WORKFORCE SOFTWARE SAAS AGREEMENT

This WorkForce Software SaaS Agreement (the "Agreement") is entered into between WorkForce Software, LLC, 38705 Seven Mile Road, Suite 300, Livonia, Michigan 48152 ("WFS") and the "Customer" defined below.

Customer Name: _____

Address: _____

_____

_____

1. Definitions

1.1. "Affiliate" means a legal entity separate from and controlled by or under common control with the either party. For purposes of this Agreement, the term "control" shall mean ownership of a beneficial controlling interest.

1.2. "Customer Data" shall mean any content, materials, data and information provided by the Customer to WFS in the course of using the SaaS Service.

1.3. "Documentation" shall mean all written or electronic materials provided to Customer by WFS for facilitating use of the SaaS Service as applicable, but does not include advertising or similar promotional materials.

1.4. "Effective Date" is the Schedule Effective Date of the first executed Schedule.

1.5. "e-Learning Courseware" shall mean video or online training content and related materials which may be provided to Customer by WFS under a separate Schedule to this Agreement.

1.6. "Force Majeure" shall mean any event outside of the control of WFS, such as, but not limited to, a natural disaster, fire or extended power, electrical or Network outage, which renders the SaaS Service temporarily unavailable or permanently affects or prevents performance under this Agreement.

1.7. "Intellectual Property Rights" shall mean all copyrights, trade secrets, patents, and other intellectual property rights or portion thereof including, but not limited to, the ideas, methodologies, methods of operation, processes, and look and feel in the SaaS Service.

1.8. "Network" means the Internet, phone network, cell phone network, and other transmission methods by which the SaaS Service is delivered.

1.9. "Party" or "Parties" shall mean WFS or Customer individually or collectively.

1.10. "Production Environment" means an environment provided in the SaaS Service which Customer uses for live processing.

1.11. "Related Systems" shall mean Customer owned or operated computers, web-browsers, operating systems, firewalls, e-mail servers, LDAP servers, portals, Networks, third party software, internet

connection, and any other hardware or software that connects to the SaaS Service or affects the SaaS Service if they are not configured or operating properly or are operating in such a manner as to cause an interruption or failure of the SaaS Service, whether or not provided by or configured by WFS.

1.12. "SaaS Service" or "SaaS Services" means the provision of access to and use of WFS software as a service platform, together with the provision of updates and upgrades, and related services including maintenance and support, all in accordance with the Agreement and the applicable Schedule.

1.13. "Schedule" means one or more written orders listing the services to be delivered to the Customer which is signed by both WFS and the Customer which references this Agreement.

1.14. "Service Level Agreement" or "SLA" means the service levels specified in Exhibit A.

1.15. "Support Services" shall mean the services specified in the Support Plan, including reasonable technical support via telephone, e-mail, and/or the web, to answer questions or provide assistance in the use of the SaaS Service.

2. Services Delivered

2.1. WFS shall provide access to the SaaS Service to Customer via the Network as specified in the Schedules. Any use of the SaaS Service prior to the Commencement Date specified in the Schedule(s) shall be considered a trial period during which the SLA shall not apply. Within the Production Environment, Customer may use only the applications and extensions specified in the Schedule(s), even if other applications and extensions are made available.

2.2. WFS may periodically update ("Update") the SaaS Service, but makes no representations as to the frequency of new releases or the features, enhancements, or corrections that will be provided in the Updates.

2.3. Customer shall limit the access to the SaaS Service to its own employees, consultants, and other authorized users and shall not make the SaaS Service available to third parties or make it available on a service bureau basis.

2.4. WFS shall take commercially reasonable measures, consistent with those in the industry, to prevent unauthorized parties from gaining (a) physical access to the data centers where the SaaS Service is hosted, and (b) electronic access to the SaaS Service or the Customer Data. WFS shall promptly notify Customer of any unauthorized access to the SaaS Service which WFS detects.

2.5. WFS shall periodically backup the Customer Data ("Backup Services") as specified in the SLA. WFS will undertake commercially reasonable steps to begin the restoration of Customer Data from the backup as soon as WFS is notified or becomes aware of the need to restore data. WFS shall not be responsible if Customer Data is lost or corrupted in between scheduled backups or for a reason caused by the acts or omissions of Customer. Customer Data shall not be used by WFS for any other purpose except to provide the services contemplated under the Agreement. WFS shall not preserve such Customer Data longer than contracted.

2.6. In a Force Majeure event, WFS shall make commercially reasonable efforts to restore the SaaS Service at an alternate facility as soon as feasible. Until such Force Majeure event shall have passed, the SaaS Service may be provided on a reduced use basis and may require Customer to make changes to the procedures used to access the SaaS Service. Neither party shall incur any liability to the other party on account of any loss or damage resulting from any delay or failure to perform all

or any part of this Agreement, where such delay or failure is caused, in whole or in part, by a Force Majeure event. If a party asserts a Force Majeure event for failure to perform the party's obligations, then the asserting party shall notify the other party of the event and take commercially reasonable steps to minimize the delay or damages caused by the Force Majeure event.

2.7. WFS shall provide the Support Services specified in the Support Plan. The Support Plan description attached as Exhibit B provides details of the service levels and items provided under each plan. Terms of the Support Plan supersede the terms in this Agreement.

3. Customer Responsibilities

3.1. Customer shall be responsible for entering its Customer Data into the SaaS Service and Customer shall be responsible for the maintenance of the Customer Data supplied by it. Customer hereby represents and warrants to WFS that the Customer Data is free of all viruses, Trojan horses, and comparable elements which could harm the systems or software used by WFS or its subcontractors to provide the SaaS Service. Customer agrees that it has collected and shall maintain and handle all Customer Data in compliance with all applicable data privacy and protection laws, rules and regulations.

3.2. Customer has sole responsibility to maintain the integrity, confidentiality and availability of information on Customer equipment.

3.3. Customer has sole responsibility to (a) check the accuracy of information processed using the SaaS Service, (b) run all normal processes and procedures within the SaaS Service such as end of period processing, imports, exports, and file transfers, and (c) manage and configure its Related Systems and ensure they operate properly. When using and applying the information generated by the SaaS Service, Customer is responsible for ensuring that Customer complies with the applicable requirements of federal and state law. Customer agrees: (i) using the SaaS Service does not release Customer of any professional obligation concerning the preparation and review of such reports and documents, and (ii) Customer does not rely upon WFS or the SaaS Service for any advice or guidance regarding compliance with federal and state laws or the appropriate tax treatment of items reflected on such reports or documents.

