

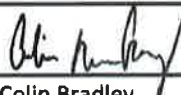
STATEMENT OF WORK

Structure of Agreement

This Statement of Work ("SOW") is entered into pursuant to the Master Services Agreement ("MSA") identified below between Winston Financial Services, Inc. and the customer identified below and is incorporated by reference into the MSA, and this SOW and the MSA together comprise the complete agreement between the parties ("Agreement") regarding those products and services defined within this SOW. If there is a conflict between the terms of this MSA and this SOW, the terms of the SOW shall prevail, and any capitalized terms not defined in this SOW shall have the meanings ascribed to them in the MSA.

Signatures

Intending to be legally bound and having reviewed this SOW in its entirety, Winston Financial Services and Customer have caused this SOW to be executed by their authorized representatives effective as of the date set forth below.

	Winston Financial Services, Inc.	Williamson County
AUTHORIZED SIGNATURE:		
PRINTED NAME:	Colin Bradley	Dan A. Gattis
TITLE:	VP, Business Development	County Judge
COMPANY NAME	Winston Financial Services, Inc.	Williamson County
ADDRESS &:	2399 Highway 34, Unit C-2 Manasquan, NJ 08736	710 S. Main Street Georgetown, TX 78627
EFFECTIVE DATE OF SOW:	January 5, 2016	
INITIAL TERM:	36 Months January 5, 2016 through January 4, 2019	
EFFECTIVE DATE OF MSA:	January 5, 2016	

1. Services

Winston Financial Services, Inc. (herein "Winston" or "WFS") will provide Williamson County (herein referred to as "Customer") in the remainder of this document, with the Benefit Communication, Enrollment, Benefits Administration Technology ("BenefitInsite") and Outsourced Administration Services identified on Schedule A ("Services").

2. Term and Termination

Term. This SOW shall become effective on the Effective Date of SOW above, January 05, 2016 and shall continue in effect for thirty six (36) months ending on January 4, 2019

Termination For Cause. Either party shall have the right to terminate this SOW with written sixty (60) day notice, in the event of a material breach by the other party, unless such breach is cured within 30 days of receipt of written notice of such breach. The obligations of the parties under this SOW that by their nature would continue beyond expiration, termination or cancellation of this SOW shall survive any such expiration, termination or cancellation.

Termination for Convenience: This agreement may be terminated at any time at the option of either party, without future or prospective liability for performance upon giving one hundred twenty (120) days written notice thereof. In the event of termination, The County will only be liable for its pro rata share of services rendered and goods actually received.

3. Service Fees and Appointments

In consideration for the Services rendered by Winston under this SOW, Customer shall pay the fees and expenses or make appointments as set forth on Schedule C subject to the terms and conditions of the MSA.

Payment for goods and services shall be governed by Chapter 2251 of the Texas Government Code. An invoice shall be deemed overdue the 31st day after the later of (1) the date The County receives the goods under the contract; (2) the date the performance of the service under the contract is completed; or (3) the date the Williamson County Auditor receives an invoice for the goods or services. Interest charges for any overdue payments shall be paid by The County in accordance with Texas Government Code Section 2251.025. More specifically, the rate of interest that shall accrue on a late payment is the rate in effect on September 1 of The County's fiscal year in which the payment becomes due. The said rate in effect on September 1 shall be equal to the sum of one percent (1%); and (2) the prime rate published in the Wall Street Journal on the first day of July of the preceding fiscal year that does not fall on a Saturday or Sunday.

Schedule A SERVICES

1. Case Setup Services

Winston will provide Customer with the appropriate resources to conduct all necessary Case Setup activities. These activities will include but not be limited to:

- a) Coordination with appropriate Customer contacts and vendors to setup a detailed communication and enrollment strategy for pending enrollments
- b) Review and discovery of current processes and workflows
- c) Coordination with Customer to receive and analyze the "Customer Discovery Templates"
- d) Communication and coordination with Customer contacts of expected enrollment conditions, time frames and access related issues

In order to construct an orderly and prosperous enrollment environment, Winston will request a completed copy of the "Customer Discovery Template" twelve (12) weeks prior to the start of the enrollment. These sheets should contain at least the following information:

- a) Important Customer Contacts, Phone Numbers and Addresses
- b) Summary of "in-force" benefits programs including voluntary benefit programs
- c) Development and Testing of file interfaces
- d) Plan documents & summaries, ongoing admin rules for life events & new hires, all eligibility classes

Whenever necessary, Winston will be able to accommodate shortened timeframes (less than eight (8) weeks' notice) for case setup and enrollment functions.

