicable)
- (v) Training. The Contractor shall prepare and deliver to the State the following training components:
 - (a) Training Material. The Contractor shall develop and deliver to the State Train-the-Trainer material for the Zendesk Service. Training material shall be prepared using State-standard Microsoft Office products.
 - (b) Train-the-Trainer Training. The Contractor shall train State-designated Zendesk Trainers using the Training Material developed in Section A.9.v.(a).
 - (c) Help Content. The Contractor shall develop and deliver content for the help functions of Zendesk.

A.10. Reporting. The Contractor will be required to submit reports validating Contract purchases under this Contract, at the State's request, which will not be made more often than once in three (3) months. Reports will detail at a minimum the following information:

1. Contract Number
2. Contract Line Item Number
3. Commodity Description



- 4. Line Item Quantity Purchased
- 5. Line Item Dollar Amount (Volume) Purchased

Additional reports (such as Service Level Reports that provide the time, severity level, description, acknowledgement time, and resolution time for each incident logged during the reporting period) may be requested in writing by the Contract Administrator with a thirty (30) day written notice to the vendor. Reports must be submitted electronically in Microsoft Excel format.

- A.11. **Support and Maintenance.** Contractor shall address the Service and its functionality issues through software upgrades, modifications, bug fixes, or other improvements in its software that it shall make generally available to its customers, including the State. Contractor shall provide direct, third-tier technical support for and shall maintain the operational readiness, interoperability, and conformance to specifications and requirements of Zendesk. These support and maintenance services for all Software required to deliver Zendesk Services are included within the Zendesk Services and at no additional cost to the State. The Contractor shall, at a minimum:
- (1) Make appropriate Contractor support resources available to the State twenty-four (24) hours a day, seven (7) days a week, and 365 calendar days a year except State holidays, to provide the services described and detailed in this section.
 - (2) Diagnose and resolve problems reported by the State that have not been diagnosed and resolved at lower levels of support within the State as practically possible. Zendesk will determine the severity level of each reported problem.
 - (3) Maintain the operational readiness of the Zendesk Service within the current State systems environment by identifying and communicating problems or issues to the State, making necessary adjustments and repairs.
- A.12. **Requirements Verification.** The Contractor shall review and verify the state's requirements, included in the Requirements Verification Matrix in Contract Attachment 1, against the Contractor's Service. The Contractor shall review and complete the Requirements Verification, identifying any additional customizations or integrations required to meet compliance with specifications.
- A.13. **Summary of Deliverables.**

Section #	Deliverable	Contract Section(s) Reference	Delivery Date
A.13.1	Requirements Verification Matrix	A.12., Contract Attachment 1	Prior to Contract Award
A.13.2	Risk Management Plan	A.9.i.	Prior to Contract Award
A.13.3	Issue Management Plan	A.9.ii.	Prior to Contract Award
A.13.4	Backup and Recovery Plan	A.9.iii.	Prior to Contract Award
A.13.5	Contingency of Operations Plan	A.9.iv.	Prior to Contract Award
A.13.6	Training materials & trained trainers	A.9.v.	No later than September 1, 2015
A.13.7	Requested Quarterly Reports	A.11.	Upon Request of the State (no more than once every 3 months).

**Contract Period Begin Date and Contract Period End Date are included in Contract Section B.*

- A.14. **Data Transfer Security.** All data transfers must be encrypted using 128bit (or higher) SSL for HTTP traffic and SSH version 2 for any batch or real-time non-http transfers. Furthermore, SSL certificates must be signed by a trusted third party. No self-signed certificates will be considered.



- A.15. **Suspension.** In addition to Zendesk's rights as set forth in this Contract, Zendesk reserves the right, in Zendesk's reasonable discretion, to temporarily suspend the State's access to and use of the Service: (i) during planned downtime for upgrades and maintenance to the Service (of which Zendesk will use commercially reasonable efforts to notify the State in advance both through the Zendesk forum page and a notice to the State's Account owner and Agents) ("**Planned Downtime**"); (ii) during any unavailability caused by Force Majeure Events; or (iii) if Zendesk suspects or detects any malicious software connected to the State's Account or use of the Service by the State, Agents or End Users. Zendesk will use commercially reasonable efforts to schedule Planned Downtime for weekends (Pacific time zone) and other off-peak hours.
- A.16. **Permitted Use.** The State agrees not to (a) 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 authorized Agents and End Users in furtherance of the State's internal business purposes as expressly permitted by this Contract; (b) use the Service to Process data on behalf of any third party other than Agents or End Users; (c) modify, adapt, or hack the Service or otherwise attempt to gain unauthorized access to the Service or related systems or networks; (d) falsely imply any sponsorship or association with Zendesk, (e) use the Service in any unlawful manner, including but not limited to violation of any person's privacy rights; (f) use the Service to send unsolicited or unauthorized junk mail, spam, pyramid schemes or other forms of duplicative or unsolicited messages; (g) use the Service to store or transmit files, materials, data, text, audio, video, images or other content that infringes on any person's intellectual property rights; (h) use the Service in any manner that interferes with or disrupts the integrity or performance of the Service and its components; (i) attempt to decipher, decompile, reverse engineer or otherwise discover the source code of any software making up the Service; (j) use the Service to knowingly post, transmit, upload, link to, send or store any content that is unlawful, racist, hateful, abusive, libelous, obscene, or discriminatory; (k) use the Service to knowingly post transmit, upload, link to, send or store any viruses, malware, Trojan horses, time bombs, or any other similar harmful software ("**Malicious Software**"); or (l) try to use, or use the Service in violation of this Agreement.

The State is responsible for compliance with the provisions of this Contract by Agents and for any and all activities that occur under the State's Account, as well as for all the Data. Without limiting the foregoing, the State is solely responsible for ensuring that, for all matters under its control, the use of the Service to store and transmit the Data is compliant with all applicable laws and regulations. The State also maintains all responsibility for determining whether the Service or the information generated thereby is accurate or sufficient for the State's purposes. The State agrees and acknowledges that each Agent will be identified by a unique username and password ("**Login**") and that an Agent Login may only be used by one (1) individual. The State will not share an Agent Login among multiple individuals. The State and its Agents are responsible for maintaining the confidentiality of all Login information for the State's Account.

- A.17. **Third Party Services.** The State shall not order Third Party Services. In the event State does enable, access or use Other Services, the State's access and use of such Other Services is governed solely by the terms and conditions of such Other Services. The State may be required to register for or log into such Other Services on their respective websites. By enabling any Other Services, the State is expressly permitting Zendesk to disclose the State's Login as well as the Data as necessary to facilitate the use or enablement of such Other Services.
- A.18. **Voice Functionality.** If the State's Service Plan and subscription to the Service allows it to use the Zendesk Voice™ service, the State understands and agrees that (a) the Service is not intended to support or carry emergency calls to any emergency services such as public safety answering points, (b) Zendesk will not be held liable for any claim, damages or loss (and the State hereby waive any and all such claims or causes of action), arising from or relating to the State's (or Agents or End Users) inability to use the Service to make such emergency calls, and (c) the State is solely responsible for its operation of Zendesk Voice in compliance with all applicable laws in all jurisdictions governing use of the Service by the State, Agents and End Users, including but



not limited to telephone recording and wiretapping laws. When enabling Zendesk Voice, the State is consenting, on behalf of the State and its Agents and End-Users to the Processing of the Data (as generated by or necessary for the provision or operation of Zendesk Voice) by the third party service provider Zendesk utilizes to provide Zendesk Voice.

B. TERM OF CONTRACT:

- B.1. This Contract shall be effective on July 31, 2015 ("Effective Date") and extend for a period of twelve (12) months after the Effective Date ("Term"). The State shall have no payment obligation for goods or services provided by the Contractor prior to the Effective Date.
- B.2. Renewal Options. This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to three (3) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.
- B.3. Term Extension. The State may extend the Term an additional period of time, not to exceed one hundred-eighty (180) days beyond the expiration date of this Contract, under the same terms and conditions, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.

C. PAYMENT TERMS AND CONDITIONS:

- C.1. Estimated Liability. The total purchases of any goods or services under the Contract are not known. The State estimates the purchases during the Term shall be Six Million, Four Hundred Thousand Dollars (\$6,400,000.00) ("Estimated Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.
- C.2. Compensation Firm. The payment methodology in Section C.3. and the Travel Compensation provided in Section C.4. of this Contract shall constitute the entire compensation due the Contractor for all goods or services provided under this Contract regardless of the difficulty, materials or equipment required. The payment methodology includes all applicable taxes, fees, overhead, and all other direct and indirect costs incurred or to be incurred by the Contractor.
- C.3. Payment Methodology. The Contractor shall be compensated based on the payment rates for goods or services contained in Contract Attachment 2, Pricing Schedule and as authorized by the State in a total amount as set forth in Section C.1. The Contractor's compensation shall be contingent upon the satisfactory provision of goods or services as set forth in Section A.
- C.4. Travel Compensation. Compensation to the Contractor for travel, meals, or lodging shall be subject to amounts and limitations specified in the current "State Comprehensive Travel Regulations."

The Contractor must include (in addition to other invoice requirements of this Contract) a complete itemization of requested travel compensation and appropriate documentation and receipts as required by the "State Comprehensive Travel Regulations."

