

**CONTRACT NO.: DMS 14/15-018
BETWEEN
FLORIDA DEPARTMENT OF MANAGEMENT SERVICES
AND
UNION SECURITY INSURANCE COMPANY (ASSURANT EMPLOYEE BENEFITS)**

AMENDMENT NO.: 3

This Amendment to Contract No.: DMS 14/15-018 (the "Contract") is by and between the State of Florida acting through the Department of Management Services (the "Department") and Union Security Insurance Company (Assurant Employee Benefits) (the "Service Provider" or "Vendor")(collectively the "Parties").

WHEREFORE, the Parties do hereby agree to amend the Contract as follows:

1. Extension Term. The Department does hereby extend the Contract until December 31, 2017. This Contract Extension will be in effect, with no plan or premium changes for or during the Contract Extension Term.
2. Amendment No. 2 of the Contract required the Parties to execute a contract amendment by April 1, 2017, in order to extend the Contract beyond June 30, 2017. The Parties have agreed to execute this Amendment No. 3 after the April 1, 2017, deadline and before the expiration of the Contract.
3. Subsection 5.2.1 of the Contract is replaced with the following:

5.2.1 General

Vendor will provide any and all labor, materials and supplies necessary to perform the Services in the manner prescribed by this Contract. Vendor will meet or exceed the Performance Guarantees set forth in Attachment B.

No compensation shall be paid by the Department to Vendor for the Services. Except as specifically set forth in this Contract, the Department will not reimburse Vendor for any travel expenses or other costs incurred in connection with the Contract or the Services. Vendor's sole remuneration shall be the premiums paid by the Subscribers.

Vendor agrees to comply with section 110.123(9), Florida Statutes, and section 501.171, Florida Statutes.

Vendor acknowledges that it is a covered entity as defined in 45 CFR § 160.103, and shall perform all duties required of a covered entity pursuant to HIPAA, the Privacy Rule, the Security Rule, and the HITECH Act. Vendor must cooperate with any investigations by the Secretary of the U.S. Department of Health and Human Services or his or her designee.

Vendor must create and retain all records required to be maintained by Vendor pursuant to HIPAA, the Privacy Rule, the Security Rule, and the HITECH Act for the time period required by applicable law and the Contract. Vendor agrees to comply with all applicable provisions of HIPAA standards for electronic transactions and code sets, also known as the Electronic Data Interchange ("EDI") Standards, in accordance with 45 CFR § 162 and the Annual Guidance as issued by the Secretary pursuant to the HITECH Act, section 13401 to the extent applicable

to such agent or subcontractor. Vendor shall require that every agent and subcontractor that conducts standard transactions on its behalf, agrees to comply with the EDI Standards and the Annual Guidance as issued by the Secretary pursuant to the HITECH Act, section 13401. Vendor shall require that its agents and subcontractors comply with all applicable provisions of 45 CFR § 164, subparts A, C, and E, and all applicable standards relating to Electronic PHI.

Vendor acknowledges that it is a covered entity as defined in section 501.171, Florida Statutes, and shall perform all applicable duties required of a covered entity therein.

As used in Subsection 5.2 and its subparts, the below capitalized terms are defined as follows:

“Access” means the ability and/or means to review, inspect, instruct, communicate with, store Data in, retrieve Data from, or otherwise make use of any Data, regardless of type, form, or nature of storage. Access to a computer system or network includes local and remote access.

“Data” or “State of Florida Data” means personal information regarding Subscribers and/or Eligible Dependents that is disclosed by the Department to Service Provider or created by Service Provider from personal information so disclosed and is considered (i) “Nonpublic Personal Information” as defined in Title V of the Gramm-Leach-Bliley Act of 1999, (ii) “Personal Information” as defined in Florida Statutes 501.171 or the law of the resident state of the Subscriber or Eligible Dependent, or (iii) “Protected Health Information” as defined in 45 C.F.R. § 160.103. Data may be in any form, including but not limited to, storage media, computer memory, in transit, presented on a display device, or in physical media such as paper, film, microfilm, or microfiche. Data includes the original form of the Data and all metadata associated with the Data.