2. Benefits Administration and Enrollment System

Provide all features and functions of Winston's Benefits Administration and Enrollment system, hereafter "BenefitInsite," delivered and made accessible through a web browser with Internet connectivity. The application will be accessible through various browser software including, but not limited to Mozilla Firefox 4.0 or greater and Internet Explorer 7.0 or greater, Google Chrome and Apple Safari. The application is provided on Software as a Service (SaaS) and is jointly hosted by Winston and its Managed Hosting Vendor, currently Rackspace LLC.

- a) Employee Application Access. Access to the application will be limited to employees of Customer as identified on the Customer's eligibility files.

- b) **Enrollment and Transactional Support.** Winston will, through the BenefitInsite application, enable eligible employees of the Customer to enroll in and/or modify certain employee benefit programs identified by the Customer as being available to employees and their eligible dependents. This application will support rules based eligibility management including the segmentation of data and enrollment options based on Customer benefit plan rules. Winston will provide this application and perform this service throughout the calendar year and Customer benefit plan year, currently running from January 1st through December 31st for the purpose of supporting the following transactions:
- i. Benefits Enrollment during Annual Open Enrollment
 - ii. Benefits Enrollment for Newly Hired Employees
 - iii. Initiation of Qualified Life Events by Employees
 - iv. Designation and/or updating of Beneficiary Information for applicable plans
- c) **Beneficiary Management.** Winston will allow Benefit Plan Participants to change beneficiary and dependent information via the Web Application. Winston will be the primary holder of beneficiary information for Life and Disability plans should a claim arise. Customer will be responsible to ensure the electronic storage of beneficiary information is allowable by their chosen vendors.
- d) **Administrative Access and Rights.** Winston will allow Customer-designated Human Resources Professionals to have Administrative Rights to the benefits administration system. Administrative Rights provides access to the following features within the application:
- i. To access and view Participant benefit records, transaction history and customer service records
 - ii. To access and view participant documents, confirmation statements and other documents attached to the participant record
 - iii. To add/edit notes attached to the participant record
 - iv. To manage pending transactions based on Customer benefit plan rules
 - v. To execute approved transactions on behalf of participants using the "impersonate" or manager self-service functionality.
- e) **Customer/Winston Interface.**
- i. As part of managing eligibility and processing Plan enrollments, Winston will require a regular file of Participant census data including demographic information from Customer. Customer will produce these files no less than two times (2X) monthly in mutually agreed upon format and remit them to Winston in the agreed-upon secure file transfer protocol between Customer and Winston.
 - ii. Customer is aware that any deviation from agreed upon census file schedule may impact the delivery of its instruction file described in following paragraph.
 - iii. Winston will transmit to Customer via agreed upon secure file transfer protocol a benefit enrollment instruction file, indicating required deductions for Programs, the elected Plan and Plan or Program tier (if required) and any changes to demographic data allowed by Customer on no less than a two times (2X) monthly basis, following the receipt and processing of the above mentioned census file. Customer acknowledges that any Internet encryption technology employed in connection with the transmission of data contemplated under this Agreement is not invulnerable. Notwithstanding any provision of this Agreement, Winston assumes no liability under this Agreement to Customer or any third party as a result of a violation or failure, for any reason, of any such encryption unless due to the gross negligence or willful misconduct of Winston.
- f) **Third Party Administrator/Carrier Eligibility/Enrollment Files**
- i. Customer requires that Winston build, manage and maintain secure, electronic connectivity to benefit vendors as identified by the Customer for the purposes of communicating employee and dependent enrollment data and eligibility.
 - ii. Winston will coordinate with Customer designated benefit vendors to develop the necessary file interface requirements including file layout, delivery protocols and calendars for sending of Enrollment, Eligibility and Coverage data.
 - iii. Winston will assume all costs associated with developing, testing and administering electronic interface files to approved benefit vendors. If either the Customer or benefit vendor request changes to the file layout and/or interface protocol, Winston will make reasonable and customary changes to the files and protocols as necessary at no additional cost to the Customer. Except in circumstances where the vendor does not use either industry accepted interface protocols (i.e ANSI 834, XML, CSV) nor accept electronic files requiring a custom interface for which, WINSTON reserves the right to identify and discuss with Customer additional costs for which the Customer may be responsible.
 - iv. Winston will perform quality testing, and upon approval, initiate live production files.