3.4. Customer assumes all responsibilities and obligations and expertise with respect to (a) the selection of the SaaS Service to meet its intended results, and (b) any decision it makes based on the results produced by the SaaS Service. Customer understands and acknowledges that WFS and the Third Party Content Vendors are not engaged in rendering legal, accounting, tax or other professional advice either as a service or through the SaaS Service and it is not relying on WFS and the Third Party Content Vendors for any advice or guidance regarding laws and regulations. Customer shall review all calculations and determinations made using the SaaS Service and satisfy itself those results are accurate. If legal, accounting, tax or other expert assistance is required, the services of a competent professional will be sought by Customer. To the extent permitted by law, Customer shall indemnify and hold WFS harmless from claims and demands of its employees or former employees arising from the use by Customer of the SaaS Service.

3.5. Customer is solely responsible to ensure Related Systems operate properly. The support provisions of this Agreement do not apply to Related Systems or problems in the SaaS Service caused by Related Systems, regardless of who provided, installed, or distributed such. Should WFS identify that the root cause of a problem is caused by Customer modifications to the SaaS Service or behavior in Related Systems it shall notify Customer and request approval to provide additional assistance (if

applicable). Should Customer give its approval, the additional time spent by WFS after such approval shall be billed to customer on a time and materials basis at the then current rates.

3.6. Customer shall not perform any stress test, load test, or security test on the SaaS Service without first obtaining WFS permission and executing a separate agreement for the services required by WFS to support such tests. Notwithstanding the foregoing, stress testing, load testing and security testing shall not be allowed for WorkForce Forecasting & Scheduling.

3.7. Customer shall change all passwords used to access the SaaS Service at regular intervals. Should Customer learn of an unauthorized third party having obtained knowledge of a password, Customer shall inform WFS thereof without undue delay and promptly change the password. Customer will terminate old users in the SaaS Service.

3.8. Customer is responsible for monitoring user access to the SaaS Service.

3.9. Customer is responsible for the connection to the SaaS Service, including the Internet connection.

4. Term and Termination

4.1. The term of this Agreement starts on the Effective Date and terminates when all Schedules terminate. Schedules automatically renew for additional one (1) year periods unless either party provides a written notice of termination to the other party at least sixty (60) days prior to the end of the then current term. The per-unit pricing during any such renewal term shall increase by 5% per year over the base prices listed in the Schedules for the relevant services in the immediately prior term.

4.2. The provisions of Sections 2.5, 2.6, 3, 5, 7, 8.4, 8.5, 8.6 and any payment obligations incurred by Customer prior to or upon termination shall survive termination of this Agreement.

4.3. If either party commits a material breach of this Agreement, and should such breach not be corrected within thirty (30) days after receipt of written notice from the non-breaching party, this Agreement may be terminated by the non-breaching party upon written notice. Notwithstanding the foregoing, if the nature of the breach requires longer than thirty (30) days to cure, and WFS is taking commercially reasonable efforts to cure such breach at the end of the initial thirty (30) day cure period, WFS shall have a reasonable time thereafter to continue to effectuate a cure of such breach. Upon termination in such instance, WFS shall refund the unexpired portion of any fees paid.

4.4. Upon the effective date of termination, Customer's access to the SaaS Service will be terminated. Thirty (30) days after the effective date of termination, WFS shall have no obligation to maintain or provide any Customer Data. Upon termination of the Agreement, WFS shall use commercially reasonable efforts to permanently and irrevocably remove, purge or overwrite all data still remaining on the servers used to host the SaaS Service, including, but not limited to, Customer Data, unless and to the extent applicable laws and regulations require further retention of such data. All indemnifications relating to the unauthorized disclosure of Customer Data shall continue until such data is returned to Customer or destroyed.

5. Proprietary Right, Non-Disclosure

5.1. Each party shall maintain as confidential and shall not disclose, publish, or use for purposes other than as intended in this Agreement the other party's Confidential Information except to those employees, contractors, legal or financial consultants and auditors of the recipient and its Affiliates who need to know such information in connection with the recipient's performance of its rights and obligations under the Agreement and in the normal course of its business and who are bound by

confidentiality terms no less stringent than the terms contained herein. "Confidential Information" shall include, but shall not be limited to, Customer Data, the SaaS Service, the pricing and terms of this Agreement, benchmarks, statistics or information on the capabilities of the SaaS Service, financial information, business plans, technology, marketing or sales plans that are disclosed to a party and any other information that is disclosed pursuant to this Agreement and reasonably should have been understood by the receiving party to be proprietary and confidential to the disclosing party because of (i) legends or other markings, (ii) the circumstances of disclosure, or (iii) the nature of the information itself. Each party shall protect such Confidential Information with reasonable care and no less care than it would exercise to protect its own Confidential Information of a like nature and to prevent the unauthorized, negligent, or inadvertent use, disclosure, or publication thereof. Notwithstanding anything else in this Agreement, either party may disclose Confidential Information in accordance with a judicial or governmental order, or as otherwise required by law, provided that the recipient either: (i) gives the disclosing party reasonable notice prior to such disclosure to allow the disclosing party a reasonable opportunity to seek a protective order or equivalent, or (ii) obtains written assurance from the applicable judicial or governmental entity that it will afford the Confidential Information the highest level of protection afforded under applicable law or regulation. Notwithstanding the foregoing, neither party shall disclose any computer source code that contains Confidential Information in accordance with a judicial or other governmental order unless it complies with the requirement set forth in sub-section (i) of this Section 5.

5.2. Either party may disclose the existence of this Agreement and its terms to the extent required by law, the rules of any applicable regulatory authority or the rules of a stock exchange or other trading system on which that party's securities are listed, quoted, and/or traded.

5.3. Breach of the obligations in Section 5 may cause irreparable damage to the disclosing party and therefore, in addition to all other remedies available at law or in equity, the disclosing party shall have the right to seek equitable and injunctive relief for such breach. In the event of any litigation to enforce or construe this Section 5, the prevailing party shall be entitled to recover, in addition to any charges fixed by the court, its costs and expenses of suit, including reasonable attorneys' fees, costs and expenses.

5.4. WFS shall retain all rights, title, and interest in the e-Learning Courseware, Third Party Services and the SaaS Service. Customer shall not alter, modify, copy, edit, format, translate, or create derivative works of these materials, except as provided herein or when approved in writing by WFS.