“Breach” shall have the same meaning as specified in Florida Statutes 501.171 or any applicable state and federal breach notification law, including but not limited to 45 CFR § 164.402.

“Event” means any transmission of State of Florida Data to or from Vendor’s information system (except for internal transmissions of State of Florida Data between Vendor’s database and information systems) or any modification to State of Florida Data in an information system.

“Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information set forth in 45 CFR § 160 and 45 CFR § 164, subparts A and E, as amended.

“Protected Health Information” or “PHI” means individually identifiable health information as defined in 45 CFR § 160.103, whether secured or unsecured, and in any type or format.

“Security Rule” means the security provisions set forth in 45 CFR § 160 and 45 CFR § 164, subparts A and C, as amended.

4. The following is added after the second paragraph of Subsection 5.2.3 of the Contract:

Except as provided in subsection 5.2.5, Vendor will not utilize any Subcontractor Services that are performed, in whole or in part, outside the United States.

The use of any Subcontractor or Subcontractor Services in a manner that is not permitted by this subsection is a breach of this subsection and constitutes an Event of Default.

5. Subsection 5.2.4 of the Contract is replaced with the following:

5.2.4 Warranty of Security

A. Background Screening

In addition to any background screening required by Vendor as a condition of employment, Vendor warrants that it will conduct a criminal background screening of, or ensure that such a screening is conducted for, each of its employees, Subcontractor personnel, independent contractors, leased employees, volunteers, licensees or other person, hereinafter referred to as "Person" or "Persons," operating under their direction who directly perform Services under the Contract, whether or not the Person has access to State of Florida Data, as well as those who have Access, including indirect Access, to State of Florida Data, whether or not they perform Services under the Contract. Vendor warrants that all Persons will have passed the background screening described herein before they have Access to Data or begin performing Services under the Contract. The look-back period for such background screenings shall be for a minimum of six (6) years where six (6) years of historical information is available.

The minimum background check process will include a check of the following databases through a law enforcement agency or a Professional Background Screener accredited by the National Association of Professional Background Screeners or a comparable standard:

- Social Security Number Trace or trace of a comparable identifier if outside of the United States; and
- Criminal Records (Federal, State, and County criminal, felony, misdemeanor or their equivalent in Canadian jurisdictions, e.g., indictable offense, and summary offense) for all relevant jurisdictions which make such data available, including Canadian jurisdictions for any Canadian employees, as applicable).

Vendor agrees that each Person will be screened as a prior condition for performing Services or having Access to State of Florida Data. Vendor is responsible for any and all costs and expenses in obtaining and maintaining the criminal background screening information for each Person described above. Vendor will maintain documentation of the screening. Vendor will abide by all applicable laws, rules and regulations including, but not limited to the United States' Fair Credit Reporting Act and/or any equal opportunity laws, rules, regulations or ordinances.

1. Disqualifying Offenses

If at any time it is determined that a Person has a criminal misdemeanor or felony record regardless of adjudication (e.g., adjudication withheld, a plea of guilty or nolo contendere, or a guilty verdict) within the last six (6) years from the date of the court's determination for the crimes listed below, or their equivalent in any jurisdiction, Vendor is required to immediately remove that Person from any position with Access to State of Florida Data or directly performing Services under the Contract; however, Vendor may allow the Person to Access State of Florida Data after completing the Individualized Assessment described below. The Disqualifying Offenses are:

- Computer related or information technology crimes
- Fraudulent practices, false pretenses and frauds, and credit card crimes
- Forgery and counterfeiting
- Violations involving checks and drafts

- Misuse of medical or personnel records
- Felony theft

If Vendor has knowledge of a Disqualifying Offense for a Person within the last six (6) years from the date of the court's disposition, it may obtain information regarding the incident and determine whether that Person should continue providing services under the Contract or have Access to State of Florida Data. Vendor will consider the following factors only in making the determination: i.) nature and gravity of the offense, ii.) the amount of time that lapsed since the offense, iii.) the rehabilitation efforts of the Person and iv.) relevancy of the offense to the job duties of the Person (collectively, "Individualized Assessment"). If Vendor determines that the Person should be allowed Access to State of Florida Data, then Vendor shall maintain all criminal background screening information and the rationale for such Access.