- C.5. Invoice Requirements. The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in Section C.3., above. Contractor shall submit invoices and necessary supporting documentation, no later than thirty (30) days after goods or services have been provided to the following address:



State Agency Billing Address

a. Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):

- (1) Invoice number (assigned by the Contractor);
- (2) Invoice date;
- (3) Contract number (assigned by the State);
- (4) Customer account name: State Agency & Division Name;
- (5) Customer account number (assigned by the Contractor to the above-referenced Customer);
- (6) Contractor name;
- (7) Contractor Tennessee Edison registration ID number;
- (8) Contractor contact for invoice questions (name, phone, or email);
- (9) Contractor remittance address;
- (10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;
- (11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;
- (12) Applicable payment methodology (as stipulated in Section C.3.) of each good or service invoiced;
- (13) Amount due for each compensable unit of good or service; and
- (14) Total amount due for the invoice period.

b. Contractor's invoices shall:

- (1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;
- (2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;
- (3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes, provided that the State provides Contractor with the respective tax exemption certificate in advance; and
- (4) Include shipping or delivery charges only as authorized in this Contract.

c. The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.5.

C.6. **Payment of Invoice.** A payment by the State shall not prejudice the State's right to object to or question any payment, invoice, or other matter. A payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced.

C.7. **Invoice Reductions.** The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, to not constitute proper compensation for goods delivered or services provided.

In the event Contractor's Service is, for any reason other than for causes under the control of the State or its agents or arising from services provided by other contractors or suppliers of goods or services to the State or due to a Force Majeure event, unavailable or unusable by the State for a period of time greater than twenty-four (24) continuous hours, the State may reduce Contractor's invoice by an amount representing a pro rata refund for the time the service was unavailable or



unusable. In the event there are no future invoices under this Contract, Contractor shall provide such a pro rata refund to the State. Service outages due to Force Majeure events shall be governed by Section D.24.

- C.8. **Deductions.** The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any Contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor. Notwithstanding the above, no deduction by the State shall prejudice the right of Contractor to file a claim as allowed by the rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 407
- C.9. **Prerequisite Documentation.** The Contractor shall not invoice the State under this Contract until the State has received the following, properly completed documentation.
- The Contractor shall complete, sign, and present to the State an "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, all payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, shall be made by automated clearing house.
 - The Contractor shall complete, sign, and present to the State a "Substitute W-9 Form" provided by the State. The taxpayer identification number in the Substitute W-9 Form must be the same as the Contractor's Federal Employer Identification Number or Tennessee Edison Registration ID.
- C.10. A "day" shall be defined as a minimum of eight (8) hours of service. If the Contractor provides fewer than eight hours of service in a standard twenty-four hour day, the Contractor shall bill *pro rata* for only those portions of the day in which service was actually delivered. The Contractor shall not bill more than the daily rate even if the Contractor works more than eight hours in a day.

D. MANDATORY TERMS AND CONDITIONS:

- D.1. **Required Approvals.** The State is not bound by this Contract until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Contract, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval. The State represents and warrants that this Contract will be signed by the State only upon receipt of all indicated approvals.
- D.2. **Communications and Contacts.** All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by email or facsimile transmission with recipient confirmation. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address, facsimile number, or email address as stated below or any other address provided in writing by a Party.

The State:

Trey Norris
Central Procurement Office
3rd Floor, William R Snodgrass, Tennessee Tower
312 Rosa L. Parks Avenue
Nashville, TN 37243-1102
trey.norris@tn.gov
Telephone # 615-741-7148



FAX # 615-741-0684

The Contractor:

Jose Vilar, Senior Manager, Finance Operations
Zendesk, Inc.
1019 Market Street
San Francisco, CA 94103
jvilar@zendesk.com
Telephone # 415-418-7506
FAX # 415-778-9355

All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

- D.3. Modification and Amendment. This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials. The State's exercise of a valid Renewal Option or Term Extension does not constitute an amendment so long as there are no other changes to the Contract's terms and conditions.
- D.4. Subject to Funds Availability. The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and accepted by the State and for all satisfactory and authorized services completed as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount, and the State shall receive a pro rata refund for any amounts prepaid to Contractor beyond the date of a termination under this Section.
- D.5. Termination for Convenience. The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all remaining subscription charges for the remaining Service Subscription Term, and, for any professional services fees for all satisfactory, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any services neither requested nor accepted by the State or for any services neither requested by the State nor satisfactorily performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.
- D.6. Termination for Cause. If a Party ("Breaching Party") fails to properly perform its obligations under this Contract, or if a Party materially violates any terms of this Contract ("Breach Condition"), the other Party ("Non-breaching Party") may provide written notice to the Breaching Party specifying the Breach Condition. If within thirty (30) days of notice, the Breaching Party has not cured the Breach Condition, the Non-breaching Party may terminate the Contract. In the event the Non-breaching Party is the State, the State may withhold payments in excess of compensation for completed services or provided goods. The Breaching Party shall not be relieved of liability to the Non-breaching Party for damages sustained by virtue of any breach of this Contract, and the Non-breaching Party may seek other remedies allowed at law or in equity for breach of this Contract.



- D.7. Assignment and Subcontracting. The Contractor shall not assign this Contract or enter into a subcontract for any of the goods or services provided under this Contract without the prior written approval of the State, which approval shall not be unreasonably withheld. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Contract. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Contract in whole or in part or the use of subcontractors in fulfilling the Contractor's obligations under this Contract.
- D.8. Conflicts of Interest. The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Contract.
- The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.
- D.9. Nondiscrimination. The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal or state law. The Contractor shall, upon request, show proof of nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.
- D.10. Prohibition of Illegal Immigrants. The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.
- a. The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Contract Attachment 3, at the State's request. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.
 - b. Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.
 - c. The Contractor shall maintain records for all personnel used in the performance of this Contract. Such Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.



- d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.
- e. For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.
- D.11. Records. The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of five (5) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.
- D.12. Monitoring. The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives.
- D.13. Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested, in relation to professional services.
- D.14. Strict Performance. Failure by any Party to this Contract to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.
- D.15. Independent Contractor. The Parties shall not act as employees, partners, joint venturers, or associates of one another. The Parties are independent contracting entities. Nothing in this Contract shall be construed to create an employer/employee relationship or to allow either Party to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one Party are not employees or agents of the other Party.
- D.16. Patient Protection and Affordable Care Act. The Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act ("PPACA") with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless for any costs to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees.
- D.17. Limitation of State's Liability. The State shall have no liability except as specifically provided in this Contract. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, money, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. Notwithstanding anything else herein, the State's total liability under this Contract (including without limitation any exhibits, schedules, amendments or other attachments to the Contract) or otherwise shall under no circumstances exceed the Estimated Liability. This limitation of liability is cumulative and not per incident.



- D.18. Limitation of Contractor's Liability. In accordance with Tenn. Code Ann. § 12-3-701, the Contractor's liability for all claims arising under this Contract shall be limited to an amount equal to two (2) times the Estimated Liability amount detailed in Section C.1. and as may be amended, PROVIDED THAT in no event shall this Section limit the liability of the Contractor for: (i) intellectual property or any Contractor indemnity obligations for infringement for third-party intellectual property rights; (ii) any claims covered by any specific provision in the Contract providing for liquidated damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death.

The parties agree that during the Term in the event the State's procurement policies or relevant statutory law regarding the calculation of Estimated Liability of contractors change to the benefit of the State's suppliers, the parties agree to negotiate in good faith an amendment to this Contract regarding the calculation of Estimated Liability in this Contract to reflect such change in the policies or law. Any such revision is subject to the State's amendment process.

- D.19. Reserved.

- D.20. HIPAA Compliance. The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Contract.

- a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.
- b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.
- c. The State and the Contractor will sign documents, including but not limited to the business associate agreement, attached as Exhibit C, and as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.
- d. Subject to the Contract, the Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.

- D.21. Tennessee Consolidated Retirement System. Subject to statutory exceptions contained in Tenn. Code Ann. §§ 8-36-801, *et seq.*, the law governing the Tennessee Consolidated Retirement System ("TCRS"), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established under Tenn. Code Ann. §§ 8-35-101, *et seq.*, accepts State employment, the member's retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Contract to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Contract is that of "employee/employer" and not that of an independent contractor, the Contractor, if a retired



member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the Term.

- D.22. Tennessee Department of Revenue Registration. The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Contract.
- D.23. Debarment and Suspension. The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:
- a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;
 - b. have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;
 - c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and
 - d. have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded or disqualified.

- D.24. Force Majeure. "Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workarounds or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event. The remedies listed above shall not be exercised by the State



for any loss of Service for causes under the control of the State or its agents or arising from services provided by other contractors or suppliers of goods or services to the State.

- D.25. State and Federal Compliance. The Contractor shall comply with all applicable state and federal laws and regulations in the performance of this Contract applicable to its role as the provider of the Service; provided, however, that Zendesk disclaims any representations, warranties and covenants that the State's use of the Service will satisfy any statutory or regulatory obligations or government controls or mandates applicable to the State ("Regulations") or will assist with, guarantee or otherwise ensure compliance with any Regulations specifically associated with any Regulated Information. For purposes of the foregoing, the term "Regulated Information" shall mean (a) any "non-public personal information" as that term is defined in the Gramm-Leach-Bliley Act found at 15 USC Subchapter 1 Sec. 6809(4); and (b) any Customer Data as that term is used in Data Security Standards of the Payment Card Industry.
- D.26. Governing Law. This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Contract. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Contract shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 407.
- D.27. Entire Agreement. This Contract is complete and contains the entire understanding between the Parties relating to its subject matter, including all the terms and conditions of the Parties' agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the Parties, whether written or oral.
- D.28. Severability. If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Contract shall not be affected and shall remain in full force and effect. The terms and conditions of this Contract are severable.
- D.29. Headings. Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.
- D.30. Incorporation of Additional Documents. Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:
- a. any amendment to this Contract, with the latter in time controlling over any earlier amendments;
 - b. this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below);
 - c. any clarifications of or addenda to the Contractor's proposal seeking this Contract;
 - d. the State solicitation, as may be amended, requesting responses in competition for this Contract;
 - e. any technical specifications provided to proposers during the procurement process to award this Contract; and,
 - f. the Contractor's response seeking this Contract.