5.5. As between WFS and Customer, Customer shall own all title, rights, and interest in Customer Data.

5.6. Both parties agree to comply with all applicable privacy and data protection statutes, rules, or regulations governing the respective activities of the parties. Customer hereby consents to the use, processing and/or disclosure of Customer's data only for the purposes described herein and to the extent such use or processing is necessary for WFS to carry out its duties and responsibilities under this Agreement or as required by law.

6. Payments, Credits, and Refunds

6.1. Customer shall pay all fees specified in the Schedule(s) to WFS or its designated representative. Unless specified otherwise in the Schedule(s): (i) fees are based on services purchased in the Schedule(s) and overage fees, (ii) payment obligations for the Service Term specified in each Schedule are non-cancelable and fees paid are non-refundable, (iii) the quantities ordered under the Schedule cannot be decreased during the term, and (iv) all fees quoted and payments made hereunder shall be in U.S. Dollars. The Schedule(s) specify how the Customer may use the SaaS

Service and how the usage of the SaaS Service will be measured. Any use of the SaaS Service in excess of the amounts specified in the Schedules shall be billed to the Customer quarterly in arrears at 125% of the unit prices specified in the Schedule ("Overage Fees").

6.2. WFS fees are exclusive of all taxes, levies, or duties imposed by taxing authorities, and Customer shall be responsible for payment of all such taxes, levies, or duties, except for taxes on WFS net income (including FCC and related taxes and charges for phone based systems).

6.3. Customers outside of the United States shall pay all invoices via electronic transfer. All invoices submitted shall be due Net 30. If Customer reasonably disputes an invoice, Customer must pay the undisputed amount when due and submit written notice of the disputed amount (with details of the nature of the dispute and the invoice(s) disputed) within thirty (30) days of receipt of the invoice. WFS may assess interest at the rate of 1.5% per month or the maximum allowed by law on balances not paid when due. Customer shall pay all costs incurred in the collection of charges due and payable, including reasonable attorney fees, whether or not suit is instituted.

6.4. Upon written notice by Customer to WFS of its failure to satisfy the Uptime Commitment of the SLA within thirty (30) days of the end of a month, WFS shall credit Customer the fees as calculated in the SLA towards the next payment due from Customer. The credits provided to Customer shall be its sole and exclusive remedy for WFS's failure to comply with the Uptime Commitment.

7. Warranties and Indemnifications

7.1. WFS shall, at its expense, indemnify, defend and hold Customer harmless from and against any claim that the SaaS Service infringes an Intellectual Property Right; provided, however, that (a) Customer promptly notifies WFS of any such claim, and (b) permits WFS to defend with counsel of its own choice, and (c) Customer gives WFS such information and/or assistance in the defense thereof as WFS may reasonably request. In no event shall Customer settle any such claim without the written consent of WFS. If the SaaS Service is adjudged to infringe an Intellectual Property Right by a court of competent jurisdiction, WFS shall, at its expense and election either: (i) procure the right for Customer to continue using the infringing items, (ii) replace the infringing items with a functionally equivalent non-infringing product, (iii) modify the infringing items so that they are non-infringing, or (iv) terminate the affected Schedule and refund the unexpired portion of any fees paid. In no event shall WFS, its employees, agents and sub-contractors be liable to the Customer to the extent that the alleged infringement is based on: (a) a modification of the SaaS Services or Documentation by anyone other than WFS, or (b) the Customer's use of the SaaS Services or Documentation in a manner contrary to the instructions given to the Customer by WFS, or (c) the Customer's use of the SaaS Services or Documentation after notice of the alleged or actual infringement from WFS or any appropriate authority. The provisions of Section 7.1 constitute the entire liability of WFS and sole remedy of Customer with respect to any claims or actions based in whole or in part upon infringement or violation of an Intellectual Property Right of any third party.

7.2. WFS represents and warrants: (a) it has the right to grant the rights specified herein, and (b) the SaaS Service will not contain any viruses or Trojan horses.

7.3. THE WARRANTIES AND REMEDIES SET FORTH HEREIN ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, WHETHER ORAL OR WRITTEN, EXPRESSED OR IMPLIED. EXCEPT AS SPECIFICALLY SET FORTH IN THIS SECTION 7, WFS SPECIFICALLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES TO THE SAAS SERVICES AND ANY OTHER MATTER WHATSOEVER. IN PARTICULAR, BUT WITHOUT LIMITATION, WFS SPECIFICALLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD

PARTY RIGHTS OR ANY OTHER WARRANTY ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE. NO WFS AGENT, CONTRACTOR OR EMPLOYEE IS AUTHORIZED TO MAKE ANY MODIFICATION TO THIS WARRANTY, UNLESS IN A SIGNED WRITING EXECUTED BY A WFS EMPLOYEE WITH ACTUAL AUTHORIZATION TO BIND WFS. WFS DOES NOT WARRANT THAT THE SAAS SERVICE OR ANY PORTION THEREOF WILL OPERATE UNINTERRUPTED, WILL BE ERROR FREE OR THAT WFS WILL CORRECT ALL NON-MATERIAL ERRORS.

7.4. In no event shall either party be liable for any loss of profits, loss of use, loss of data, interruption of business or indirect, special, incidental or consequential damages of any kind in connection with or arising out of this Agreement, whether alleged as a breach of contract or tortious conduct. The limitation of liability specified in this paragraph applies regardless of the cause or circumstances giving rise to such losses or damages, including without limitation, whether the other party has been advised of the possibility of damages, the damages are foreseeable, or the alleged breach or default is a fundamental breach or breach of a fundamental term.

7.5. WFS's liability hereunder for damages shall not, in any event, exceed the fees paid by Customer in the twelve (12) month period preceding which the claim arose. Such fees shall be limited to the particular Schedule to which the default relates. The limitations specified in this Section 7.5 shall not apply to a breach of the non-disclosure provisions of Section 5, the indemnification provisions of Sections 7.1, or to any death, personal injury, or damage to tangible property caused solely by the negligence or willful misconduct of WFS's staff while on-site at Customer's locations.

8. General Provisions

8.1. Each party may include the other party's name or logo in a list of its clients, vendors, or service providers. Each party may make reference to the other in an initial press release, provided that any use of the other party's trademark(s) retain proprietary notices and/or are properly attributed to their owner and also provided that any such press release will require the review and prior written consent of both parties, which shall not be unreasonably withheld, conditioned, or delayed.