2. Refresh Screening

Vendor will ensure that all background screening will be refreshed every five (5) years from the time initially performed for each Person during the Term of the Contract.

3. Annual Certification

Vendor is required to submit an annual certification demonstrating compliance with the Warranty of Security to the Department by December 31st of each Contract year.

B. Duty to Provide Secure Data

Vendor will use reasonable administrative, technical, and physical safeguards to maintain the security of State of Florida Data including, but not limited to, physically secured areas, computer access controls, and encryption of all Data that is transmitted over public networks not owned or managed by Vendor or stored within Vendor databases. Vendor will also comply with all applicable requirements under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and any other applicable state and federal laws, rules, and regulations, as well as all laws, rules, and regulations applicable in the jurisdictions in which Data is stored, regarding security of information. Data cannot be disclosed to any person or entity that is not included on the list of Persons with Access to Data (as described in subsection 5.2.4.D below), except Vendor may disclose Data as required by law, judicial, or administrative process.

C. Department's Ability to Audit Screening Compliance and Inspect Locations

Upon five (5) days prior written notice to Vendor during the Term of the Contract, the Department reserves the right to audit the method by which Vendor conducts its background screening and Individualized Assessment of Persons and all information relating thereto, subject to the restrictions set forth in Section 5.2.4 D below. Upon ten (10) days written notice, the Department will have the right to inspect Vendor's working area, computer systems, and/or location to ensure that access to the State of Florida Data is secure and in compliance with the Contract and all applicable state and federal rules and regulations. The Department's right to inspect under this subsection does not include physical access to the raised floor area of the Data Center, but will, if deemed necessary by the Department, include visual inspection through in-person or live camera viewing.

D. Record Retention

Vendor shall retain a list of all Persons with Access to Data, including a statement confirming that each Person has passed the background screening required herein. Such a statement shall not include the substance of the screening results, only that the Person

has passed the screening. Vendor shall maintain a written policy for the protection of Data, including a policy and procedure for Access to Data.

Vendor certifies and confirms it has reviewed the National Institute of Standards and Technology (NIST) publication Framework for Improving Critical Infrastructure and Cybersecurity and NIST.SP.800-53r4, completed a detailed review of its security program, mapped each function to the NIST Common Security Framework, determined its target profile suitable for its business and applicable risk, and maintains a security program to support the target profile. The Department acknowledges and understands that Vendor's security program and target profile is proprietary and confidential to Vendor, and that Vendor will not disclose any details to the Department related to its NIST review and target profile.

Vendor's information system shall generate audit records containing information that establishes what type of Event occurred, the date and time the Event occurred, where the Event occurred, the source of the Event, the outcome of the Event, and the identity of any Persons associated with the Event.

Vendor must maintain all background screening information, including the identification of the entity that performed the background screening for each Person; criminal history results; the list of all Persons with Access to Data; the statement confirming that each Person has passed the background screening; and records relating to the Individualized Assessment of a Person, including the identification of each person whose access is removed due to a disqualifying offense, the disqualifying offense, any investigation thereof, the Individualized Assessment, and the rationale, if any, for subsequently allowing the Person to Access Data, if applicable. The written policy and information required in this subsection 5.2.4 shall be included in the Department's audit and screening abilities as defined in subsection 5.2.4.C, except that Vendor shall not be required to produce or allow the Department to access any of Vendor's trade secret information as defined in section 812.081, Florida Statutes, or any information which is confidential or exempt from disclosure pursuant to Florida law, U.S. federal law, or Canadian law. The written policy and information required in this subsection 5.2.4 shall also be subject to immediate disclosure upon written or oral demand at any time by the Department or its designated agents or auditors.

