

RFP C000979 Salesforce Implementation EA

NEW YORK STATE Office of Information Technology Services (ITS)

Attachment 5 - CONFIDENTIALITY & NON-DISCLOSURE AGREEMENT

THIS CONFIDENTIALITY & NON-DISCLOSURE AGREEMENT (hereinafter "Agreement") is hereby executed between the State of New York (hereinafter "State"), acting by and through the New York State Office of Information Technology Services (hereinafter "ITS"), having its principal place of business at State Capitol, ESP, P.O. Box 2062, Albany, New York 12220-0062, and _____, having a principal place of business at _____, _____, _____ (hereinafter "Vendor"), executed by _____, an individual who is Vendor's duly authorized representative (hereinafter "Authorized Representative").

Certification & Affirmation

The Authorized Representative, by signing this Agreement in the name and on behalf of the Vendor, subscribes and affirms the following:

1. that he/she is signing this Agreement on behalf of Vendor intending to bind said Vendor to the representations made herein.
2. that Vendor will comply with all requirements of this Agreement; and
3. that Vendor will certify the return or destruction of Confidential Information received as specified in this Agreement, if applicable.

Purpose

This Agreement is being entered into regarding services being provided by Vendor as described in ITS RFP No. C000979 ("RFP") and the contract(s) resulting from the RFP.

PART 1. DEFINITIONS

A. Confidential Information

Confidential Information shall be defined to include any information that ITS or the State, regardless of form or medium of disclosure (e.g., verbal, hard copy, or electronic) or source of information (e.g., ITS, other state agencies, state employees, electronic systems, or third-party contractors) provides to Vendor, or which Vendor obtains, discovers, derives or otherwise becomes aware of solely as a result of Vendor's performance of the other than:

- (a) information that is previously rightfully known to Vendor without restriction on disclosure.
- (b) information that is or becomes, from no act or failure to act on the part of Vendor, generally known in the relevant industry or in the public domain; and
- (c) information that is independently developed by Vendor without the use of Confidential Information.

Title to all Confidential Information remains the property of the State. Confidential Information is provided on an "as is" basis, and the State makes no warranties, guarantees or representations of any kind express or implied, or arising by custom or trade usage, as to any matter whatsoever, without limitation, and specifically makes no implied warranty of fitness for any particular purpose or use, including but not limited to adequacy, accuracy, completeness or conformity to any representation, description, sample or model.

B. Authorized Use

"Authorized Use" shall be defined as the use of Confidential Information by Vendor, its employees, consultants, and subcontractors, solely for the purpose of performing the services as agreed to, as now or

hereafter modified or amended. Disclosure, display, use, duplication, storage or transmittal of Confidential Information, in any form, for any purpose other than as agreed to, including extrapolation or retention of summary information, data or business processes, even if without specific identifiers, shall be deemed an “unauthorized use.”

C. Authorized Person

“Authorized Person” shall be defined as those persons within Vendor’s employ or control identified by Vendor to ITS as having a need to receive, possess, store, access, or view Confidential Information for an Authorized Use.

PART 2. CONFIDENTIALITY & NON-DISCLOSURE REQUIREMENTS

A. Duty to Protect Confidential Information

Upon proper execution of this Agreement, Vendor will be granted a non-exclusive, non-transferable license to display, use, duplicate, store, and disclose Confidential Information only for an Authorized Use. Vendor shall safeguard all Confidential Information which is delivered from the State to Vendor to ensure its authorized use and to protect and prevent its unauthorized use or disclosure.

“Safeguard all Confidential Information” shall be defined as Vendor taking either one, or a combination of the following security measures, whichever standard is higher:

- (1) Where Vendor has established security procedures for its own confidential, sensitive business information which impose security requirements for the protection of its own trade secret, proprietary or confidential information, Vendor shall protect the Confidential Information using the same means; and/or
- (2) Where Vendor has not established such internal procedures, Vendor shall take the commercial measures defined below, to protect the Confidential Information.

Commercial Measures to Protect Confidential Information

For purposes of this Agreement, “commercial measures” shall be defined to include all of the following responsibilities to be undertaken by Vendor:

I. Use Restriction

Confidential Information shall only be received, possessed, stored, accessed and/or viewed by Authorized Persons.

II. Access by Authorized Person(s)

- a. Vendor shall be responsible for identifying those persons within its employ or control (e.g., subcontractors, consultants) who have a need to receive, possess, store, access, or view Confidential Information for an authorized use (hereinafter “Authorized Person(s)”).
- b. Vendor shall be required to take commercially reasonable steps to inform each Authorized Person of their individual obligation to protect the security of Confidential Information in accordance with the requirements of this Agreement.
- c. Vendor shall not permit Confidential Information to be received, possessed, stored, accessed, or viewed by any Authorized Person until such person has agreed to comply with the required security obligations set forth below.

III. Access by Subcontractors and Consultants

- a. Vendor shall not permit Confidential Information to be received, possessed, stored, accessed, or viewed by any consultant or subcontractor until such entity’s legal representative has been made aware of and has agreed to comply with the required security obligations of this Agreement.
- b. Consultants and subcontractors shall not be allowed to further disseminate or distribute Confidential Information, other than to provide access by Authorized Person(s) within consultant’s or subcontractor’s control and oversight.