- v. Ongoing Electronic eligibility and data exchange (availability dependent upon vendor). It will be the responsibility of WINSTON to receive and review feedback and error reports following a file processing. If there are data errors caused by the benefit vendor, the benefit vendor must correct accordingly. Any data errors caused by the Customer must be resolved collectively by the Customer and Winston. Errors causing premium miscalculations, underpayments or overpayments will be addressed individually as to the financial obligation of the WINSTON and/or Customer.
- vi. Winston will conduct a semi-annual audit of the enrollment and eligibility data exchanged between WINSTON and the benefit vendors to ensure data synchronization. These will be conducted at no expense to the Customer.
- vii. For any benefit vendor that is unable to send or receive an electronic data file Winston will provide secure, readable electronic files (ie excel, csv, fill able PDF) to those vendors for manual inputting by those vendors. Winston will notify Customer of vendors unable to receive secure, electronic eligibility files.

3. Federal Forms Generation, Filing

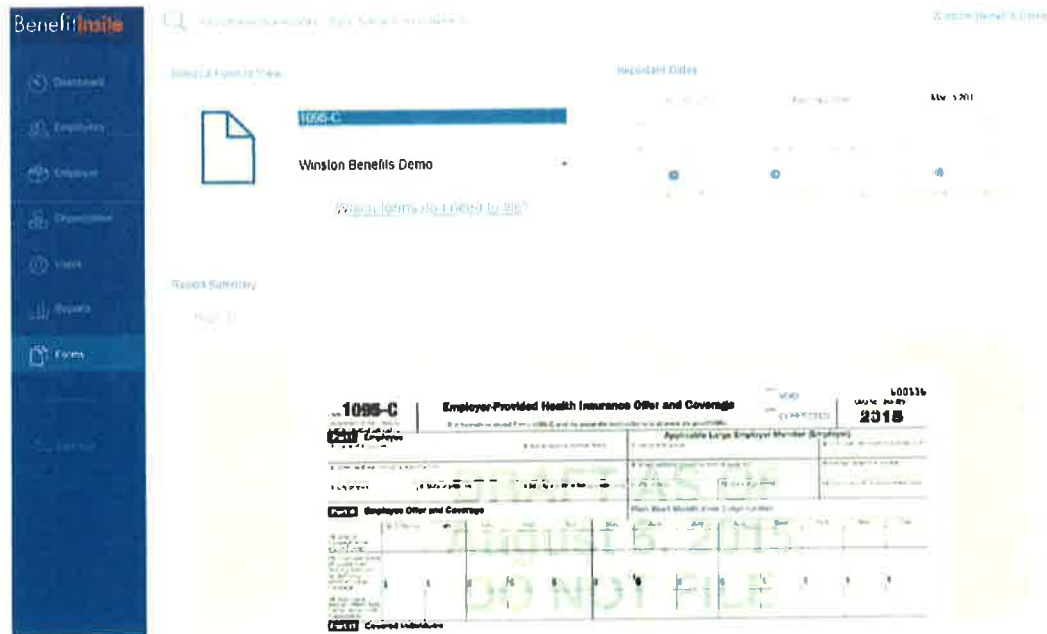
Winston will provide Customer and their applicable employees with reporting related to Form 1094 and 1095 for Applicable Large Employers. Reporting will consist of information gathered by the Customer Census Data, enrollment data from our own application ("BenefitInsite") and additional data points collected from the Customer.

- a) **Administrative Rights and Access.** Winston will allow Customer-designated Human Resources Professionals to have Administrative Rights to the application. Administrative Rights provides access to the following features within the application:
 - a) Access Employee records and related applicable IRS Forms
 - b) Edit Employee records and related applicable IRS Forms
 - c) To view Dashboards and Reporting which includes the following features;

a) 1094-C – Employer Reporting – Electronic Filing of Employer Form



b) 1095-C Employee Form – Electronic Generation and Storage of the Form 1095-C form.



4. Dependent Verification and Auditing Procedures

- a) **For All Benefit Transactions.** Employees completing a Qualified Life Event Enrollment transaction will be required to independently verify, through an online acknowledgement when performing the transaction on a self-service basis that the dependents they are enrolling in coverage meet the definition of the Customer's dependent relationship definitions.

Customer has instructed that the enrollment transactions require substantiation proving such event occurred:

Transactions to Audited	Plans to be Audited
1. Marriage/Legal Separation 2. Domestic Partnership (if applicable) 3. Birth/Adoption 4. Death 5. Spouse Loss of Coverage 6. Dependent Age Out 7. Change In Employment Status of Self or Spouse 8. Loss/Gain in Coverage	1. Medical/Rx 2. Dental

- b) **System Processing of Dependents.** Transactions which require verification will be held in a pending state until the employee acknowledges through the approved upon procedure, the relationship with the dependent. In the event the documentation is not received within the required period, the enrollment transaction will be deleted.

All enrollments that are started but incomplete will remain in such status until Winston deletes. A waiting period, to be determined in conjunction with the Customer, will be provided to Participants to complete their enrollment prior to deletion.