Vendor shall retain the written policy and information required in this subsection 5.2.4 as follows: 1) audit records of Vendor's computer information system shall be maintained by Vendor for a period of no less than six (6) years from the date of the Event, and 2) all other records required by subsection 5.2.4. shall be maintained by Vendor for six (6) years from the completion of each unique plan year. For example, for plan year 2017, Vendor shall maintain the background check information and policy until December 31, 2023. This requirement shall survive the termination of this Contract and any Contract extensions.

Failure to compile and retain the written policy as required in subsection 5.2.4.D, background screening information as required in subsection 5.2.4, and audit records as required in subsection 5.2.4 shall be considered an Event of Default not subject to cure. Failure to provide access to the written policy as required in subsection 5.2.4.D, background screening information as required in subsection 5.2.4, and audit records as required in subsection 5.2.4 shall be considered an Event of Default subject to cure within three (3) business days.

E. Breach of State of Florida Data

1. Responsibility to Notify the Department

Within three (3) business days of a determination by Vendor's Compliance Department that a Breach of State of Florida Data has occurred, Vendor shall notify (via a telephone call to be followed up in writing with an email) the Department's Contract Manager, unless Vendor is prohibited from issuing such notification as a result of state law. Where Vendor is prohibited from issuing such notification, Vendor shall notify the Department's Contract Manager no later than three (3) business days after the expiration of the prohibition. In its written notice, Vendor shall provide the Department with the following information: (a) the date or estimated date of the Breach, (b) a brief description of the Data that is subject to the Breach, (c) a brief description of the circumstances surrounding the Breach, (d) Vendor's determination of the cause of Breach (if known), and (e) the corrective action Vendor took or will take to prevent further Breach of Data. This notification process shall apply to the Breach of any State of Florida Data maintained, Accessed, or transmitted by Vendor or its Subcontractor.

Vendor's failure to perform the obligations in this subsection 5.2.4.E. shall also be an Event of Default, subject to cure upon written notice from the Department as provided in Section 9.1, and will entitle the Department to recover any other damages it incurs arising from a failure to perform the obligations in this subsection (including any actual out-of-pocket expenses incurred by the Department to investigate and remediate the violation) and/or to pursue injunctive relief.

2. Vendor's Responsibility to Notify Participants

Vendor shall pay all costs to notify all persons affected by a Breach of Data, as required by section 501.171, Florida Statutes. Vendor shall pay all costs to notify all persons affected by a Breach of Data, as required by HIPAA.

If Vendor cannot identify the specific persons whose Data may have been accessed, such notice shall be provided to all persons whose Data reasonably may have been accessed. Vendor shall pay all costs to notify such persons unless the Breach was caused by the Department or the Department's contractors or agents. Nothing in this subsection will alter or replace the application of section 501.171, Florida Statutes, as to the Vendor's obligations and liability for Breaches concerning confidential personal information.

Vendor shall pay all costs associated with mitigating any potential damage or harm of a Breach of State of Florida Data, including establishing a toll free telephone line, e-mail link, or fully functioning web page to respond to any person's concerns about security and any Breach.

3. Credit Monitoring and Notifications

Vendor acknowledges that it is a covered entity as defined in section 501.171, Florida Statutes, and shall perform all duties required of a covered entity therein.

In addition to the requirements of section 501.171, Florida Statutes, in the event of any Breach of Data, Vendor shall provide credit monitoring at its own cost to any person affected by a Breach for no less than a two year period of time following the Breach.

4. Data Security Notification Letter

In addition to the foregoing notification requirements, Vendor shall provide to the Department annually on Vendor's letterhead and signed by a corporate officer of Vendor, a Data Security Notification Letter providing documentation and notification of any Breach of security involving State of Florida Data or any Subcontractor or Vendor facility housing State of Florida Data. In the event that no Breach has occurred, Vendor shall provide written confirmation of such.