8.2. In recognition of the pricing provided under this Agreement, Customer shall (subject to its reasonable right to review and approve): (a) allow WFS to include a brief description of the SaaS Service and Global Services furnished to Customer in WFS promotional materials, and (b) allow WFS to make reference to Customer in case studies, ROI analyses, white papers and related marketing materials, and (c) serve as a reference for WFS potential clients, and (d) provide interviews to the news media and provide quotes for press releases, and (e) organize mutually convenient site visits for WFS potential clients, and (f) make presentations at conferences, upon WFS reasonable request and at WFS's cost.

8.3. Any notice to be sent relating to this Agreement shall be in writing and mailed to the other party at the addresses set forth herein addressed to Legal Department, by certified mail, return receipt requested. This Agreement, including all Schedules, contains the entire agreement of the parties with respect to its subject matter, and there are no promises, conditions, representations or warranties except as expressly set forth herein. This Agreement may be modified or amended only by written instrument executed by the parties. This Agreement has been the subject of arm's length negotiations and shall be construed as though drafted equally the parties. No terms, provisions or conditions of any purchase order or other document that Customer may use in connection with this Agreement shall have any effect on the rights, duties or obligations of either party. Unless expressly stated to the contrary in any Schedule, any terms or conditions specified in the Agreement shall prevail over terms and conditions in the Schedules. Silence shall not constitute a conflict.

8.4. No term or provision of this Agreement shall be deemed waived, and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of, a breach by the other party, whether express or implied, shall not constitute a consent to or waiver of any different or subsequent breach. If a court of competent jurisdiction holds any provision of this Agreement to be illegal, unenforceable, or invalid in whole or in part for any reason, the validity and enforceability of the remaining provisions, or portions of them, will not be affected. The headings and titles provided in this Agreement are for convenience only and shall have no meaning on the terms of this Agreement. Consent is not required for an assignment of this Agreement in connection with a sale or disposition of a majority of all the assets, voting securities or equity interests of WFS, or a reorganization, merger or similar transaction of WFS. Customer may, upon notice to WFS, assign or otherwise transfer this Agreement if done in its entirety and in conjunction with a merger, consolidation or reorganization of the Customer. For assignments related to internal reorganizations of Customer, the prior, written consent of WFS shall be required, such consent not to unreasonably withheld, conditioned or delayed. This Agreement binds and inures to the benefit of the parties hereto and their respective successors and permitted assigns. The parties agree that reliable copies such as scanned or facsimile counterpart signatures are acceptable.

8.5. No action arising out of any claimed breach of this Agreement may be brought by either party more than one (1) year after the cause of action has accrued. Each party shall be liable for breaches of its Affiliates and contractors under this Agreement. Any dispute under or in connection with this Agreement or related to any matter which is the subject matter of this Agreement shall be subject to the exclusive jurisdiction of the courts of Wayne County, Michigan, and shall be governed by and interpreted in accordance with Michigan law, without regard to choice of law provisions.

8.6. EACH PARTY ACKNOWLEDGES THAT THE WARRANTY DISCLAIMERS, LIABILITY AND REMEDY LIMITATIONS, AND SERVICE LEVELS IN THIS AGREEMENT ARE MATERIAL BARGAINED FOR BASES OF THIS AGREEMENT AND THEY HAVE BEEN TAKEN INTO ACCOUNT AND REFLECTED IN DETERMINING THE CONSIDERATION TO BE GIVEN BY EACH PARTY UNDER THIS AGREEMENT AND IN THE DECISION BY EACH PARTY TO ENTER INTO THIS AGREEMENT.

IN WITNESS WHEREOF, the Parties have executed this Agreement and the Exhibits indicated below as of the Effective Date.

EXHIBITS

[x] Exhibit A – Service Level Agreement

[x] Exhibit B – Support Plan Descriptions

[x] Exhibit C – Data Security Addendum

[x] Exhibit D – Privacy Addendum

[x] Exhibit E – Data Retention Policy

[x] Exhibit F – Third Party Services

CUSTOMER		WORKFORCE SOFTWARE LLC	
Date:		Date:	
Signature:		Signature:	
Printed Name:		Printed Name:	
Title:		Title:	

EXHIBIT A – SERVICE LEVEL AGREEMENT

WFS shall provide the following service levels for the SaaS Service during the term of this Agreement.

Service Area	Service Level Commitment
Uptime Commitment	Production Environments: 99.5%
Backup Services	WFS is responsible for backup and restore of data stored in the SaaS Service. WFS shall backup all Customer Data in its entirety every seven (7) days. WFS shall backup all changes to Customer Data every twenty-four (24) hours.
Data Retention	Customer Data will be kept online for three (3) years or 30 days from end of the contracted service, whichever comes first. Upon Customer's request, WFS will retain Customer Data for a period longer than three (3) years according to the fee schedule listed in the WFS Data Retention Policy.
Disaster Recovery Time Objective	• Except as otherwise noted herein, failover of Production Environment functionality to the Disaster Recovery site will occur within five (5) hours of WFS declaring a Disaster. • Failover of WorkForce Forecasting & Scheduling Production Environment functionality to the Disaster Recovery site will occur within five (5) hours of WFS declaring a Disaster in the Amsterdam data center. • Failover of other WorkForce Forecasting & Scheduling Production Environment functionality to the Disaster Recovery site will occur within twenty-four (24) hours of WFS declaring a Disaster in the remaining data centers.
Disaster Recovery Point Objective	Maximum data loss of one-and-a-half (1.5) hours of data stored in the Production Environment.

NOTES, DEFINITIONS, AND ADDITIONAL TERMS

The following notes, definitions, and additional terms are an integral part of the Service Level Agreement.

1. "Disaster" means an event after which WFS determines the SaaS Service should be failed over to the disaster recovery site.
2. "Downtime" means the Total Minutes in the Month during which the Production Environment is not available, except for Excluded Downtime.
3. "Excluded Downtime" means Total Minutes in the Month attributable to:
    (i) Scheduled Maintenance Windows;
    (ii) SaaS Service updates;
    (iii) Content provided by Third Party Content Vendors;

(iv) Unavailability caused by factors outside of WFS's reasonable control, such as unpredictable and unforeseeable events that could not have been avoided even if reasonable care had been exercised, including, without limitation, a Force Majeure event.