E. SPECIAL TERMS AND CONDITIONS:

- E.1. Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, the special terms and conditions shall be subordinate to the Contract's other terms and conditions.



- E.2. Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with applicable state and federal law.

The obligations set forth in this Section shall survive the termination of this Contract.

- E.3. Prohibited Advertising or Marketing. The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Contract. The Contractor, however, shall have the right to indicate that the State is a customer of Zendesk on its website and in other marketing materials.
- E.4. Contractor Commitment to Diversity. The Contractor shall comply with and make reasonable business efforts to exceed the commitment to diversity represented by the Contractor's Response to Contract Attachment 4 and resulting in this Contract.

The Contractor shall assist the State in monitoring the Contractor's performance of this commitment by providing, as requested, a quarterly report of participation in the performance of this Contract by small business enterprises and businesses owned by minorities, women, and Tennessee service-disabled veterans. Such reports shall be provided to the State of Tennessee Governor's Office of Diversity Business Enterprise in the required form and substance.

- E.5. Intellectual Property. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor notice of any such claim or suit and full right and opportunity to conduct the Contractor's own defense thereof, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State's failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106. Subject only to limited rights to access and use the Service as expressly stated herein, all rights, title and interest in and to the Service and all hardware, software and other components of or used to provide the Service, including all related intellectual property rights, will remain with and belong exclusively to Zendesk. Zendesk shall have a royalty-free, worldwide, transferable, sub-licensable, irrevocable and perpetual license to incorporate into the Service or otherwise use any suggestions, enhancement requests, recommendations or other feedback Zendesk receives from the State, Agents or End Users.

- E.6. Personally Identifiable Information. While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time



("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Contract, GLBA and Privacy Laws; and (ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify and/or procure that Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within twenty-four (24) hours after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor, at the sole discretion of the State, shall provide no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law.

- E.7. Contractor shall provide the State a copy of its current security attestation ("SOC 2 Report").
- E.8. Disaster Recovery. In the event of disaster or catastrophic failure that results in significant Data loss or extended loss of access to Data, Contractor shall notify the State Chief Information Security Officer, in writing, immediately and no later than within forty eight (48) hours after Contractor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Contractor shall inform the State of the following:
- 1) The scale and quantity of the Data loss;
 - 2) What Contractor has done or will do to recover the Data and mitigate any deleterious effect of the Data loss; and
 - 3) What corrective action Contractor has taken or will take to prevent future Data loss.
 - 4) If Contractor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Contract.

Contractor shall restore continuity of Zendesk, restore Data and secure accessibility of Data, and repair Zendesk as needed to meet the performance requirements stated in the this Contract. Contractor shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the



right to lead (if required by law) or participate in the investigation. Contractor shall cooperate fully with the State, its agents and law enforcement in fulfilling its mitigation, investigation, and notification obligations under applicable law or regulation.

If a Security Incident is found to be the result of Contractor's failure to take reasonable security precautions, including, but not limited to, adoption and enforcement of a technology security policy, Contractor will assume complete responsibility for notifying affected individuals as directed by the State. The State's Chief Information Security Officer, or designee, shall determine whether notification to the individuals whose Data has been lost or breached is appropriate.

E.9. Reserved.

E.10. Rights to Use and Availability. Zendesk Service may be accessed and used by authorized users of the State.

The Service will be available as set forth in Exhibit A hereto and as set forth in this Contract.

E.11. Contractor must comply with all applicable law, regulations, and state policies regarding its provision of services under this Contract including all laws, regulations, and state policies regarding the treatment of Data.

E.12. Discovery. Contractor shall promptly notify the State of any requests which in any way might reasonably require access to the Data of the State or the State's use of Zendesk. Contractor shall notify the State by in writing to the Chief Information Security Office, within forty-eight (48) hours of the receipt of the request, with additional notification provided to the Chief Information Security Officer, unless prohibited by law from providing such notification. Contractor shall not respond to subpoenas, service of process, Public Records Act requests, and other legal requests directed at Contractor regarding this Contract without first notifying the State unless prohibited by law from providing such notification. Contractor agrees to provide its intended responses to the State with adequate time for the State to review, revise and, if necessary, seek a protective order in a court of competent jurisdiction.

E.13. Data Retention. The Contractor will not destroy any of the State's data or records, even in the event of Contract cancellation or expiration, for ninety (90) days following the cancellation or final expiration date of the Contract term.

E.13.1. For ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Contractor shall assist the State in extracting and/or transitioning all Data in the format determined by the State ("Transition Period"). During the Transition Period, Zendesk and Data access shall continue to be made available to the State without alteration. Such transitioning of Data may be subject to additional fees. Following the expiration or termination of the Contract and upon the export (transitioning) of the Data, as applicable, the Data will be deleted in accordance with Zendesk's procedures.

E.13.2. No Data shall be copied, modified, destroyed or deleted by Contractor other than for normal operation or maintenance of Zendesk during the Contract period without prior written notice to and written approval by the State.

E.13.3. Upon request from authorized users of the State, Contractor shall return or destroy any State data provided under this Contract.



E.14. Contract Not Unique. The Contractor understands and agrees that the State has executed and may execute contracts with other parties for services the same as or similar to those described herein.

IN WITNESS WHEREOF,

ZENDESK, INC.:



CONTRACTOR SIGNATURE



 / 

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

7/29/15

DATE

DEPARTMENT OF GENERAL SERVICES, CENTRAL PROCUREMENT OFFICE



Michael F. Perry, Chief Procurement Officer

7/30/15

DATE



ATTACHMENT 1

REQUIREMENTS VERIFICATION EVALUATION GUIDE

REQUIREMENTS VERIFICATION. The Proposer shall enter the appropriate Response Code into the box ("Enterprise" and "Enterprise Elite" Plans) located to the right of every requirement in the Requirements Verification Matrix that follows.

Valid Response Codes:

- A = Requirement is satisfied by the Zendesk Service as provided 'out of the box'
- B = Requirement can be satisfied by the Zendesk Service with a modification, customization and/or configuration with no additional cost
- C = Requirement can be satisfied by Zendesk Service with a modification, customization, and/or configuration at an additional, separate cost
- D = Requirement can be satisfied by the Zendesk Service with a proprietary add-on, package, or third party module offered by the Proposer at an additional, separate cost
- E = Requirement cannot be satisfied by the Zendesk Service even with modification, customization, configuration, proprietary add-on, package, or third party module.

If "C" or "D" are entered, please detail any associated cost necessary for compliance with the feature in Attachment 2. It is important that all costs associated with meeting any of the requirements are described and isolated in Attachment 2.

Section	Feature	Description	Enterprise Elite Plan	Enterprise Plan
COMMUNICATION CHANNELS				
1	Email	The State has its own email domain and supports any number of email addresses. All emails sent to your center become tickets. You can set your reply ("from") address for outgoing email. Also, you can customize the HTML and text email templates.	B	B
2	Twitter	Convert tweets, DMs, and faves into tickets. Capability to monitor one or more Twitter accounts and convert tweets to tickets as needed. All tweet activity between agents and Twitter users is added as ticket comments.	B	B
3	Facebook	Convert Facebook wall posts and private messages into tickets.	B	B
4	Help Center	Build a Help Center to offer self-service options to customers and agents. Built into the solution and available in multiple languages (including English and Spanish), Help Center is knowledge base, community, and customer portal, all-in-one. Customers can find answers to their own questions; agents can use it as an internal knowledge base.	B	B
5	Mobile Help Center	Mobile-friendly version of Help Center that can be customized with various brands.	B	B
6	Zopim Chat	Provide real-time support to your customers and proactively initiate chats with visitors on your website. With tools like shortcuts and agent-to-agent chat, that allow for collaboration between agents on multiple chat conversations. Ability to determine location of customer.	D	D
7	Voice (native phone support)	Ability to make or receive customer calls in solution. Agents can set their availability and all phone conversations are recorded and tracked in tickets. Voicemail recordings and transcriptions can also be automatically captured. Recordings have a maximum length of 2 minutes.	D	D
8	Voice (multiple greetings)	Set up a customized greeting (via phone or upload of existing audio file) when routing customers to voicemail. Use the greeting to tell customers an agent will answer shortly and incorporate hold music. Multiple greetings can be set up for each solution Voice number.	B	B
9	Voice (group routing)	Set up call routing for a specified solution Voice number to a specific agent group(s) in the solution. The call will only route to agents in the assigned group. If more than one group is selected, the call will route to agents in the primary group first.	B	B
10	Cisco phone system integration	The solution must be able to integrate seamlessly with the State's Cisco phone system.	D	D
11	Microsoft Office Integration	The solution must be able to integrate with various Microsoft Office applications.	B	B