- c) **Document Retention Policy.** Winston in its role as the benefits administrator and recipient of documents related to enrollment and eligibility will be responsible for retaining and archiving all documents received by Winston on behalf of the Customer and its participants. At a minimum, digital copies of these documents will be retained throughout the length of Customer relationship and continue for a period of at least seven (7) years following the severance of the relationship.

4. Service Center Services

Throughout the year, Winston will provide all employees of the Customer toll-free access to our Service Center for the following purposes:

- a) **Application/Technical Support.** Representatives will provide the Customer's employees with assistance in resetting passwords, login assistance and navigational support across BenefitInsite.

Call-Center Hours of Operation. The Service Center will be staffed from Monday through Friday, 8:30AM to 8:00PM EST. Additional hours will be supported during Open Enrollment Periods.

Call Recording. All records taken by a Representative will be recorded and retained through the duration of our relationship with the Customer.

5. Additional Considerations

During the implementation of the services described in Schedule A, the Customer agrees to partner with Winston on the successful delivery of described services. Winston will assign a Project Manager to the implementation that will manage the timely delivery of all deliverables and track progress on a weekly basis. The Project Manager will create and distribute a Project Plan to everyone associated with the implementation that will list all of the tasks required to complete the project. After discussing the tasks and due dates, the Customer and Winston agree to adhere to all of the due dates listed in the Project Plan. This is necessary to ensure that the project remains on schedule. In many cases, work performed by Winston is dependent on receiving items from the Customer. If the Customer is unable to meet any of its due dates, the project may be delayed. If Winston incurs additional cost to compensate for the late delivery of items from the Customer, Winston reserves the right to adjust the deliverable dates of our services and/or request additional fees as compensation for out of scope work, significant work performed after hours by staff and costs incurred to obtain temporary staffing such as Benefit Counselors. Proposed alternate delivery dates, penalties and/or additional fees will be identified to Customer at the time of delay.

6. Custom Programming and Customer Service Requests

As part of this SOW, Winston will provide Customer with up to ten (10) hours of IT support per quarter in the form of programming, configuration adjustments and where necessary, appropriate and/or requested by the Customer, customizations made to the software which are not currently part of the application.

All modifications and changes to the existing application which are beyond the scope of support, operations or the functionality of the software will be assessed and scoped for impact and time. A change request will be generated which requires the Customer signature and authorization before work will begin.

Other than for any Customer-identifiable portion of any deliverable created pursuant to this paragraph, which shall belong to Customer, all such deliverables shall remain Winston's property and may be incorporated into BenefitInsite.

Schedule B : Site Availability, Performance and Security Protocols

Winston agrees that the services and applications described in this SOW shall be subject to the site availability, performance and security protocols described in this Schedule B.

This Schedule is attached to and forms a part of the Statement of Work ("SOW"). Winston agrees that the services and applications described in this SOW shall be subject to the site availability, performance and security protocols described below.

- 1) WFS agrees to comply with, and require its hosting providers, subcontractors and other representatives (collectively, "Representatives") who are assigned to perform services under the MSA to comply with industry standards for information security.
- 2) In addition to the general covenants of legal compliance set forth in the MSA, WFS shall adhere to all applicable regulatory requirements pertaining to privacy and handling of customer information, including those that become applicable by reason of international business activities of Customer or WFS. If WFS intends to use any processing facility located outside the United States to process any data relating to Customer or its customers or otherwise transmit any data relating to Customer or its customers across national borders, WFS shall provide advance written notice to Customer. If WFS proposes to do so, WFS shall see that all related processing facilities and systems comply with all applicable laws, regulations, treaties, and other legal requirements of the United States, all other affected countries, and any international organizations having jurisdiction, including without limitation, those with regard to data security and privacy, data processing and transmittal of data across national borders.
- 3) The design, hosting, maintenance and operation of BenefitInsite includes, but is not limited to, the standards and practices set forth below:
 - a) Availability. BenefitInsite will be available 24 hours per day, 7 days a week and 365 days a year, subject to the below terms and conditions.
 - b) Reliability. It is our policy to be fully operational a minimum of 99.5% of the time (measured on a monthly basis), excluding Scheduled Maintenance. Winston will notify Customer of any scheduled maintenance which exceeds a period of 60 minutes. From time to time, scheduled maintenance may need to occur during regular business hours. Significant scheduled maintenance (more than one hour) during normal business hours will not occur more than twice in any 30-day period unless due to Winston's hosting provider notification that such maintenance is required. Winston will provide notice of any expected downtime due to scheduled maintenance. In the event Winston experiences an unplanned outage, Winston will notify Customers with a description of the material downtime (downtime lasting longer than 30 minutes), including an approximate length of time the site was down and a best-known reason for the downtime.
 - c) Performance Standards. Winston will maintain an average response time of twenty-five (25) seconds; "response time" is defined as server response time only and excludes network transmission time. In the event that response times are lower than described in the preceding sentence, Winston will make the necessary adjustments and remedy within a 30 day period. Winston will report on its compliance to the average response time on a quarterly basis.
 - d) Data Protection and Security. Winston (or its hosting agent, currently Rackspace LLC) will maintain a protected and secure data center environment with physical access restricted to authorized personnel, and network and remote access for end users restricted by firewall, two factor authentication, encryption and other electronic means. Winston's hosting facility will also provide sufficient fire suppression equipment so as to protect the computer hardware and network hardware used by BenefitInsite, and backup power supplies to provide uninterrupted supplies of electricity.
 - e) Security Incident Response. (A) "Security Incident" shall mean the loss or destruction of, unauthorized disclosure of, or unauthorized access to or use of, Customer Data. In the event Winston determines that it has experienced a security incident involving Participant data which may require Winston, as allowed by law and subject to the terms of the Business Associate Agreement in Appendix C of the Agreement, to provide notice of such Incident ("Security Incident"), Winston will do the following:
 - i. Provide Customer, as soon as is reasonably practicable, with the following information, to the extent then available: (a) the date the Security Incident occurred, (b) the date Winston discovered the Security Incident, (c) a brief description of such Security Incident, and (d) a description of the steps that have been, or will be, taken to investigate the Security Incident, mitigate its potential harmful effects, and prevent a recurrence. As allowed by law,