IV. Security Obligations Regarding Confidential Information

Any person(s) who receive, possess, store, access, or view Confidential Information from either Vendor or its approved Subcontractor or Consultant (hereinafter "Custodian") shall be subject to the following security obligations:

- a. Custodian is the SOLE entity authorized to duplicate, distribute, or otherwise transmit Confidential Information.
- b. Custodian's legal representative must approve any process used to duplicate, distribute, or otherwise transmit Confidential Information to Authorized Person(s), and may NOT approve or use any process which involves the use of any public internet or other non-secure medium.
- c. Unless otherwise authorized by Custodian's legal representative, Confidential Information may NOT be stored on personal (non-business) computing or other electronic devices or taken or removed in any form outside of the physical premises of Custodian.
- d. Confidential Information may only be duplicated, distributed, or otherwise transmitted "as is", without alteration of any kind. "Confidential" or "Copyright" notices, whether originally in physical or electronic medium, shall not be removed from and shall be duplicated on Confidential Information when such information is duplicated, distributed, or otherwise transmitted pursuant to (b) above.
- e. Other than as set forth in (a-d), above, Confidential Information may not be duplicated, distributed, stored or otherwise transmitted or communicated to or by any person or system. Authorized Person(s) may not copy, re-duplicate, re-transmit or re-distribute Confidential Information, in any form, whether whole or in part, or in any medium, whether electronic or hard copy.
- f. Upon termination of employment, Authorized Person(s) shall be required to return Confidential Information to Custodian's legal representative, and/or to certify that all electronic, optical or other copies have been destroyed within any electronic storage or other medium.

V. Chain of Custody

Vendor shall be required to keep a record of all copies of the Confidential Information that have been made and distributed to those persons within the employ of Vendor, and to those consultants or subcontractors who have a need to access Confidential Information for such authorized use.

Those consultants or subcontractors which receive Confidential Information from Vendor shall, as a condition of accessing such information, certify that such entity shall keep a record of all copies of the Confidential Information that have been made and distributed to those persons within the employ of such entity, and that such entity will provide its written certification of compliance with the provisions of this Agreement to the Vendor as provided in paragraph VI, below.

VI. Certification by Vendor of Return of Confidential Information

Vendor and its Consultants and Subcontractors who have received Confidential Information shall certify the chain of custody of such information as follows:

1. Of Vendor:

Upon termination of the engagement, Vendor shall independently certify, in writing, to the State, its compliance, during the period agreed to, with the terms of this Agreement. Vendor shall specifically certify:

- (i) the documented chain of custody naming all Authorized Person(s), consultants and subcontractors to whom the Confidential Information was duplicated, distributed or transmitted,

(ii) As to Authorized Person(s) within the internal employment or control of Vendor, that all

copies of Confidential Information have either been returned to the State or are certified by such person(s) as having been destroyed or permanently deleted from all forms of electronic storage, and Vendor shall attach the certifications of its consultants and subcontractors.

2. Of Vendor's Consultants and Subcontractors:

Upon termination of the engagement, such entity shall independently certify, in writing its compliance with the terms of this Agreement, and shall specifically certify:

(i) the documented chain of custody naming all Authorized Person(s) to whom the Confidential Information was duplicated, distributed, or transmitted, and

(ii) As to such Authorized Person(s) within the internal employment or control of such entity, that all copies of Confidential Information have either been returned to the State or are certified by such person(s) as having been destroyed or permanently deleted from all forms of electronic storage.

Termination

The license to use Confidential Information terminates automatically upon the happening of any of the following: (a) breach of this agreement or (b) completion of Vendor's services as agreed to.

Compliance

Should Vendor breach or threaten to breach this Agreement, the State shall have all equitable and legal rights (including the right to obtain injunctive relief) to prevent such breach and/or to be fully compensated (including reasonable attorney's fees) for losses or damages resulting from such breach. Vendor is deemed to acknowledge that compensation for damages may not be sufficient and that injunctive relief to prevent or limit any breach of confidentiality may be the only viable remedy to fully protect the Confidential Information.

Vendor affirms that its employees with access to Confidential Information will not disclose such Confidential Information to anyone, except as provided in this Agreement. In addition, Authorized Persons shall safeguard all Confidential Information from unauthorized access, loss, theft, destruction, and the like. Vendor shall notify ITS immediately upon becoming aware that Confidential information is in the possession of or has been disclosed to an unauthorized person or entity.

Governing Laws

This Agreement shall be governed by and construed in accordance with the laws of the State of New York. If any provision of Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, the other provisions shall remain in full force and effect.

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK

IN WITNESS WHEREOF, Vendor has caused this Non-Disclosure Agreement to be signed as of the date set forth below.

By: _____

Print Name: _____

Title: _____

Date: _____

STATE OF New York)

) SS:.

COUNTY OF)

On this _____ day of _____, 20____, before me personally came _____, to me known, and known to me to be the person who executed the above instrument, who, being duly sworn by me, did for her/himself depose and say that she/he is the _____ (title) of _____ (Vendor), with its principal place of business located at _____ and that she/he executed the foregoing instrument in the name of the Vendor, and that she/he executed the same as the act and deed of the Vendor for the uses and purposes mentioned therein.

Notary Public

Vendor, having a principal place of business at _____ (hereinafter _____), and having entered into a Confidential Non-Disclosure Agreement (NDA) with the NYS Office of Information Technology Services (ITS) on _____, and having been provided by ITS with Confidential Information in accordance with that NDA, now certifies on behalf of itself and all Authorized Persons provided Confidential Information as agreed to, as to the following:

Date _____

On this _____ day of _____, 20____, before me personally came _____, to me known, and known to me to be the person who executed the above instrument, who, being duly sworn by me, did for her/himself depose and say that she/he is the _____ (title) of _____ (Vendor), with its principal place of business located at _____, and that she/he executed the foregoing instrument in the name of the Vendor, and that she/he executed the same as the act and deed of the Vendor for the uses and purposes mentioned therein.

Notary Public