12	Channel management	Easily add, remove, or configure channels (e.g. chat, Facebook, Twitter, phone) to adapt to changing support needs.	B	B
TICKET MANAGEMENT				
13	Views	Views are a collection of tickets based on ticket status, assignee, group, or any other ticket conditions. Use views to help manage ticket workflow and organize tickets. Should come standard with pre-configured views that can be modified, turned off, or added to. The State should also be able to create their own views for personal or group(s) use.	B	B
14	Macros	Macros allow agents to quickly respond to common requests with a standard reply. In addition, macros can generate an action, like changing the status of the ticket. Should come standard with pre-configured macros that can be modified, turned off, or added to. The State should also be able to create their own macros for their personal or group(s) use.	A	A
15	Rich text formatting	Add rich text to your tickets responses by using simple text markup to add useful formatting such as headings or bullet points.	A	A
16	Custom ticket fields	Custom ticket fields help gather all the information needed around a support request. These fields can be made visible to agents and/or your customers and can appear on tickets in the solution and the support request form.	A	A
17	View original email	For any ticket, view the original email sent by the customer —including source code and HTML.	A	A
18	Attachments	Agents and customers can attach files to tickets, including via drag-and-drop files into the ticket response.	A	A
19	On-hold ticket status	When a ticket requires input and resolution from a third party, set the ticket status as on-hold, in order to differentiate response times of the State versus the third party.	A	A
20	Dynamic Content	Dynamic content is essentially multi-language placeholders that dynamically insert ticket content based on the customer's preferred language. Agents can use dynamic content to easily provide localized support interactions. Dynamic content is supported in automations, macros, triggers, and other system-generated messages.	B	B
21	Ticket forms	With ticket forms, you can create multiple support request forms that show a unique set of ticket fields. Ticket forms help ask the right questions and gather all the important information needed up-front. It can be made visible to agents and/or your customers.	B	B
22	Multibrand	Support multiple brands, products, service tiers, or regions with unique Help Centers, support channels, and business rules. Data and activity are centralized within a single account.	B	B
23	Change History Of Ticket	Users can see the previous actions step by step of an issue. Who worked on an issue, which actions were taken and when, add notes, etc.	A	A
24	Private notes/comments	Ability to comment on a ticket internally, for team collaboration.	A	A
25	Bulk Updating	Manage multiple tickets at once for greater efficiency.	A	A
26	Ticket classification	Classify tickets on multiple levels and sub-levels based on various classification criteria (e.g. product ID, customer type, key word) in a tree structure with types and sub-types. Each of those may involve changes in the parent's workflow or interfaces. Creating new ticket topics, updating existing ones could be done by business units without need of a technical support.	B	B
27	Ticket Cloning	A ticket could be cloned to create a new instance of the original ticket. Cloned tickets are related with the same customer and the original ticket automatically. This enables to submit more than one ticket for the customer at a time.	A	A
AGENT PRODUCTIVITY TOOLS				
28	Agent interface in 14 languages	Agent interface can be set in our agent's preferred language with a localized interface in English or Spanish.	A	A
29	Tickets requiring your attention	This is a view on the agent dashboard that, when the agent first logs into the solution, showcases tickets that are new and open and assigned to you, unassigned in your groups, and not currently assigned to a group.	A	A
30	Multi-tab interface	A multi-tab interface where each tab can open a ticket, a customer profile, or knowledge base search results. Agents can open multiple tabs in one view and be able to multi-task by performing several actions.	A	A
31	Instant search	Click the search icon in the navigation bar to perform an instant search across tickets, users, organizations, or Help Center in a new tab.	A	A
32	Keyboard shortcuts	Solution comes pre-built with various keyboard shortcuts to perform ticket actions and navigate through the solution.	A	A



33	Single page app	The solution a single page app built on Ember.js to allow for an interactive, real-time experience.	A	A
34	Agent collision detection	Agent collision detection prevents multiple agents working on a ticket at the same time by giving agents a warning when opening or updating a ticket that another agent is simultaneously viewing a ticket.	A	A
35	Agent alias	Agents can use an alias that will be publicly displayed on all communications with your customer.	B	B
36	Less-than-full-time agents	Unlimited Less-than-full-time agents, also known as light agents, who are only permitted to view tickets and add private comments.	A	A
37	Availability of documentation and training materials	Access to user guides, manuals, and online video training materials for customer support tool.	A	A
38	Powered User	Powered User could take an action on all type of tickets, regardless of their status and ownership.	A	A
SUPPORT WORKFLOWS				
39	Service level targets	Monitor your team's performance by setting specific service level targets for response times and time to full resolution. Tickets that threaten service level targets are highlighted in separate views.	B	B
40	Ticket sharing between accounts	Tickets from your account can be shared with other accounts for external collaboration, and vice versa. Should be able to share manually or set to share automatically.	A	A
41	Business rules: Triggers	Triggers initiate a workflow based on specific changes or actions on a ticket. Your account comes with pre-configured triggers that we recommend as best practices. Should come standard with pre-configured triggers that can be modified, turned off, or added to.	A	A
42	Business rules: Automations	Automations initiate a workflow based on time-based conditions. Should come standard with pre-configured automations that can be modified, turned off, or added to.	A	A
43	Business hours	Set business hours in your account and apply to ticket workflows, triggers, automations, and SLA targets.	A	A
44	Business rules filtering by usage	Filter and sort business rules (by date created, date updated, group, and category) to gain an understanding of how your automations, macros, triggers, and views are used.	A	A
45	Business rules analysis	Analyze the usage and effectiveness of your business rules, like triggers, automations, macros, and views.	A	A
46	User Priority Specification	Ability to set/change predetermined priorities of the tickets in the submit form.	A	A
47	Automatic distribution of tasks and tickets	Based on the ticket property, channel, ticket location, location of the support available and current workload. In any step in the workflow, the actions or tasks can be distributed to the employees of the groups based on their workload. The distribution could be done by any number of tasks (one by one, 10 by 10, etc.)	A	A
48	Custom alerts and notifications	Alert users or user groups with the proper automated notifications (i.e. action required, ticket status) to support a more efficient, transparent workflow (through e-mail and the Solution)	A	A
KNOWLEDGE BASE				
49	Knowledge base	In Help Center, create a resource of helpful articles that answer customers' most popular questions. Sections within the knowledge base can be restricted to certain groups of customers by specifying an organization or tag.	A	A
50	Help Center category and section	Each article in the Help Center is organized into category and sections.	A	A
51	Promoted articles	Highlight articles that you want to be more prominent in Help Center. Promoting an article moves it to the first position of an article list. It also highlights the article in the list with a star to draw attention to it.	A	A
52	Internal knowledge base	The State should be able to create an internal knowledge base for agents to be able to reference information, documentation, and processes.	A	A
53	Ticket-to-article integration	Easily turn a useful ticket into a knowledge base article.	A	A
COMMUNITY				
54	Community	A community where customers and logged-in users can engage with one another in a community discussion to gather feedback and ideas.	A	A
55	Community post	Contribute a community post to ask a question or suggest useful information such as tips, feature requests, etc. Allow customers to choose to follow a post.	A	A
56	Community topic	Community posts are organized under various topics. Set community topics around feature requests, product tips, or other popular discussions. Your customers can choose to follow a topic.	A	A
57	Community voting	The community in Help Center gives your customers the opportunity to vote questions and answers— from other customers— up and down.	A	A



58	Community official answers	For any community question, provide a company-approved answer. The answer will be denoted as the official answer and moved to the top of the answer list. Only admins or approved users will be able to provide an official answer.	A	A
59	Trending questions	Intelligently surface the most popular community questions, directly in your customers' view, based on top searches, views, and activity.	A	A
CUSTOMER PORTAL				
60	Customer activities	Customers can log into a dedicated customer portal to access their ticket history and activity, submit and track tickets, and view a list of subscribed community topics and questions.	A	A
61	Follow a question, article, or topic	Any logged-in user can follow community topics, questions, or knowledge base articles. They will receive alerts on any update made to that topic, question, or article, so they can stay up-to-date on conversations of interest.	A	A
CONTENT MANAGEMENT TOOLS				
62	Rich text formatting	Format your articles by applying styles such as Bold, italicize, underline, etc. to the text. Insert video, images, or tables to add visual elements.	A	A
63	Drag and drop content arrangement	Move articles from section to section on the individual article pages, or re-arrange articles, sections, and categories via drag and drop on the Arrange Content page.	A	A
64	Integrated search	Search the knowledge base and community simultaneously.	A	A
65	Draft articles	Add draft articles in Help Center that are saved but not published. Publish a draft article or unpublish a live article with a tick of a checkbox on the article page.	A	A
66	Multilingual content management	Enable multiple languages in your Help Center and surface only articles in the customer's preferred language. Add localized content and manage all your multilingual content in one place.	A	A
67	Dynamic Content	Support Dynamic Content that dynamically inserts ticket content based on the customer's preferred language.	A	A
68	Asset Tracking and Inventory	Product, service, contact or inventory data could be added to ticket forms.	D	D
BRANDING AND CUSTOMIZATIONS				
69	Localized interface	Help Center's admin interface can be set in your preferred language with a localized interface in multiple languages (including English and Spanish).	A	A
70	Support for multiple languages	Specify the languages you want to support in your Help Center, and set a different name for the Help Center for multiple support languages (including English and Spanish).	A	A
71	Customization panel	Built into Help Center is a customization panel where you can change your Help Center theme, colors, fonts, logo, and name.	A	A
72	Real-time preview	See the customizations you make in real-time without affecting what your customers are seeing in your live Help Center. You can preview by role—: anonymous, logged in customer, agent, or manager.	A	A
73	Themes	Select a theme to quickly change the layout of your Help Center. Themes are design layouts built on self-service best practices. You can select from several pre-defined themes and further customize the theme.	A	A
74	Unlimited Branded Help Centers	Manage multiple Help Centers—each with a unique destination, content, and branded design—from a single account.	A	A
75	Branding for mobile Help Center	After enabling the mobile version of Help Center, customize the logo, favicon, and colors to match your company's brand.	A	A
76	Built-in HTML editor	Help Center comes with a built-in code editor so you can customize Help Center with HTML, CSS, or JavaScript. Select a template to access the page code.	A	A
77	Templates	Work with the page code used to build the Help Center. The code is contained in editable templates that define the layout of each page type. Help Center templates include home page, category page, or article page, as well as the global header and footer.	A	A
78	Components	No code experience should be needed for basic customization. Should include components, a set of code that enables a functionality to occur. Components are inserted into the page code on any template to perform advanced customizations to Help Center.	A	A
79	Host mapping	Host mapping, also known as domain mapping, enables you to use your own subdomain, such as help.mycompany.com. This allows you to route users from a company page to the solution page automatically.	B	B
80	Embeddable Widgets	Ability to add various widgets to the dashboard.	A	A