4. "Month" means a calendar month.
5. "Total Minutes in the Month" are measured 24 hours at 7 days a week during a Month.
6. "Scheduled Maintenance Windows" means a window of time during which the SaaS Service may be down for maintenance, which window is (a) 3:00 am Sunday to 4:00 am Sunday U.S. Eastern Time for the US and Canada data centers (b) 3:00 am Sunday to 4:00 am Sunday Central European Time for the European data centers; (c) 3:00 am Sunday to 4:00 am Sunday Australian Eastern Time for the Asia Pacific/Australia data centers; (d) for an extended maintenance window in which case the customer will be notified at least ten (10) business days in advanced; and (e) a maintenance window scheduled with the customer to perform maintenance or updates to the customer's Production Environment.
7. "System Availability Percentage" means the average percentage of total time during which the Production Environment is available to Customer and is calculated as follows:

$$SystemAvailabilityPercentage = ((\left(\frac{TotalMinutesInTheMonth - Downtime}{TotalMinutesInTheMonth}\right) * 100)$$

8. Data collection terminals will continue to accept swipes during system downtime and swipes will be uploaded when the Online System becomes available.
9. If Customer elects to have any services provided by a third party, WFS shall have no liability for any defect or failure of the SaaS Service caused by such third-party services, and Customer shall not be entitled to any reduction in fees for the SaaS Service. WFS may deny access to the SaaS Service to any third party which WFS determines in its sole discretion poses a security risk or other risk to WFS systems, data or intellectual property.
10. Customer shall notify WFS in writing at least sixty (60) days in advance of any period when it reasonably believes the number of Active Employees or peak usage transaction volume to the SaaS Service may increase by more than 20% over the prior thirty (30) day period and at least ninety (90) days in advance if it expects more than a 50% increase. Failure to provide such notification shall release WFS of the Uptime and Support Estimated Resolution Times obligations herein for a period of ninety (90) days from the date such increase occurred.
11. The Uptime Commitment does not apply in the first thirty (30) days of use in a Production Environment, during which time WFS may need to tune the environment for Customer based on its actual usage patterns.
12. The Uptime Commitment does not apply during a Force Majeure event and shall be reinstated again only after service has been fully restored at the primary facility.
13. Access to archived or backup data, if available, will be quoted to Customer, provided as a Global Service, and may be made available as a database extract or in a separate environment.

CREDITS IF WFS FAILS TO MEET THE UPTIME COMMITMENT

If Customer provides written notice to WFS of WFS's failure to satisfy the Uptime Commitment within thirty (30) days of the end of a month, WFS will credit to Customer 2% of Monthly Subscription Fees for each 1% below SLA, not to exceed 100% of Monthly Subscription Fees.

EXHIBIT B – SUPPORT PLAN DESCRIPTIONS

A. Estimated Service Levels

Support Ticket Type	**Initial Response Times**	
Severity Level 1	1 Hour from Initial Request (24x7)**	
Severity Level 2	2 Hours from Initial Request (24x7)**	
Severity Level 3	1 Business Day from Initial Request*, **	
Support Ticket Type	**Estimated Resolution Times**	
	WorkForce Suite (excluding WorkForce Forecasting and Scheduling and DCTs)	WorkForce Forecasting and Scheduling
Severity Level 1	4 Hours from Initial Response	1 Day from Initial Response
Severity Level 2	1 Business Day from Initial Response	1 Month from Initial Response
Severity Level 3	3 Business Days from Initial Response*	2 Months from Initial Response*

*Excepting requests that require a patch or new functionality.
**Standard support Customers: 85% commitment to achieving response SLA guarantee.
**Premium support Customers: 98% commitment to achieving response SLA guarantee.

B. Severity Level Definitions

- **Severity Level 1:** Production application services are down and no workaround is immediately available. All or a substantial portion of the application or critical data is unavailable or at a significant risk of loss or corruption. Business operations have been severely disrupted. Severity 1 support requires the client to have dedicated resources available to work with WFS on the issue on an ongoing basis while the issue is active.
- **Severity Level 2:** Major application functionality is severely impaired and a temporary workaround is available. Application services are impaired however continue to function without an immediate impact to the critical components of the application. Long term issues may occur if not addressed however are not imminent. A major business milestone is at risk.
- **Severity Level 3:** All other issues not categorized as Severity Level 1 or 2. A Severity Level 3 issue is an issue that results in a non-critical loss of application services or functionality. A workaround may or may not be available that allows the user to continue to use the non-critical application functionality. Severity Level 3 does not include new enhancements to any WFS product.

C. General Plan Definitions, Hours and Availability

- Response time is the time from Customer's call into WFS until a return call is provided.
- WFS support will make analysts available for phone contact Monday through Friday from 8:00 am – 6:00 pm during the business hours observed in Customer's time zone (where Customer's headquarters are

located), excluding the holidays listed below. For the purposes of this document, those business hours will be described as “Standard Support Call Times.”

- WFS and its support staff observe public holidays of England, New South Wales or U.S federal holidays. No live support is offered to Customer on those days, except for Severity Level 1 and Severity Level 2 issues.
- WFS provides Live Phone Support coverage for critical issues outside of Standard Support Call Times as defined below:

24 x 7 Live Phone Support	
Severity Level 1	Included
Severity Level 2	Included
Severity Level 3	Will be addressed according to the Estimated Resolution Target

- WFS may modify the service levels, fees, and offerings of any Support Plan, but such changes shall not apply to the Support Plan for the current Support Period.
- WFS support will address reported “defects” to WFS applications, which result in a loss of previously available functionality and performance.
- New enhancements, including, but not limited to paycode, pay rules, accrual banks, holiday policies, etc. will be routed to WFS’s Service Request Department for completion.
- All Global Services will be directly invoiced to customer as Billable Technical Support at the applicable hourly rate after services have been rendered.
- All enhancement requests estimated over sixteen (16) hours will require the generation of a Statement of Work defining the project scope and will be assigned a WFS project manager.
- Customers selecting Standard Support are able to elect up to six (6) Support contacts and understands that a minimum of two (2) contacts must be Level 1 Certified at all times. Premium Support Customers are able to elect up to ten (10) Support contacts and understands that a minimum of two (2) contacts must be Level 2 Certified at all times.

    - Standard Support Customers are granted two (2) free registrations, based on products purchased, to:
        - Customer Certification Level 1: Time and Attendance Troubleshooting or Customer Certification Level 1: Forecasting and Scheduling Troubleshooting
    - Premium Support Customers are granted two (2) free registrations to Customer Support Level 1 courses listed above and the following Level 2 courses identified below, based on products purchased:
        - Customer Certification Level 2: Time and Attendance Configuration Maintenance or Customer Certification Level 2: Forecasting and Scheduling Administration
    - Greater than two (2) registrations, for either course, for the term of the contract are billed at market price.
    - Customers without either Standard or Premium Support Plans must pay the market price for Customer Certification courses.