- Customer shall treat any information received from Winston in connection with a Security Incident as Confidential Information;
- ii. Update the information provided pursuant to paragraph A on a reasonable basis as material, new information becomes available to Winston;
 - iii. Provide Customer, as soon as is reasonably practicable and in all events before Winston delivers any security breach notification to any Participant, with a complete list, including name and mailing address, of each Participant to whom Winston will deliver the notice;
 - iv. Provide Customer with a reasonable opportunity to review and comment upon any security breach notification that Winston plans to deliver to any Participant before Winston delivers such notice; provided, however, that Winston may provide the security breach notification to any Participant prior to providing Customer the information in paragraph A.e.3 and prior to the completion of Customer's review and comment period pursuant to this paragraph if necessary to comply with applicable law; provided, further, that Winston shall not be responsible for and Customer shall indemnify, defend and hold harmless Winston with respect to any delay in notifying Participants caused by Customer's review of the notifications described in this paragraph;
 - v. In the event Winston does not offer in its security breach notification, at no charge to the Participant to whom Winston will deliver the notice, services to mitigate the potential harmful effects of the security breach, such as credit monitoring and fraud resolution services, promptly reimburse Customer for the reasonable costs incurred by Customer in connection with its offering such services, which are reasonable and customary in relation to the security breach, including, but not necessarily limited to, credit monitoring and fraud resolution services, to any Participant to whom Winston delivered a security breach notification;
 - vi. In the event Winston in its security breach notification, at no charge to the Users to whom Winston delivers the notice, offers services to mitigate the potential harmful effects of the security breach, promptly reimburse Customer for the reasonable costs incurred by Customer in connection with its offering any supplemental services which Customer in good faith and after consultation with Winston reasonably believes are necessary to mitigate the potential harmful effects of the security breach to the affected Participants.
- f) Availability of Cloud Services. Winston (or its hosting agent) will maintain resiliency of the web servers and Internet connectivity for the BenefitInsite system. The infrastructure will accommodate the failure of individual items by not impairing the delivery of text, graphics, or other information to users of BenefitInsite.
- g) Backup. Winston will perform automatic and regularly scheduled backup of all data entered on BenefitInsite on a daily basis and will maintain procedures for restoration of such backups. Backups will be stored at a commercial media storage vendor located offsite from the server facility. Transport of media will be provided by bonded courier or vendor's agent. Winston will regularly back up programs running on BenefitInsite whenever these programs are modified. Backup media sets containing Customer data will be stored in encrypted format, per Winston security standards, and retained for a maximum of four (4) months unless otherwise amended by contractual obligations.
- h) Staffing Levels. Winston (or its hosting agent) will maintain twenty-four (24) hours per day, seven (7) days per week staffing of the data center hosting facility.
- i) Security Monitoring. Winston will maintain a plan for identifying and avoiding losses of data or programs, breaches of security, viruses, and disabling or harmful devices on the computers operated in connection with the design, hosting, operation and maintenance of BenefitInsite.
- j) Facilities Management. Winston (or its hosting agent) will maintain a facilities management plan, including data backups, computer hardware maintenance, network hardware maintenance, installation of software updates and fixes as supplied by the manufacturers of the computer and network hardware in place.
- k) Real Time Activity Monitoring. Winston will maintain a real time activity monitor that will detect any significant performance degradation or down time for BenefitInsite, including, but not limited to, server availability and health, effectiveness of the firewalls, and the availability of the database.
- l) Disaster Recovery. Winston (or its hosting agent) will apply all Disaster protection and recovery mechanisms set forth in Winston's Disaster Recovery Plan (as updated by Winston from time to time) to avoid and/or minimize the loss of service and/or damage arising from any impairment of BenefitInsite, caused by and/or resulting from a Disaster. For purposes of this subsection, a "Disaster" includes any threatened or actual interruption or shutdown (of any duration) of any facility that directly or indirectly affects BenefitInsite. Winston will report on the results of its real-time activity monitoring that will detect significant performance degradation or down time on BenefitInsite on a quarterly basis.