CUSTOMER CONTEXT				
81	Customer profiles	View information about your customers such as basic contact info, language preferences, and other customer data captured in custom user fields.	A	A
82	User Data app	App that gives you a view of customer information and —user and organization details like tags, ticket activity, and contact info —right next to a ticket.	A	A
83	Custom user and organization fields	Custom user and organization fields capture information about individual customers. In addition, custom user and organization fields can be used in triggers and automations, so dedicated workflows can be set based on customer data.	A	A
84	Customer lists	Customer lists are a group of customers filtered by the custom user/org fields and tags you set. Export a list to a CSV file.	A	A
85	Membership- Anonymous Customer Entry	Customers can access the customer interface through either a registered account (with an e-mail address and password) or anonymously.	A	A
86	Enterprise Capability	Ability to link multiple agency accounts into one portal allowing for custom reporting.	A	A
REPORTING AND ANALYTICS				
87	Key Benchmark Metrics	Compare yourself against your peers on key benchmark metrics like customer satisfaction, first response time, and ticket volume.	A*	A*
88	Export ticket view to CSV	Export a ticket view to a CSV file, containing an entry for each ticket and all its associated ticket information in the view.	A*	A*
89	Support performance dashboards	Measure your performance by having visibility into ticket volume, agent performance, and other key support metrics. Data in the reporting dashboard should be updated on a minimum hourly basis.	A*	A*
90	Customer satisfaction ratings	Your customers can rate how satisfied they are with the support they received. By default, your customers will receive an email 24 hours after the ticket has been set to solved that asks whether the customer is satisfied or unsatisfied.	A*	A*
91	Google Analytics	Set up custom event tracking around specific customer activity, like the actions a visitor takes prior to submitting a ticket.	B*	B*
92	Help Center dashboards	Get an instant snapshot of your Help Center activity with three pre-built dashboards that capture trends around knowledge base activity, community engagement, and search behaviors.	A*	A*
93	Time tracking	Automatically track the time spent on each of your tickets.	B*	B*
94	Custom reports & dashboards	Ability to build custom dashboards and reports. Interact, filter, and drill into over 50 best practice reports (including from custom fields) to measure operational efficiency, agent performance, and customer experience.	B*	B*
95	Share Reports	Share reports with others ad hoc, or schedule reports to be sent regularly via email.	A*	A*
96	Hourly data sync for reporting	Data synched every hour (at a minimum) for reporting purposes.	A*	A*
97	Built-in reports on key metrics	Pre-built reports in the support tool that analyze and visualize data on customer service metrics such as: -Survey Report/ Track Summary of Satisfaction Ratings from Survey Results -Performance Reports / Tracking user, group and unit performances -Analysis Reports / Average solution time and escalations. -Distribution Reports / Reporting ticket distributions according to the communication channel, ticket type and different parameters. -Status Reports / Reporting ticket status -Operational Reports / Exportable ticket Lists, History, Details. -System Reports / Logs of user actions, SMS, e-mail deliveries etc. -Self-Service Reports/ Analytics of customer self-service actions (i.e. search key words and popular articles)	A*	A*
SECURITY AND ACCESS				
98	SSO (Single sign-on) with SAML support	Secure Assertion Markup Language (SAML) should be supported, which allows the State to provide single sign-on (SSO) for the solution using enterprise identity providers such as Active Directory and LDAP. Additionally, SSO for user authentication means that users can access the solution with existing credentials such as Facebook, Twitter, or Google without needing to enter separate login credentials.	A	A
99	Configurable password policy	Solution provides the following levels of password security: low, medium, and high. Set one password security level for end-users, and a different one for admins and agents. High level users, such as admins, should be able to specify custom password security levels.	A	A
100	Agent device management	Solution tracks the devices used to sign in to your account. Check the list on a regular basis for any suspicious devices. Admins will receive an email notification when a new device is added.	A	A



101	SSL (Secure Socket Layer) encryption/ certificate hosting	SSL should be enabled by default to ensure secure communications between the State and solution's web portal. The secure connection is indicated in the customer's browser by https (for HTTP Secure) in the URL and by a padlock icon in the address bar. The general setup workflow should consist of obtaining a SSL certificate from a certificate authority and then sending it to the vendor to install on their servers.	A	A
102	Digitally signed emails (DKIM/DMARC)	Supporting the DKIM and DMARC standards, digitally sign outbound emails from solution to prove that an email actually came from somebody in the State and not somebody pretending to be from the State.	A	A
103	Sandbox test environment	Ability to Perform tests on the solution in a trial environment, separate from our production instance.	A	A
104	Network access restriction	Restrict account access to specified IP ranges. Choose to apply restriction to all users or only to the agent portal.	A	A
105	Custom roles and permissions	Specify granular permissions for agents, and control what they have access to in the solution. This allows you to define agent roles that suit your own organizational structure and workflow.	A	A
106	Audit logs	View a detailed list of critical changes (account, user, business rules, tickets, etc.) that have been made to your account.	A	A
107	Email compliance archive	Send all account email notifications privately to an external address of our choice, keeping a complete archive of communication.	A	A
108	U.S. location	Vendor should have a primary location of business in the U.S.	A	A
109	Data Storage	Data to be stored in cloud on U.S. based servers whether in-use or at-rest	A	A
110	Web Traffic and Visitor Monitoring	Ability to monitor web traffic and track visitors in real time, graphically.	C/B	C/B
111	Integrated Screen Recordings	Remote web and e-mail case capture.	C	C
112	PCI Certified Cloud	PCI certification to allow for use of payment card over the Cloud Solution	E	E
113	ISO 10002:2004 Support	Compliance with international quality management standards that promote customer satisfaction: ISO, ITIL and COBIT. Certifications on customer complaints and customer satisfaction management require a system that identifies complaints and causes, and that creates solution processes and analyzes customer satisfaction.	A	A
114	ISO 27001 Compliance	Risk assessment process should align with ISO 27001 STANDARD.	A	A
115	Health Insurance Portability & Accountability Act (HIPAA) compliance	Compliance with HIPAA	B	B
116	National Institute of Standards & Technology (NIST) compliance	Compliance with NIST	E	E
117	Federal Information Security Management Act (FISMA) compliance	Compliance with FISMA	E	E
API AND INTEGRATIONS				
118	REST, Email, JavaScript API	Ability to use an API to automate and enhance customer support for solution. Documentation for the latest API should be available via the web at no additional cost to the State.	A	A
119	Additional third party apps	Plugs into third party apps and integrations with tools for time tracking, CRM, bug tracking, e-commerce, and many others.	A**	A**
120	MailChimp Campaign app	Send an email (through solution) with MailChimp to a targeted customer list. View past email campaigns delivered to a customer in the MailChimp App next to a ticket.	B	B
121	SurveyMonkey Create app	Send a survey (through the solution) with SurveyMonkey to a targeted customer list. The integration should come pre-configured with several survey templates.	B	B
122	Net Promoter Score survey	Send an NPS survey (through the solution) to measure customer loyalty and gather customer feedback. As customers' responses flow in, their latest NPS rating and comment will be captured in their user profile.	B**	B**

*Subject to use of GoodData within the Zendesk Application. Without GoodData, the reporting responses become B's.

**Based on third party terms of service discussion with procurement.



PRICING SCHEDULE

Please provide a fee breakdown. Be sure to isolate costs between the software—agents, maintenance, and estimated implementation costs, as well as any additional fees associated with the following features. Please note any add-on cost or included in per-agent pricing. Please specify the unit of measure for the pricing (monthly, annually, hourly, etc). Also, please note any caps or limits to use. This Section must isolate any cost that could be charged or associated with this Contract. If costs for any of the above are included in the per agent pricing, please specify that is included.

ELITE

Price Per Agent (Monthly)

Number of agents purchased - Aggregate total for net new agents

Zendesk SKU	Term	1-300	301-499	500+
<i>ENTERPRISE EDITION</i>	12 Month	\$146.00	\$140.00	\$130.00
<i>ENTERPRISE EDITION</i>	24 Month	\$140.00	\$135.00	\$125.00
<i>ENTERPRISE EDITION</i>	36 Month	\$135.00	\$130.00	\$120.00
<i>Zopim Chat</i>		\$12.50	\$12.50	\$12.50
<i>Zendesk Voice</i>	<i>Bulk purchase of 60,000 Minutes @ \$50,000/Block</i>			

ENTERPRISE EDITION

Price Per Agent (Monthly)

Number of agents purchased - Aggregate total for net new agents

Zendesk SKU	Term	1-300	301-499	500+
<i>ENTERPRISE EDITION</i>	12 Month	\$104.25	\$100.00	\$96.00
<i>ENTERPRISE EDITION</i>	24 Month	\$100.00	\$94.00	\$88.00
<i>ENTERPRISE EDITION</i>	36 Month	\$96.00	\$92.00	\$86.00
<i>Zopim Chat</i>		\$12.50	\$12.50	\$12.50
<i>Zendesk Voice</i>	<i>Bulk purchase of 60,000 Minutes @ \$50,000/Block</i>			

1 The pricing above is based on the aggregate number of Agents purchased by the State under the Pro Forma Contract executed between the parties identified as Contract #46567 ("Contract"). Departments wishing to participate are eligible for discounts based on the total number of Agents that the State subscribes to at the time of each purchase order issued by the State during with the Contract Term.