- Certified Contact will be defined as support contacts that have successfully completed Level 1: Time and Attendance Troubleshooting and/or Forecasting and Scheduling Troubleshooting and/or Level 2: Time and Attendance Configuration Maintenance and/or Forecasting and Scheduling Administration.
- Customer Certification Level 1: Time and Attendance Troubleshooting and Customer Certification Level 1: Forecasting and Scheduling Troubleshooting are prerequisites for Customer Certification Level 2: Time and Attendance Configuration Maintenance and/or Customer Certification Level 2: Forecasting and Scheduling Administration respectively.
- Customer's uncertified contacts will have access to WFS support staff to report only Severity Level 1 or 2 incidences.
- Certified Contacts are required to request and approve all alterations of the Service.
- New WFS Customers: the named certified contacts shall be selected by Customer and shall complete the Customer Certification Level 1: Time and Attendance Troubleshooting or Customer Certification Level 1: Forecasting and Scheduling Troubleshooting course within one hundred eighty (180) days of the Agreement Effective Date and Customer Certification Level 2: Time and Attendance Configuration Maintenance or Customer Certification Level 2: Forecasting and Scheduling Administration within sixty (60) days of implementation "Go Live".

- Renewal Customers: the named certified contacts shall be selected by Customer and shall complete the WorkForce Certification Process within sixty (60) days of the agreement Effective Date.
- Certification remains valid for two (2) years and must be renewed within sixty (60) days of the anniversary of the certification Effective Date.
- If any of the named certified contacts are replaced by the Customer, the newly named contact(s) shall complete the appropriate WorkForce Certification Process within sixty (60) days of being selected.
- Customers electing the Premium support plan will receive a twenty (20) percent discount on WFS's standard rates for all post implementation "Go Live" Services. The foregoing discounts shall not apply to any Managed Services.
- Premium Support Plan Customers will receive a twenty (20) percent discount on VISION registration fees and one (1) Health Check Service per schedule term, as requested, starting upon the schedule effective date.

    - Health Check Service is defined as an in-depth analysis of the configuration/environment where WFS consults with the customer, conducts interviews and provides an executive summary of recommendations.

- Premium support plan Customers will be provided access to WFS's Compliance Portal.

    - Additional terms and conditions, which can be accessed via web pages from within the Compliance Portal, shall apply to Customer and remain in full effect throughout the full term of this Schedule.

D. Data Collection Terminals (if applicable)

- "DCT" shall mean the data collection terminal(s) rented or purchased under an applicable Schedule. If the DCT is rented by the Customer under a Hardware Rental Schedule, the term of the DCT Support Plan shall match the term of the rental. If the DCT is purchased by the Customer under a Hardware Purchase Schedule, the term of the DCT Support Plan shall be listed in the applicable Schedule, subject to any renewal terms.

- DCT Severity Level Definitions:
  - Severity Level 1: A critical problem that renders one or more key functions of the DCT unusable, no reasonable work around exists, and for which immediate resolution is required to meet processing deadlines.
  - Severity Level 2: Any other critical problem that renders one or more key functions unusable.
  - Severity Level 3: Any other problem with the DCT that is not at the Severity 1 or Severity 2 level.

- Both Support Plans cover the cost of parts, labor, and shipping to Customer's facility for any covered repairs for manufacturer's defects and manufacturer's workmanship of the DCT. Customer is responsible for shipping charges to WFS. To make a support claim, Customer shall first contact WFS and speak to the WFS support department. After diagnosis and upon authorization, Customer will be provided shipping instructions to return the unit to WFS for repair.

  - Under Standard Support, WFS repairs the DCT, or if in its opinion such repair cannot be made, it will provide a replacement DCT. Repairs are generally completed within 5-10 business days. WFS makes no delivery guarantees for delays caused by international shipping or customs. WFS will return units to the Customer at no charge via ground shipping. Alternate shipping methods may be selected by the Customer at an additional charge.
  - Under Premium Support, WFS ships a replacement DCT overnight at no cost to Customer the same business day (or the next business day for calls after 3 pm Eastern Time). WFS makes no delivery guarantees for delays caused by international shipping or customs. Customer ships the faulty DCT to WFS concurrently via ground shipping. If the faulty DCT is not received within ten (10) business days, Customer will be invoiced for the DCT shipped.

- The Support Plans only cover repairs or replacement units of the same type and model. If parts or replacement units are not available, a next generation DCT will be provided.
- Customer shall be responsible for all set up and maintenance of the DCT's on Customer site. WFS will not provide installation assistance under either Support Plan.
- Notwithstanding anything to the contrary contained herein, in no event shall any Support Plan for DCT extend or be effective beyond six (6) years from the Effective Date except upon mutual agreement of the parties.
- Discounts and replacement options do not apply to IVR systems. Contact WFS for additional information on IVR.
- Normal wear and tear and intentional damage to equipment is excluded and fees for such DCTs will be chargeable to Customer at WFS's standard charges for parts and labor upon receipt of any such DCT.

WFS makes no representations on the availability of parts or replacement units. WFS reserves the right to deliver new DCTs, repaired DCTs, or refurbished DCTs at its option for any covered repair. WFS's obligation shall be subject to our determination that the DCT has not been modified, serviced, or repaired by any other party and that the product was installed and operated within the product specifications for its intended use. Any misuse, negligence, accident, abuse, or alteration of a serial number will void the support obligations. The Support Plan extends solely to the original purchaser of the DCT and all claims must be made by the Customer.

- THE SUPPORT PLAN EXPRESSLY PROVIDED HEREIN IS THE SOLE WARRANTY AND OBLIGATION OF WFS WITH RESPECT TO THE DCT. ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED ARE HEREBY DISCLAIMED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL WFS BE LIABLE FOR ANY LOSS OR INJURY TO EARNINGS, PROFITS, OR GOODWILL OR FOR ANY SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, EVEN IF WFS IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. WFS'S LIABILITY SHALL IN ANY EVENT BE LIMITED TO THE REPAIR, REPLACEMENT, OR IF NEITHER IS FEASIBLE, A REFUND OF THE RENTAL FOR THE PERIOD THE DCT IS NOT FUNCTIONING OR THE PURCHASE PRICE OF THE DCT AS APPLICABLE.
- The Support Plans provide for full intellectual property indemnification of Customer for the DCT and the DCT Software while under support, per the indemnification provisions of the Agreement.