Schedule C: Maintenance and Support Services

This part describes the terms and conditions relating to Maintenance and Support that WFS shall provide during the Term of this Agreement for the BenefitInsite. The Maintenance and Support described in this SOW does not limit any warranty set forth in the MSA. Winston will provide the following services:

- 1) **Help Desk.** WFS shall provide phone and email technical support for Customer related to the use and operation of BenefitInsite during Business Hours. "Business Hours" means 8:30AM ET to 5:00PM ET, Monday through Friday excluding holidays.
- 2) **Software Maintenance Releases.** WFS shall without additional charge make, install, configure, test and do everything necessary to see that BenefitInsite includes software and documentation for any maintenance releases and any new versions of BenefitInsite.
- 3) **Error Correction.** WFS shall make, install, configure, test and do everything necessary to see that BenefitInsite includes appropriate workarounds or bug-fixes or otherwise repair or correct any material, reproducible deviations from normal operating performance of the System in a timely fashion according to the severity of the error, as determined by Customer, as set forth in the table below for Severity 1 - 3 Errors and the impact on the end user's ability to operate and use BenefitInsite. WFS will promptly log, research and resolve errors Deviations in BenefitInsite.

Severity Level	Definition
Severity Level 1	High Visibility Any error, bug or malfunction that causes a failure or imminent failure of BenefitInsite as a whole or any critical component of BenefitInsite, resulting in it being largely unusable for its intended purpose.
Severity Level 2	Moderate Visibility An error, bug, or malfunction that causes significant system degradation, without causing a Severity 1 Error . Limited capability but only with a difficult work around.
Severity Level 3	Low to Medium Visibility An error, bug, or malfunction that affects use of BenefitInsite or a component of BenefitInsite but is not: (a) a Severity 2 Request; (b) a Severity 1 Request; or (c) a single question regarding features of BenefitInsite. Limited capability but is excessively slow or inconvenient to use.

- 4) **Response and resolution times.** WFS will make best efforts basis to respond and address all issues during business hours, according to the timetables below.

Severity	Phone Response Time Goal	Engagement Time	Resolution Time
Severity 1	2 hours	2 Hours	6 hours
Severity 2	6 hours	1 Business Day	2 Business Days
Severity 3	1 Business Day	2 Business Day	10 Business Days

Schedule D: Outsourced System and Data Security

This Schedule describes the obligations, procedures and protocols that Winston agrees to as it pertains to Outsourced Systems and Data Security. If provisions in the MSA and this Schedule impose inconsistent obligations on WFS, the provisions of this Schedule shall control. Obligations set forth herein that are more stringent than (or additional to) those of the MSA shall be deemed cumulative, not inconsistent.