2 When additional Agents are purchased by a Department, they will be added co-terminously, at the appropriate *pro rata amount* through the end of the agreement, with said Department's existing Agents. These additional agents may be renewed with the existing seats upon the end of the initial subscription term.



- 3 After an initial Subscription Term for a Department expires, the Department may continue to use Zendesk on a month-to-month basis at the list price posted at www.zendesk.com/product/pricing - or the Department may renew for the same term at the pricing tier based on the State's aggregate purchases at time of the renewal.

- 4 Upon expiration of a Subscription Term for a Department, a Department that has purchased under the Contract may renew the Service for the corresponding rate based on the total number of Agents the State subscribes to at the time of renewal purchase order issuance.

- 5 "Subscription Term" as used above assumes minimum amount of time that a Department commits to paying for the Service under the Contract. Departments can terminate the Service during the committed term but will not be eligible for refund or credit for any unused portion of the Department's Subscription Term.

example:

Department 1 buys 250 Enterprise seats for 12 months term starting 6/30/15. On 9/30/15 they add 150 net new enterprise seats. The add on order sequence would be

250 - 6/30/15 @ 104.25

50 - 9/30/15 @104.25

100 - 9/30/15 @ 100.00

All subsequent departments are eligible for new discount rate until next threshold is achieved



ATTACHMENT 3

ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE

SUBJECT CONTRACT NUMBER:	
CONTRACTOR LEGAL ENTITY NAME:	Zendesk, Inc.
FEDERAL EMPLOYER IDENTIFICATION NUMBER: (or Social Security Number)	26-4411091

The Contractor, identified above, does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.

DocuSigned by:
Marcus Bragg
F6892E0A0D09418...



CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. Attach evidence documenting the individual's authority to contractually bind the Contractor, unless the signatory is the Contractor's chief executive or president.

Marcus Bragg

SVP WW Sales & Customer Success

PRINTED NAME AND TITLE OF SIGNATORY

7/17/2015

DATE OF ATTESTATION



LETTER OF DIVERSITY COMMITMENT

Zendesk, Inc.
1019 Market Street
San Francisco, CA 94103

Zendesk, Inc. ("Zendesk") is committed to assisting the State of Tennessee with its supplier diversity efforts. Diversity businesses are defined as those that are owned by minority, women, small business and Tennessee service-disabled veterans which are certified by the Governor's Office of Diversity Business Enterprise (Go-DBE). We accept that our commitment to diversity advances the State's efforts to expand opportunity of diversity businesses to do business with the State as contractors and sub-contractors.

Zendesk is committed to working with the Go-DBE office to accomplish this goal.

Regards,

DocuSigned by:

Marcus Bragg

F6892E0A0D09418...

Marcus Bragg
Senior Vice-President
Worldwide Sales & Customer Success



Exhibit A Service Level Commitments

Zendesk agrees to take all commercially reasonable efforts to make the Service available at all times except for: (a) Planned Downtime, or (b) Force Majeure Event(s). Zendesk cannot guarantee the performance and/or availability of internet service providers employed by the State or any network outside of Zendesk's control. Zendesk will use commercially reasonable efforts to schedule Planned Downtime for weekends (Pacific time zone) and other off-peak hours.

Zendesk will provide at least 99.5% Service Availability over any calendar month. "Service Availability" means all time periods other than continuous periods of ten (10) minutes or more during which time 10% or more of the State's Agents and End-Users are unable to communicate via the Service ("Downtime"), excluding Downtime resulting from Force Majeure Events, Planned Downtime not exceeding four (4) hours in such calendar month, or any suspension or termination of the State's rights to access or use the Service pursuant to Sections B.4 and D.6. of this Contract ("Permitted Suspension").

Zendesk will restore Service Availability (other than Downtime resulting from Force Majeure Events or any Permitted Suspension) within four (4) hours of the commencement of any Downtime.

If Zendesk fails to reach the above-detailed Service Availability and Service restoration commitments in any three (3) consecutive calendar months (a "Service Level Failure"), the State's sole and exclusive remedy is to cancel its Account and terminate its subscription to the Service within thirty (30) days of the Service Level Failure. Upon such termination, Zendesk will, upon request, repay the State, on a pro-rated basis, any Subscription Charges previously paid to Zendesk for the corresponding unused portion of the State's Subscription Term.



Exhibit B Security Standards

As of the Effective Date of the Contract, Zendesk will abide by the security standards set forth below ("Security Standards"). During the Subscription Term, these Security Standards may change without notice, as standards evolve or as additional controls are implemented or existing controls are modified as deemed reasonably necessary by Zendesk.

1. Security Policies and Personnel. Zendesk has and will maintain a managed security program to identify risks, implement preventative technology as well as technology and processes for common attack mitigation. This program is and will be reviewed on a regular basis to provide for continued effectiveness and accuracy. Zendesk has, and will maintain, a full-time information security team responsible for monitoring and reviewing security infrastructure for Zendesk networks, systems and services, responding to security incidents, and developing and delivering training to Zendesk employees on compliance with Zendesk security policies.
2. Data Transmission. The State's account will have Hypertext Transfer Protocol Secure (HTTPS) enabled by default. Information sent via HTTPS is encrypted from the time it leaves Zendesk until it is received by the recipients' computer. In addition, if the State has subscribed to the Plus+ or Enterprise Service Plans it may upload an SSL certificate for its custom domain.
3. Incident Response. Zendesk has an incident management process for security events that may affect the confidentiality, integrity, or availability of its systems or data. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. The incident response program includes 24x7 centralized monitoring systems and on-call staffing to respond to service incidents.
4. Access Control and Privilege Management. Zendesk restricts access to customer production systems to operational personnel. Zendesk requires such personnel to have unique IDs and associated cryptographic keys. These keys are used to authenticate and identify each person's activities on Zendesk systems, including access to customer data. Upon hire, operational personnel are assigned unique keys. Upon termination, these keys are revoked. Access rights and levels are based on an employee's job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities.
5. Network Management and Security. The data centers utilized by Zendesk maintain industry standard fully redundant and secure network architecture with reasonably sufficient bandwidth as well as redundant network infrastructure to mitigate the impact of individual component failure. The Zendesk information security team utilizes industry standard utilities to provide defense against known common unauthorized network activity, monitors security advisory lists for vulnerabilities, and undertakes regular external vulnerability audits.
6. Data Center Environment and Physical Security. The data center environments which are utilized by Zendesk in connection with its provision of the Service employ the following security measures:
 - A security organization responsible for physical security functions 24x7x365.
 - Access to areas where systems or system components are installed or stored within data centers is restricted through security measures and policies consistent with industry standards.
 - N+1 uninterruptable power supply and HVAC systems, backup power generator architecture and advanced fire suppression.



Exhibit C BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is made and entered into by and between Zendesk, Inc., a Delaware corporation with offices at 1019 Market Street, San Francisco CA 94103 ("Zendesk") and State of Tennessee, Department of General Services, Central Procurement Office ("Subscriber" or "Company"). Zendesk and Subscriber are hereinafter sometimes referred to collectively as the, "Parties".

RECITALS

- A. Subscriber is a "covered entity" or a "business associate" under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and 45 CFR Part 160.103 and, as such, must enter into so-called "business associate" contracts with certain contractors that may have access to certain health-related personal information regulated by HIPAA.
- B. Pursuant to the Contract, Zendesk provides the Service to Subscriber, including the provision of the HIPAA Enabled Account(s) and the Service accessible by the HIPAA Enabled Account(s). To facilitate Zendesk's provision and support of the Service, Subscriber wishes to disclose certain information to Zendesk, some of which may constitute Protected Health Information (defined below).
- C. Subscriber and Zendesk desire to protect the privacy, and provide for the security, of Protected Health Information that Zendesk may create, receive, maintain, or transmit pursuant to its performance of the Service, in compliance with HIPAA, the Health Information Technology for Economic and Clinical Health Act of 2009, Public Law 111-005 ("HITECH Act"), and HIPAA Regulations (defined below) promulgated thereunder by the U.S. Department of Health and Human Services.
- D. As part of the HIPAA Regulations, the Privacy Rule and the Security Rule (each defined below) require Subscriber to enter into a contract with Zendesk containing specific requirements prior to the disclosure of Protected Health Information, as set forth in, but not limited to, Title 45, §§ 164.314(a), 164.502(e) and 164.504(e) of the Code of Federal Regulations ("C.F.R.") and contained in this BAA.

NOW, THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to this BAA, Subscriber and Zendesk agree as follows:

AGREEMENT

1 Applicability and Definitions.

- 1.1 **Applicability.** This BAA applies only to Subscriber's HIPAA Enabled Accounts. This BAA does not apply to any other Account that Subscriber may have now or in the future, and Subscriber acknowledges that PHI shall not be stored or transmitted in or through the Service except through a HIPAA Enabled Account to which this BAA applies.
- 1.2 **Definitions.** Capitalized terms not otherwise defined in this BAA shall have the meanings assigned to such terms under the Contract, HIPAA, the HITECH Act, and the HIPAA Regulations, as applicable. The following terms shall have the following meanings in this BAA:

"Breach" has the meaning given to such term under 42 U.S.C. § 17921(1) and 45 C.F.R.