5. Late Notice

If timely notice is not provided as prescribed in subsections 5.2.4.E.1. and 5.2.4.E.2. of this Contract, then the Department shall be entitled to a payment equal to \$1,000 per day for the first 30 days, \$50,000 for each subsequent thirty (30) day period not to exceed \$500,000 per Breach, from the date the Vendor should have provided notice, in order to cover, among other things, the Department's internal staffing and administrative costs, as well as the diminished value of Services provided under this Contract.

F. Indemnification

Vendor agrees to defend, indemnify and hold harmless the Department, the State of Florida, its officers, directors and employees for any claims, suits or proceedings related to a breach of section 5.2 and its subparts.

6. Subsection 5.2.5 of the Contract is replaced with the following:

5.2.5 Work Locations; Off-shoring of Data

Except as specified in this subsection, Vendor and its Subcontractors and agents (i) will not perform any of the Services from outside of the United States, and (ii) will not allow any State of Florida Data to be sent by any medium, transmitted, or Accessed outside of the United States, (collectively "off-shoring").

Vendor is only permitted to store State of Florida Data outside the United States at the following locations: (i) the Waterloo, Ontario, Canada Data Centre facility that, at the time of the execution of Contract Amendment No. 3, is located in [REDACTED] ("Waterloo Facility") and (ii) the Brampton, Ontario, Canada site which, at the time of the execution of this Contract Amendment No. 3, is utilized for business continuity and disaster recovery purposes only and is located at [REDACTED] ("Brampton Facility"), (collectively, "Authorized Canadian Locations"). Department understands that Vendor considers that the physical addresses of the Authorized Canadian Locations constitute confidential, proprietary, and trade secret information of Vendor and subject to the protections of Florida Statutes 688.001 et seq. and 812.081 et seq. As such, the Department warrants and represents that it will (i) take at least the same precautions to protect such information as it would its own confidential information; (ii) use such information only in performing its duties under the Agreement; (iii) redact such information from all versions of this Amendment and the Agreement that are publicly available or viewable; (iv) limit disclosure of such information to only those Department personnel with a specific need to know such information; and (v) not disclose such information in any form to any third party. Vendor will follow the following process when receiving Data from the Department:

- (1) Data will be transmitted using a secure file transfer protocol (sFTP) between the source, the Department's vendor (People's First), and the Vendor's U.S. data center in Wellesley, Massachusetts ("Wellesley Facility");
- (2) The Wellesley Facility will act as an entry point into Vendor's network (Sterling File Gateway);
- (3) Utilizing Network Address Translation ("NAT"), the U.S. Vendor's destination IP address for the secure file transfer will be mapped to Vendor's Sterling File Gateway sFTP application servers at the Waterloo Facility;
- (4) The files in transit will remain encrypted and in transit until they reach the Vendor's Sterling File Gateway secure environment where they will be decrypted and sent to Vendor's application servers.

Vendor agrees to protect, defend, indemnify, and hold harmless the Department for any and all third party claims and litigation, including attorney's fees and costs, arising from or in any way relating to, Vendor's assertion that the physical addresses of the Authorized Canadian Locations are trade secrets or otherwise exempt from public disclosure under chapter 119, Florida Statutes.

At the time of the execution of Contract Amendment No. 3, the Authorized Canadian Locations maintain a Tier III Certification of Constructed Facility and a Tier III Certification of Design Documents from the Uptime Institute. Vendor must notify the Department within three (3) days of any change to any of the aforementioned certifications. Upon any change to any of the aforementioned certifications, the Department, in its sole discretion, will elect whether to continue or discontinue the storage of State of Florida Data at the Authorized Canadian Locations. In the event the Department elects to discontinue storage of State of Florida Data at the Authorized Canadian Locations, and Vendor does not provide an alternative data storage facility within the United States, the Department reserves the right to terminate the Contract at its sole discretion and shall be entitled to any damages incurred as a result of such termination.