EXHIBIT C - DATA PROTECTION

WFS will adhere to best practice standards in security risk management for the SaaS Service.

1. Data Protection Planning and Management

1.1. Data Protection Program - WFS will implement and maintain a data protection strategy, program, policies, and initiatives to ensure the security, privacy and relevant regulatory requirements are updated and met consistently.

1.2. Risk Assessment and Treatment - The Information Security function in association with the Legal function will have developed an enterprise-wide risk management program that integrates governance, risk management, and compliance at all key operational levels such as: security, privacy, regulatory requirements, business operations, customers' requirements, etc.

1.3. Data Protection Policies - WFS will develop and implement data protection policies and standards that apply to all employees, contractors, part-time and temporary workers to perform work on company premises.

1.4. Security and Privacy Awareness Training Program - An awareness training methodology will be in place to ensure that WFS's policies and standards are being adhered to by employees, contractors, part- time and temporary workers.

1.5. Code of Conduct and Acceptable Use Policy - WFS will ensure that all employees, contractors, part-time and temporary workers processing, having access to, or managing Customer data as well as working directly with customers adhere to a Code of Conduct and Acceptable Use Policy.

1.6. Regulatory Requirements and Industry Best Practices - WFS will exercise due diligence to ensure compliance with various regulatory requirements. In addition, WFS will provide Customer evidence of compliance with SSAE 16, SOC 2 and other industry standard requirements as applicable.

1.7. WFS will ensure that its data protection program includes the use of appropriate vulnerability scanning tools and techniques to scan for vulnerabilities in its information systems that impact Customer data. Scanning activities will be scheduled to avoid interference with Customer' operations and network traffic.

2. Physical and Environmental Security

2.1. Alternate Secure Site - WFS will identify an alternate secure site for the storage of information system backup media.

2.2. Physical Access Points - WFS will control all physical access points (including designated entry/exit points) to facilities containing information systems and issues appropriate authorization credentials for personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible). WFS will ensure that third-party colocation providers meet WFS minimum standards for access security, but that actual management of that security will be performed by the colocation provider.

2.3. Eavesdropping prevention - WFS will control, using commercially reasonable standards, the physical access to information system transmission lines carrying unencrypted or unencrypted information to prevent eavesdropping, in-transit modification, disruption, or physical tampering.

3. Operational Procedures and Responsibilities

3.1. Change Management - WFS will use commercially reasonable standards to manage changes to information systems within our control.

3.2. Separation of Duties - WFS's information system will enforce separation of duties through assigned access authorizations.

3.3. Malicious Software Prevention - Appropriate controls (anti-virus software, anti-malware, patch management) will be implemented to detect, remove and to prevent the introduction or spread of unauthorized software, malicious software, and other malware.

3.4. Backup Management - WFS will adhere to best practice standards with regards to backups of data and information systems. Backups will be recovered in a timely manner in case of system failures.

3.5. Media Management - Appropriate controls over media creation, storage and disposal will be in place to protect Customer data from unauthorized access.

4. Network Security Management

4.1. Attack Prevention - WFS will employ adequate measures to protect the networks hosting information systems against or limit the effects of attacks by unauthorized users.

5. Online Transactions – Data Encryption

5.1. Encryption Mechanisms - Controls to ensure the use of encryption mechanisms, preventing unauthorized disclosure of information, will be used by WFS to satisfy data protection requirements. Such controls will ensure data is protected while being transmitted and at rest unless protected by alternative physical measures.

6. Online Transactions – Information Integrity

6.1. Unauthorized Changes - WFS's information system will use its best efforts to protect against unauthorized changes to information.

7. Monitoring

7.1. Access Monitoring – Authorized and unauthorized access to WFS's information system will be monitored.

8. Access Control

8.1. NDA - All contractors, consultants, and temporary employees of WFS will sign the WFS Non-Disclosure Agreement.

8.2. Account Review – WFS will review user accounts accessing customer data on a regular basis. Frequency will be based on application risk and data classification. Inactive accounts will be deactivated following WorkForce Software policies and standards.

8.3. Separation of Duties - WFS's information system will use commercially reasonable efforts to enforce separation of duties through assigned access authorizations.

8.4. Least Privilege - The information system will use commercially reasonable efforts to enforce the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.

8.5. Need-to-know Only Principle - WFS will use commercially reasonable efforts to ensure that the use of data by end-users is based on the need-to-know only principle.

8.6. Password Use - All WFS users will be required to change passwords, avoiding re-using or cycling old passwords, and at regular intervals of 90 days or whenever there is any indication of possible system

or password compromise. Users will be trained to keep passwords confidential. There will be no sharing of user accounts and passwords among employees, contractors, part-time and temporary workers.

8.7. Unattended User Equipment - WFS's information system will provide mechanisms for locking sessions either user initiated or automatically controlled by locking the session after a maximum of 15 minutes of inactivity.

8.8. Privileged Password Management - Privileged access for network, system or application functions in production system will be controlled and restricted to as few personnel as operationally feasible. Default password or other embedded security bypass mechanism from manufacturer will be changed or disabled.

9. Information Systems Acquisition, Development and Maintenance

9.1. Continuous Monitoring - Information resources will be used to identify and maintain awareness of relevant technical vulnerabilities.

9.2. Periodic Maintenance - WFS will schedule, perform, and document routine preventative maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or agreed to Customer requirements.

10. Information Security Incident Management

10.1. Incident Response Procedures - WFS will develop, implement and maintain formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

10.2. Incident Response Notification - WFS will inform Customer of a security or privacy breach within 24 hours of confirmation of said breach.

11. Business Continuity Management

11.1. Contingency Plan - WFS will have a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals, and activities associated with restoring the system after a disruption or failure.

11.2. Contingency Planning Procedures - WFS will develop, implement and maintain formal, documented procedures for contingency planning and associated controls.

EXHIBIT D – PRIVACY COMMITMENTS

Our privacy program governs how we collect, use and manage customers' information – ensuring the confidentiality of Personally Identifiable Information stored and processed in our products, as well as protecting and securing that information.

DEFINITIONS

"Personally Identifiable Information" or "PII" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data. The customer is the Data Controller.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. WFS is the Data Processor.