§164.402.

"Business Associate" has the meaning given to such term under 42 U.S.C. § 17938 and 45 C.F.R. § 160.103.

"Covered Entity" has the meaning given to such term under 45 C.F.R. § 160.103.

"Designated Record Set" has the meaning given to such term 45 C.F.R. § 164.501.

"Electronic Protected Health Information" or **"EPHI"** means Protected Health Information that is maintained in or transmitted by electronic media.

"Electronic Health Record" has the meaning given to such term under 42 U.S.C. § 17921(5).

"Health Care Operations" has the meaning given to such term under 45 C.F.R. § 164.501.

"HIPAA Enabled Account" shall mean an Account to the Service which meet all the requirements set forth in this BAA, including without limitation, being an Account under a HIPAA Enabled Subscription Plan and compliance with the configuration and security requirements set forth in Section 3.4.

"HIPAA Enabled Subscription Plan" shall mean Zendesk's Enterprise and Enterprise Elite Service Plans.

"HIPAA Regulations" means, collectively, the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Parts 160 and 164.

"Privacy Rule" means the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

"Protected Health Information" or **"PHI"** means any information, whether oral or recorded in any form or medium: (a) that relates to the past, present or future physical or mental 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 (b) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under 45 C.F.R. § 160.103, but limited to such information that Zendesk creates, receives, maintains, and/or transmits for or on behalf of the Subscriber in the performance of the Service and that is held by Zendesk as contemplated by 45 C.F.R. § 164.308(a)(1)(ii)(A). Protected Health Information includes Electronic Protected Health Information.

"Purchase Order" has the meaning as set forth in the Contract.

"Security Rule" means the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

"Service" has the meaning as set forth in the Contract. For avoidance of doubt, Subscriber acknowledges and agrees that Service shall not be deemed to include and this BAA shall not apply to (a) any service, software, tools, or technology provided by any Zendesk Affiliate, including without limitation, the hosted online communication services provided by Zopim Technologies Pte Ltd; (b) Zendesk Voice or any data, call recordings and recorded voicemails in Zendesk Voice; or (c) any Other Services (as defined in the Contract), including, for avoidance of doubt, any Subscriber-managed or third-party email service to which any HIPAA-Enabled Account is connected or integrated.

"Contract" means the Pro Forma Contract executed by Zendesk and Subscriber, such other



definitive agreement by and between Zendesk and Subscriber governing the terms and conditions of Subscriber's use of and access to the Service.

"**Unsecured PHI**" has the meaning given to such term under 42 U.S.C. § 17932(h), 45 C.F.R. §164.402 and guidance issued pursuant to the HITECH Act including, but not limited to that issued on April 17, 2009 and published in 74 Federal Register 19006 (April 27, 2009), by the Secretary of the U.S. Department of Health and Human Services ("**Secretary**").

"**Zendesk Voice**" has the meaning as set forth in the Contract.

2 Obligations of Zendesk.

2.1 Permitted Access, Use or Disclosure.

Zendesk shall:

- (a) use appropriate safeguards and comply, where applicable, with the Security Rule with respect to EPHI, to prevent use or disclosure of PHI other than as provided for in this BAA;
- (b) not use or disclose, PHI other than as permitted or required by the Contract or this BAA, or as permitted or required by applicable law; and
- (c) be permitted to use PHI to de-identify such information in accordance with 45 CFR 164.514(a)-(c) to deliver and improve the Service, and shall be permitted to use such de-identified information as permitted by applicable law.

Except as otherwise limited in the Contract or this BAA, Zendesk may access, use, or disclose PHI:

- (a) to perform or provide the Service, including, subject to the other provisions of this Section 2.1 to any subcontractor that Zendesk utilizes in performing or providing the Service; and
- (b) for the proper management and administration of Zendesk, or to carry out Zendesk's legal responsibilities, provided that such access, use, or disclosure would not violate HIPAA, the HITECH Act, the HIPAA Regulations, if done or maintained by Subscriber.

If Zendesk discloses PHI to a third party, other than at the instruction or direction of the Subscriber, Zendesk shall obtain, prior to making any such disclosure:

- (a) reasonable assurances from such third party that such PHI will be held confidentially and only disclosed as required by applicable law, and
- (b) agreement from such third party to promptly notify Zendesk of any instances of which it is aware that the confidentiality of the information has been breached.

2.2 Safeguards. Zendesk shall implement reasonable safeguards designed to prevent the access, use or disclosure of PHI other than as permitted by the Contract or this BAA. Zendesk shall use administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of EPHI. Zendesk shall comply with each of its obligations under the applicable requirements of 45 C.F.R. §§ 164.308, 164.310, and 164.312 and the policies and procedures and documentation requirements of the HIPAA Security Rule set forth in 45 C.F.R. § 164.316.

2.3 Reporting of Improper Access, Use or Disclosure.



- (a) Generally. For all reporting obligations under this BAA, the parties acknowledge that, because Zendesk does not know the nature of PHI contained in Subscriber's HIPAA Enabled Account(s), it may not be possible for Zendesk to provide information about the actual identities of individuals who may have been affected, or a description of the type of information that may have been subject to impermissible use or disclosure, any Security Incident or any Breach. However, if this information is known to Zendesk then it shall provide it to Subscriber unless legally impermissible to do so.
- (b) Impermissible Use or Disclosure. Zendesk shall promptly notify Subscriber of security incidents of which Zendesk becomes aware and/or any use or disclosure of PHI not provided for by this BAA of which Zendesk becomes aware.
- (c) Security Incidents. Zendesk shall, as requested by Subscriber, report to Subscriber on a regular and periodic basis (not to exceed more than once in any quarterly period) the existence and occurrence of "Unsuccessful Security Incidents" (as defined below). The parties agree that compliance with this section shall satisfy Zendesk's obligations to provide Subscriber notice of the existence and occurrence of Unsuccessful Security Incidents, for which no additional notice shall be required. For purposes of this BAA, the term "Unsuccessful Security Incident" shall mean any security incident that does not result in any unauthorized access, use, disclosure, modification, or destruction of electronic PHI or any interference with system operations in Zendesk's information system. Notwithstanding the foregoing, the parties acknowledge that notice is hereby deemed provided, and no further notice will be provided, for Unsuccessful Security Incidents such as pings and other broadcast attacks on firewalls, denial of service attacks, port scans, unsuccessful login attempts, interception of encrypted information where the key is not compromised, or any combination of the foregoing.
- (d) Breaches of Unsecured PHI. Without limiting the generality of the reporting requirements set forth in Section 2.4(a), Zendesk also shall, to the extent permitted by applicable law following the discovery of any Breach of Unsecured PHI, notify Subscriber in writing of such Breach without unreasonable delay and in no case later than thirty (30) days after discovery. The notice shall include the following information if known (or can be reasonably obtained) by Zendesk: (i) a brief description of the circumstances of the Breach, including the date of the Breach and date of discovery; and (ii) a brief description of what the Zendesk has done or is doing to investigate the Breach and to mitigate harm created by the Breach.
- (e) Mitigation. Zendesk shall establish and maintain safeguards to mitigate, to the extent practicable, any deleterious effects known to Zendesk of any unauthorized or unlawful access or use or disclosure of PHI not authorized by the Contract, or this BAA.
- 2.4 Business Associate's Subcontractors. Zendesk shall ensure that any subcontractors to whom it provides PHI agree to the same restrictions and conditions to those that apply to Zendesk with respect to such PHI. To the extent that Zendesk creates, maintains, receives or transmits EPHI on behalf of the Subscriber, Zendesk shall ensure that any of Zendesk's subcontractors to whom it provides PHI agrees to implement the safeguards required by Section 2.2 (Safeguards) with respect to such EPHI. Subscriber agrees and acknowledges that no provider of an Other Service shall be deemed a subcontractor or agent of Zendesk for purposes of this Agreement and that Subscriber shall be solely responsible for the transmission and disclosure to, and access, use or disclosure of, any PHI to any provider of an Other Service.



- 2.5 Access to PHI. If and to the extent Zendesk maintains a Designated Record Set on behalf of the Subscriber, Zendesk shall make PHI maintained by Zendesk in that Designated Record Set available to Subscriber for inspection and copying, within a reasonable period of time following ten (10) calendar days of a request by Subscriber, as required to enable Subscriber to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. § 164.524. If Zendesk maintains an Electronic Health Record, Zendesk shall provide such information in electronic format to enable Subscriber to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. § 17935(e). To the extent that an individual makes a request to Zendesk for access to a Designated Record Set or Electronic Health Record that Zendesk maintains on behalf of the Subscriber, Zendesk shall forward such request to the Subscriber promptly within ten (10) calendar days of receipt and advise the individual that the Subscriber is responsible to respond to the request. Subscriber agrees that it, and not Zendesk, is responsible for responding to the individual to fulfill its obligations under the HIPAA Regulations.
- 2.6 Amendment of PHI. If and to the extent Zendesk maintains a Designated Record Set on behalf of Subscriber, Zendesk shall, within a reasonable period of time, make that PHI available to Subscriber so that Subscriber may make any amendments that Subscriber directs or agrees to in accordance with the Privacy Rule. Zendesk and Subscriber hereby acknowledge and agree that Zendesk does not, incident to its provision of the Service, maintain a Designated Record Set on behalf of Subscriber.
- 2.7 Accounting Rights. Zendesk shall, within a reasonable period of time to enable Subscriber to fulfill its obligations under the Privacy Rule and the HITECH Act, make available to Subscriber the information required to provide an accounting of disclosures requested by an individual. Zendesk may charge Subscriber a reasonable fee for performance of its obligations pursuant to this Section 2.7. Zendesk and Subscriber hereby acknowledge and agree that Zendesk does not, incident to its provision of the Service, maintain a Designated Record Set on behalf of Subscriber.
- 2.8 Governmental Access to Records. Zendesk shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining Subscriber's compliance with the Privacy Rule.
- 2.9 Minimum Necessary. To the extent feasible in the performance of services under the Contract, Zendesk (and its agents or subcontractors) shall request, use, and disclose only the minimum amount of PHI necessary to accomplish the purpose of the request, use, or disclosure.
- 3 Obligations of Subscriber.**
- 3.1 Acceptable Collection Methods. Subscriber acknowledges that once an account is classified as a HIPAA Enabled Account, that classification is irreversible unless done so by Zendesk due to Subscriber's downgrade to a Service Plan other than a HIPAA Enabled Subscription Plan. Zendesk permits Subscriber to collect PHI only through HIPAA Enabled Account(s).
- 3.2 Covered Entity or Business Associate. The obligations with regard to the treatment and handling of PHI in this BAA only apply while Subscriber is a Covered Entity or Business Associate.
- 3.3 Subscription Plan. Only HIPAA Enabled Subscription Plans support HIPAA Enabled Account(s) and this BAA may only be entered into if the HIPAA Enabled Account is under a HIPAA Enabled Subscription Plan. Under the Contract, the State shall only subscribe to the Enterprise or Enterprise Elite plans.
- 3.4 Security Configurations. Subscriber is solely responsible for configuring, and will configure all HIPAA Enabled Account(s) to which this BAA applies as follows:



- (a) Secure Agent authentication through one of two methods:
- (i) Employing native Zendesk with password settings: (1) set to "High" as described at <https://support.zendesk.com/hc/en-us/articles/203663736-Setting-the-password-security-level-for-your-Zendesk-Plus-and-Enterprise->; or (2) customized by Subscriber in a manner that establishes requirements not less secure than those established under the "High" setting. Additionally, if and to the extent that Zendesk provides 2-factor authentication natively within the Service, Subscriber will enable such functionality with respect to the Account(s) for all Agent access. Administrative controls that permits administrators to set passwords for End-Users must be disabled.
 - (ii) Utilizing an external "single-sign on" solution with established requirements not less secure than those established under the Zendesk "High" password setting and enabling and enforcing 2-factor authentication within the selected solution for all Agent access. Administrative controls that permits administrators to set passwords for End-Users must be disabled.
- (b) Secure Socket Layer encryption on HIPAA Enabled Account(s) must be and remain enabled at all times. HIPAA Enabled Accounts which utilize a subdomain other than zendesk.com must establish and maintain hosted SSL as described at <https://support.zendesk.com/hc/en-us/articles/203663726-Providing-secure-communications-with-SSL>.
- (c) Agent access must be restricted to specific IP addresses under the control of Subscriber as described at <https://support.zendesk.com/hc/en-us/articles/203663706-Restricting-access-to-your-Zendesk-using-IP-restrictions-Plus-and-Enterprise->
- (d) To the extent Subscriber's HIPAA Enabled Account enables calls to Zendesk APIs, Subscriber shall implement OAuth 2.0 as an authentication scheme to the extent practicable as described at <https://developer.zendesk.com/blog/using-oauth-to-authenticate-with-zendesk-api-v2>. Subscriber shall rotate API tokens not less than every one hundred and eighty (180) days and shall not share API tokens with any third-party except as reasonably required and pursuant to transmission methods which are encrypted from end to end.
- 3.5 Authorizations. Subscriber shall obtain and maintain any and all authorizations and/or consents by individuals or other parties required for Zendesk's use or disclosure of PHI contemplated by this BAA.
- 3.6 Permissible Requests by Subscriber. Subscriber shall not request Zendesk to access, use, or disclose PHI, nor to otherwise act, in any manner that would not be permissible under HIPAA or the HITECH Act if done by Subscriber. Without limiting the foregoing, Subscriber shall not use the Service to collect any PHI in violation of a restriction on the use or disclosure of PHI subject to 45 C.F.R. § 164.522, and shall not use the Service to collect any PHI if any use or disclosure of PHI permitted by this BAA would violate any other restriction on use or disclosure to which PHI is subject.
4. **Term and Termination.**
- 4.1 Term. This BAA shall become effective as of the later of (i) the date this Agreement is executed by Zendesk and Subscriber; and (ii) the date Subscriber's subscription to the Service commences as set forth on the Purchase Order ("**Effective Date**") and shall continue until terminated (the "**Term**").



4.2 **Termination.** This BAA shall terminate immediately upon termination of Subscriber's subscription to the Service or HIPAA Enabled Account(s) or Subscriber's downgrade to a Service Plan that is not a HIPAA Enabled Subscription Plan. In addition, this BAA may be terminated by either party as set forth in the Contract.

4.3 **Effect of Termination.** At termination or expiration of this BAA, Zendesk shall either destroy or return to Covered Entity all PHI in Zendesk's possession and/or in the possession of any subcontractor of Zendesk in accordance with Zendesk's procedures therefor, as in effect from time to time, and shall not retain any copies of such PHI; provided, however, that Zendesk and/or Zendesk's subcontractor may retain PHI as and to the extent necessary, and for so long as necessary for Zendesk or that subcontractor to continue its proper management and administration or to carry out its legal responsibilities. Moreover, in the event that return or destruction of PHI is not feasible, Zendesk shall extend the protections of this BAA to such PHI that is not returned or destroyed, and limit further uses and disclosures of such PHI to those purposes that make the return or destruction not feasible, for as long as Zendesk or the subcontractor maintains such PHI. Zendesk's obligations described in this Section 4.3 shall survive the termination or expiration of this BAA. Subscriber acknowledges that it is Subscriber's responsibility to export or backup any PHI that it wishes to retain before any termination is effected and Zendesk shall have no responsibility for any liability that may arise from any data loss caused as a result of that termination.

5. Amendments to Comply with Law.

Zendesk and Subscriber shall take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, and other applicable laws relating to the security or confidentiality of PHI. Upon the request of either party, the other party shall promptly enter into negotiations concerning the terms of an amendment to this BAA embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, or other applicable laws.

6. No Third-Party Beneficiaries.

Nothing express or implied in the Contract or this BAA is intended to confer, nor shall anything herein confer upon any person other than Subscriber, Zendesk and their respective successors or permitted assigns, any rights, remedies, obligations or liabilities whatsoever.

7 Intentionally Omitted.

8 Limitation of Liability. Pursuant to the Contract.

9 Notices.

All notices to be provided by Zendesk to Subscriber under this BAA may be delivered in writing by a nationally recognized overnight delivery service ("Courier") or US mail to the Subscriber at the mailing address provided below. All notices provided by Subscriber to Zendesk under this Agreement shall be delivered in writing by Courier or US Mail to the following address: Zendesk, Inc., Attn: General Counsel, 1019 Market St., San Francisco, CA 94103 USA. All notices shall be deemed to have been given immediately upon delivery by electronic mail during normal business hours, or if otherwise delivered upon receipt or, if earlier, two (2) business days after being deposited in the mail or with a Courier as permitted above.

10 General.

10.1 **Interpretation; Precedence.** The provisions of this BAA shall prevail over any provisions in the Contract that conflict or appear inconsistent with any provision in this BAA. This BAA and the



Contract shall be interpreted as broadly as necessary to implement and comply with HIPAA and the HITECH Act. Any ambiguity in this BAA shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HITECH Act. Except as specifically required to implement the purposes of this BAA, or to the extent inconsistent with this BAA, all other terms of the Contract shall remain in force and effect.

- 10.2 **Entire Agreement.** This BAA supersedes any and all prior and contemporaneous business associate agreements or addenda between the parties with respect to any Account(s) and constitutes the final and entire agreement between the parties hereto with respect to the subject matter hereof. Each party to this BAA acknowledges that no representations, inducements, promises, or agreements, oral or otherwise, with respect to the subject matter hereof, have been made by either party, or by anyone acting on behalf of either party, which are not embodied herein. No other agreement, statement or promise, with respect to the subject matter hereof, not contained in this BAA shall be valid or binding.
- 10.3 **Regulatory References.** A reference in this BAA to a section of regulations means the section as in effect or as amended, and for which compliance is required.
- 10.4 **Amendments.** This BAA may only be amended by mutual written agreement by the Parties.
- 10.5 **Governing Law and Jurisdiction.** Governing law and jurisdiction shall be as set forth in the Contract.
- 10.6 **Reserved.**
- 11 **Additional HIPAA Enabled Accounts.**

Subscriber may, from time to time, enter into additional Purchase Orders (each, a "Purchase Order") with Zendesk under which Zendesk supplies Subscriber with the Services for additional Agents or HIPAA Enabled Accounts ("Additional Order"). If a Purchase Order expressly states that this BAA applies to the Additional Order(s) under that Purchase Order, then this BAA will so apply, except that references to "Contract" in this BAA will be read as references to the applicable Purchase Order and Additional Order, respectively. Zendesk may, in its sole discretion, amend Exhibit A to this Agreement following the execution of such Additional Order to reflect any additional HIPAA Enabled Account to which this BAA applies.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed below by their duly authorized signatories.

Zendesk, Inc.

By: MARCUS BRATT
 Title: 7/29/15 / SVP
 Signature: [Signature] Date: 7/29/15

APPROVED
ZENDESK
LEGAL

State of Tennessee, Department of General Services, Central Procurement Office

By: Michael J. Remy
 Title: Chief Procurement Officer
 Signature: [Signature] Date: 7/30/15