If the location of the State of Florida Data stored at the Authorized Canadian Locations is expected to change, Vendor must notify the Department ninety (90) days prior to the change in location. The Department, at its sole discretion, will approve or reject the storage of State of Florida Data at the proposed facility location. In the event the Department rejects the storage of State of Florida Data at the proposed facility location, and Vendor does not provide an alternative data storage facility within the United States, the Department reserves the right to terminate the Contract at its sole discretion and shall be entitled to any damages incurred as a result of such termination. The Department must approve the change of location in writing prior to any State of Florida Data being transmitted to, stored at, or accessed by any person at the new location.

Vendor's representation that it will only off-shore State of Florida Data to the Authorized Canadian Locations or another facility approved by the Department is a material element of this Contract. The Department relies on this representation in its determination that Vendor is an appropriate entity with which to contract for the Services set forth in this Contract.

The off-shoring of any State of Florida Data or the use of any off-shore facility that is not approved by the Department introduces potential liabilities and security concerns that represent an immediate and irreparable harm to the Department in light of the high value the Department places on the security of State of Florida Data.

The off-shoring of any State of Florida Data in a manner that is not permitted by this section is a breach of this section and constitutes an Event of Default. Further, any Breach of State of Florida Data stored at or transmitted to any facility outside of the United States is a breach of this section and constitutes an Event of Default.

Vendor agrees that any violation of this subsection or any Data Breach that occurs as a result of the above-permitted off-shoring activities will result in immediate and irreparable harm to the Department, and that the resulting damages to the Department from a breach of this section are by their nature impossible to ascertain presently and will be difficult to ascertain in the future. The issues involved in determining such damages will be numerous, complex, and unreasonably burdensome to prove. The Parties acknowledge that these financial consequences are liquidated damages, exclusive of any other right to damages, not intended to be a penalty and solely intended to compensate for unknown and unascertainable damages. Vendor therefore agrees to pay to the Department liquidated damages of \$50,000 per breach of section 5.2.5 in order to cover, among other things, the Department's internal staffing, administrative costs, and litigation-related expenses, as well as the diminished value of Services provided under the Contract. These remedies are in addition to and cumulative of any remedy for breach set forth in subsections 5.2.4.E. and 5.2.4.F.

7. The following is added as Subsection 5.2.11:

5.2.11 Return or destruction of PHI upon termination

A. Destruction of Return of PHI to Department

Upon notice of termination of this Contract, Vendor shall destroy or return to the Department any and all PHI created or received by Vendor relating to the Services except to the extent that Vendor is required by law to maintain such information in its capacity as a health plan or covered entity.

Within fifteen (15) calendar days of any notice of termination of the Contract, Vendor shall notify the Department in writing as to whether Vendor elects to return or destroy such PHI, except as set forth to the contrary pursuant to paragraph B of subsection 5.2.11.

Except as provided in paragraph B of subsection 5.2.11, within thirty (30) calendar days of the notice of termination Contract, Vendor shall return to the Department or destroy any and all PHI maintained by Vendor in any form and shall retain no copies thereof. Vendor also shall recover and return or destroy, within such time period, any and all PHI in the possession of its subcontractors or agents, except as set forth to the contrary pursuant to paragraph B of subsection 5.2.11.

If Vendor elects to destroy PHI, Vendor shall obtain written confirmation from the Department that such actions will not violate the State of Florida's record retention policies. Upon destruction, Vendor shall provide written certification to the Department that such PHI has been destroyed. If any subcontractor or agent of Vendor elects to destroy PHI, Vendor will require such subcontractor or agent to provide written certification to Vendor and to the Department when such PHI has been destroyed.

B. Return or destruction of PHI not feasible

If it is not feasible for Vendor to return or destroy any PHI, Vendor shall notify the Department in writing that Vendor has determined that it is not feasible or permissible to return or destroy the PHI and the specific reasons for such determination.