- 1) WFS agrees to comply with, and require its hosting providers, subcontractors and other representatives (collectively, "Representatives") who are assigned to perform services under the MSA to comply with industry standards for information security.
- 2) In addition to the general covenants of legal compliance set forth in the MSA, WFS shall adhere to all applicable regulatory requirements pertaining to privacy and handling of customer information, including those that become applicable by reason of international business activities of Customer or WFS. If WFS intends to use any processing facility located outside the United States to process any data relating to Customer or its customers or otherwise transmit any data relating to Customer or its customers across national borders, WFS shall provide advance written notice to Customer. If WFS proposes to do so, WFS shall see that all related processing facilities and systems comply with all applicable laws, regulations, treaties, and other legal requirements of the United States, all other affected countries, and any international organizations having jurisdiction, including without limitation, those with regard to data security and privacy, data processing and transmittal of data across national borders.
- 3) In addition to any audits required by the MSA, At Customer's request, WFS shall submit its privacy statement and policy as well as its data privacy and information systems security measures and policies to an audit by Customer and its counsel and representatives, or a mutually agreeable third party. WFS shall remedy any shortcomings identified in such audit and make all changes necessary to comply with applicable law, and otherwise see that its policies and systems conform to any reasonable requests made by Customer or such auditors.
- 4) WFS shall maintain Customer's data in separate directories at all times and shall maintain a hardware/software configuration that ensures only authorized users will have a logical path to Customer's data.
- 5) WFS shall provide evidence that an intrusion detection system is installed and that monitoring is performed on a continuing basis. WFS shall maintain sufficient software, hardware, systems, personnel and other resources to ascertain whether a penetration attempt is being made against any part of the network, mainframe, server or other infrastructure or facilities used by WFS to process or transport Customer information. WFS will identify and advise Customer of any internal and external risks noted that could result in unauthorized disclosure, misuse, alteration or destruction of or access to customer information or Customer information systems and implement appropriate internal technical and procedural controls to prevent such intrusions.
- 6) WFS shall, no less frequently than annually perform or contract with an independent party to perform vulnerability scans of internal and external networks, applications, hosting sites, and other networking systems using industry accepted practices and tools. WFS shall also, no less frequently than annually, perform or contract with an independent party to perform application penetration testing. WFS shall advise Customer of the scope (in advance, unless impractical or such notice would invalidate the integrity of the simulation) of a vulnerability scan or penetration testing, the results of such scan or testing, and a plan for remediating any threats, vulnerabilities, or other weaknesses within a reasonable period of time thereafter. WFS may contract with an independent party to continually monitor website and network security, provided that WFS shall report and provide a remediation plan for any vulnerabilities to Customer as provided above.
- 7) WFS shall assure that appropriate audit trails and logs of all activities affecting Customer processing and data are captured, periodically reviewed, and retained by WFS or transferred to a next custodian for a period of at least 1 year after termination of the MSA.
- 8) Ownership and licensing rights with respect to WFS's software systems (operating systems, utilities, database and application software) shall be clearly documented and disclosed to Customer upon request. WFS shall enter into escrow agreements (and see that its mission-critical subcontractors do the same) in commercially reasonable form and substance ensuring WFS (or its subcontractors, as the case may be) the right to access the appropriate object and source code should the software provider become insolvent or fail or refuse to provide any necessary software maintenance and support.
- 9) System controls associated with all platforms and the networks or network interfaces used to process Customer applications and data shall be managed and maintained in accordance with industry standards, including remediation of vulnerabilities and known bugs that could cause exposure to malfunctions, errors or malicious activity as soon as possible.
- 10) The information and materials processed or stored by WFS on behalf of Customer shall be handled in accordance with the classification (e.g., confidential, sensitive, public) of the information under applicable regulations as well as WFS's standards and policies, as in effect from time to time.