If it is not feasible for Vendor to obtain any PHI in the possession of the subcontractor or

agent, Vendor shall provide a written explanation to the Department and require the subcontractor or agent to agree to extend any and all protections, limitations, and restrictions set forth in this Contract to the subcontractor or agent's use or disclosure of any PHI retained after the termination of this Contract, and to limit any further use or disclosure to the purposes that make the return or destruction of the PHI not feasible.

8. The following is added to the end of subsection 11.5 of the Contract: "The parties hereby agree that the 2nd Judicial Circuit in and for Leon County, Florida has personal jurisdiction and subject matter jurisdiction over claims brought pursuant to this Contract."
9. The following is added as the second paragraph to section 11.22 of the Contract:

Solely for the purposes of this section, the Department's Contract Manager is the agency custodian of public records. If, under this Contract, Vendor is providing services and is acting on behalf of a public agency, as provided by section 119.0701, Florida Statutes, Vendor shall:

- (a) Keep and maintain public records required by the public agency to perform the service;
- (b) Upon request from the public agency's custodian of public records, provide the public agency with a copy of the requested records or allow the records to be inspected or copied within reasonable time and at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes, or as otherwise provided by law;
- (c) Ensure that public records that are exempt or confidential and exempt from public records disclosure are not disclosed except as authorized by law and the Department for the duration of the Contract term and following the completion of the Contract if the Vendor does not transfer the records to the public agency; and
- (d) Upon completion of the Contract, transfer, at no cost, to the public agency all public records in possession of Vendor or keep and maintain public records required by the public agency to perform the service. If Vendor transfers all public records to the public agency upon completion of the Contract, the Vendor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements.

If Vendor keeps and maintains public records upon completion of the Contract, Vendor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the public agency, upon request from the public agency's custodian of public records, in a format that is compatible with the information technology systems of the public agency.

- (e) **IF VENDOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO VENDOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT THE TELEPHONE NUMBER, EMAIL ADDRESS AND MAILING ADDRESS PROVIDED FOR THE CONTRACT MANAGER.**

10. The following is added as section 11.32 of the Contract:

11.32. Cooperation with the Inspector General

Pursuant to section 20.055(5), Florida Statutes, Vendor and any Subcontractors understand and will comply with their duty to cooperate with the inspector general in any investigation, audit, inspection, review, or hearing.

11. Subsection 19(b)c.iv. of Attachment A of the Contract is replaced with the following:

iv. Off-shoring Report. Vendor shall provide the Department with an affidavit from an authorized representative that Vendor and its Subcontractors and agents are not utilizing or performing Services for this Contract outside the United States other than the storage of Data (as defined in Subsection 5.2.1 of this Contract) at the Authorized Canadian Locations. Vendor shall also include in this affidavit a list of all Services performed outside of the United States and its Subcontractors who perform Services outside of the United States.

12. The following is added as Subsection 19(b)c.v. of Attachment A of the Contract:

v. Breach of Data report. The Vendor shall attest annually that the Vendor has notified the Department of any Breach (as defined in Subsection 5.2.1 of this Contract) of Data (as defined in Subsection 5.2.1 of this Contract) that has occurred.

13. This Amendment sets forth the entire understanding between the Parties with regard to the subject matter hereof.

14. This Amendment is effective on the last date of execution.

SIGNATURE PAGE IMMEDIATELY FOLLOWS

SO AGREED by the Parties' authorized representatives on the dates noted below:

FLORIDA DEPARTMENT OF MANAGEMENT SERVICES



David Zeckman, Chief of Staff

June 30, 2017

Date

**UNION SECURITY INSURANCE COMPANY
(ASSURANT EMPLOYEE BENEFITS)**



Signature


Stacia Almqvist, Authorized Signor

Print Name and Title

6/29/17

Date

**UNION SECURITY INSURANCE COMPANY
(ASSURANT EMPLOYEE BENEFITS)**



Signature

Dianna Duvall Vice President + Authorized Signor

Print Name and Title

6/29/2017

Date