- 11) Use of data by WFS for data mining or for any purpose other than the processing directly contracted by Customer shall not be allowed without the express written permission of an executive officer of Customer or Chief Privacy Officer.
- 12) The release of any user information, such as access rights, shall be made only to the appropriately authorized personnel as defined by the Customer application owner.
- 13) Software, data, written materials, hardcopy of printouts, and storage media containing Customer data shall be secured at all times from unauthorized copying, use, duplication, and storage, and shall be securely destroyed when no longer required. WFS shall ensure the proper degaussing, cleansing, disposal or destruction of data contained on all media (e.g., shredding of paper, microfiche, degaussing of optical, magnetic and other media, computer drives and disks).
- 14) Access to production data and software for non-Customer and WFS employees shall be based on authorized job-related responsibilities. A record of all access requests and authorization shall be maintained and used by authorized parties alone to verify the work of the personnel implementing the access capability to the systems. A record of all access requests and authorizations granted shall be maintained for use by authorized parties to verify the work of the personnel implementing the access capability to the systems.
- 15) WFS shall log all actual or attempted log-on violations as well as access violations.
- 16) WFS shall generate access history logs for critical application transactions, retain the logs for at least one year, and keep them accessible in a format mutually agreeable to by Customer and WFS, for Customer's review, search, copying and reproduction.
- 17) Where possible, the access ID, password format or other access device (e.g., smartcard) shall be consistent with the criteria set forth in the Customer policies. Requirements include ID and password minimum characters, logging, suspension, and reset.
- 18) WFS shall ensure appropriate and prudent levels of separation of duties. Separation of duties shall be stated for security administration, review of access and violation reports when those responsibilities remain the responsibility of WFS.
- 19) WFS shall provide Customer with the evidence of WFS-equivalent security control over WFS's service providers who support, store, recover, or otherwise handle the systems or data associated with the Customer relationship.
- 20) WFS shall validate the accuracy of all access control lists that allow any WFS or Customer users to access Customer data, software, files and operational software. Such validations will include application transactions, application datasets and files, any operating system special privileges, system utilities and tools authorities, database software privileges, software management functions, console command authorities, security administration authorities, operating system and security parameters definitions.
- 21) Upon request, WFS shall provide Customer with the capability to review all access control and security parameter definition lists that directly or indirectly control the access to Customer data.
- 22) An incident response process based on a collaborative approach among Customer and WFS shall be developed to respond rapidly and effectively to security incidents. The incident notification process shall be outlined in the MSA and will include whom to notify, how to notify, and when notification will occur. WFS will provide Customer with all the legally allowed evidence and documentations of WFS's investigation related to any security incident.
- 23) WFS will maintain appropriate physical, electronic and procedural safeguards to store, and secure any and all Customer information to protect it from unauthorized access, use, disclosure, alteration, loss and destruction. If and when Customer information is to be destroyed, which shall not occur without Customer's written consent and verification, WFS shall ensure that such information is completely and properly destroyed, including by way of example and not limitation, the shredding or pulping of paper and the scrub of electronic devices using the latest available technology so no information can be reconstructed. The safeguards used by WFS to protect Customer's information will be no less than those used by WFS to protect its own confidential information and industry standards.
- 24) Customer shall have the right to perform such audits more frequently (i) if necessary for Customer to meet or respond to any regulatory requirement or inquiry; or (ii) as deemed reasonably necessary by Customer as a result of Customer's good faith belief that WFS or its hosting provider has breached (or caused a breach) any of its obligations hereunder. WFS and its hosting provider shall provide commercially reasonable access to the systems and any other documents or materials as are necessary to reasonably confirm compliance with WFS's obligations provided under this SOW and the MSA.
- 25) If any data security or similar report prepared by an independent auditor reveals that WFS's internal controls, in whole or in part, fail to constitute effective controls over financial reporting, WFS shall prepare and deliver to Customer a plan that is reasonably acceptable to Customer for promptly addressing such issues, which may consist of correcting specific deficiencies or exceptions or instituting compensating controls, as reasonably determined by WFS ("Corrective Plan"). WFS shall deliver the Corrective Plan to Customer within ninety (90) calendar days following WFS's delivery to Customer of any report containing the deficiencies and/or



exceptions. WFS shall bear all costs and expenses associated with correcting, or instituting compensating controls for, all deficiencies and exceptions identified in the Corrective Plan if such deficiencies and/or exceptions affect WFS's customers generally.

- 26) All audits and reports under this agreement shall be confidential, and Customer shall not, without WFS's prior consent, disclose or permit any other person to disclose the results of the audit to any person except as required by Applicable Laws.

Schedule E: Fee Schedule

Pricing is based on the following assumptions and highlights:

Variable	Assumption(s)
Headcount & Eligibility	1,750 Full-Time, Benefit Eligible Employees 100 Retirees
Vendor Interfaces	All Vendors including Payroll Vendor
Wellness Incentive	Yes, if applicable

2016 – 2019 Summary of Services

Benefit*insite* Communicate, Enroll & Admin

- Web Based Benefit & Communication Portal
- Manager & Employee Self Service (OE, NH, LE – *all benefits*)
- Administrator Rights & Reporting
- Beneficiary, Eligibility & EOI Management
- Recordkeeping for all enrollment and eligibility data
- Dedicated service team to manage scope of service deliverables

Vendor Administration

- Secure, Electronic Integration w/ Vendors
- Carrier Eligibility Reporting & Reconciliation

Employee Service Center

- Application and technical support
- Includes toll-free #, call recording & line charges

Dependent Eligibility Services

- Documentation pends and storage of all eligible transactions

ACA Employee & Employer Federal Form Reporting

- Form 1094-B Employer Generation & Submission
- Form 1095-C Employee Form – Electronic Generation
- Documents available within the application
- 1095-C Employee Form Printing
 - Print & Fulfillment of Form 1095-C
 - USPS 1st Class Postage

Fee For Services

\$2.88 PE/PM

1. All Implementation and/or up front charges are **WAIVED**.
2. Fixed rate pricing for 3 year period insures vendor and service stability.
3. Assumes vendor and plan and contribution rate changes within each plan year.
4. Assumes load of "in-force" data prior to go "live" date.
5. Fulfillment of the 1095-C Employee Form is based on current 1st Class postage rates. Winston reserves the right to revise the annual fulfillment cost based on changes to the 1st Class postage rate.
6. Billing of the monthly fee will begin on the month Benefit*insite* goes "live".