1. Notice
   Personally Identifiable Information stored and processed using our cloud-based products, such as WorkForce Suite and WFS Suite are uploaded and processed by the Customer, who owns all title, rights, and interest to that data. WorkForce Software does not collect or personal data for its own use in our cloud-based products.

   Customers are responsible for complying with any regulations or laws that require providing notice, disclosure and/or obtaining consent prior to transferring the data to WorkForce Software for processing purposes. WorkForce Software is not responsible for providing notice, disclosure and/or obtaining consent prior to the customer transferring the data to WorkForce Software for processing.
2. Choice
   WorkForce Software retains PII according to the timeframes set forth in the relevant Customer agreement. Individuals who would like to request that their personal data not be used for specific purposes or disclosed should contact the Customer. The customer is responsible for determining if opt-in or opt-out options are required for its employees.
3. Accountability for Onward Transfer
   WorkForce Software processes Customer Data under the direction of its Customers, and has no direct control or ownership of the PII it processes. WorkForce Software will not transfer PII to third-parties without first receiving written permission from the customer.

4. Security
   WorkForce Software will take reasonable and appropriate measures to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. Data Integrity and Purpose Limitation
   In the normal course of using the WorkForce Software SaaS Service, Customers will input electronic data into the WorkForce Software systems ("Customer Data"). The use of information collected through our service shall be limited to the purpose of providing the service for which the Customer has engaged WorkForce Software. WorkForce Software may access Customer Data for the purposes of providing the Service, preventing or addressing service or technical problems, responding to support issues, responding to Customer's instructions or as may be required by law, in accordance with the relevant agreement between Customer and WorkForce Software.

   WorkForce Software will not process PII in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the customer.

6. Access
   Individuals who seek access or who seek to correct, amend or delete inaccurate data uploaded and maintained by the customer should contact the Customer. The customer is responsible for correcting, amending, or deleting that personal information where it is inaccurate. In some instances, the Customer may have enabled the individual to perform these updates themselves through the WorkForce Software cloud-based product. If the Customer requests WorkForce Software to modify or remove the data to comply with data protection regulations, WorkForce Software will respond to the Customer's request within 30 days.

   WorkForce Software will refer any request for disclosure of personal data by a law enforcement authority to the Customer. WorkForce Software may, where it concludes that it is legally obligated to do so, disclose personal data to law enforcement or other government authorities. WorkForce Software will notify Customer of such request unless prohibited by law

7. Recourse, Enforcement and Liability
   WorkForce holds its employees and agents accountable for maintaining the trust that our customers place in our company. WorkForce will conduct periodic assessments to validate its continued adherence to this privacy policy.

   In the case that WorkForce obtains knowledge of use or disclosure of information not in accordance with the Web Privacy Policy, WorkForce will take the following reasonable steps to stop the use or disclosure:

   1. WorkForce Software will formally contact the relevant party and instruct them to stop using the data inappropriately and/or destroy the data. WorkForce Software will advise the relevant party on appropriate use and disclosure of information in accordance with the Privacy Policy.

2. If the relevant party continues to use or disclose the information inappropriately, WorkForce Software will take legal actions to prevent the continued misuse of information. WorkForce Software will also remove the information from its database to prevent further misuse."

Any privacy disputes that arise between the customer and a customer employee must be resolved by the customer.

If you have any questions or concerns regarding these privacy commitments, please contact us.

Privacy Compliance Officer
WorkForce Software, LLC
38705 7 Mile Road, Suite 300
Livonia, MI 48152
Phone: 877.493.6723
Email: privacy@workforcesoftware.com

EXHIBIT E - WORKFORCE DATA RETENTION POLICY

WorkForce Software will retain only three (3) years of Customer Data in the SaaS environment. WFS Customers will be notified ninety (90) days prior to the data purge operation. If the Customer does not confirm acceptance of the data purge prior to the end of the ninety (90) days, WorkForce Software shall not purge the data and shall instead charge the Customer data storage fees according this policy but on a monthly basis, to be invoiced monthly in arrears. Customer shall be required to give thirty (30) days' written notice prior to terminating the data storage service herein. Options for Customers who desire to retain their historical data are listed below:

1. Customers may request from WorkForce Software a backup of their data prior to the purge operation, in a mutually agreed upon format and delivery method or a standard CSV formatted data dump which they may download and retain via SFTP no more than once per year at no cost.
2. Customers may elect to have WorkForce Software retain their data online in the SaaS environment for an incremental five percent (5%) per year of their annual SaaS subscription. For example, for years 1 to 3 the cost to the customer to store all production data is included in the standard SaaS fees. For each subsequent year the customer will pay an incremental five percent (5%) per year for additional data retained. Therefore, a customer for whom WorkForce Software retains 7 years of data will pay an additional 5% for year 4, 10% for year 5, 15% for year 6, 20% for year 7 over their standard SaaS fee.

EXHIBIT F – THIRD PARTY SERVICES

1. Definitions

1.1. "Regulatory Content and Data" means legal or regulatory content, reference materials, or data supplied by Third Party Content Vendors as a function of select optional Third Party Services.

1.2. "Third Party Content Vendors" means CCH Incorporated, its licensors and Affiliates, and any other firm which provides regulatory content, data or legal reference materials in the SaaS Service.

1.3. "Third Party Services" means term-based ancillary services provided by third parties which may involve internet or phone delivery including, but not limited to, the Regulatory Update Service, Compliance Portal, IVR, Text Messaging and Mobile Services and which, if ordered by Customer, will be included on an applicable Schedule. Third Party Services shall be governed by this Exhibit F. Terms of this Exhibit F supersede the terms in the Agreement with regards to any Third Party Services.

2. Terms and Conditions

2.1. WFS shall provide access to the Third Party Services specified in the Schedules for the term specified and for the fees indicated. Any usage of the Subscription Service in excess of the amounts specified in the Schedules shall be billed to the Customer as incurred at 125% of the unit prices specified in the Schedule. Third Party Services are non-cancelable and non-refundable for the term specified. At the end of the term specified, the Third Party Services shall automatically renew for additional one-year periods unless either party provides written notice to the other at least sixty (60) days prior to the end of the then current term. The per-unit pricing during any such renewal term increase by 5% per year over the base prices listed in the Schedules for the relevant services in the immediately prior term. Customer may be required to use a compatible version of the SaaS Service to access the Third Party Services. Such use of the Third Party Services shall be restricted to Customer's employees, contractors, and other authorized users and Customer shall take necessary steps to prevent unauthorized use of the Third Party Services by third parties using its passwords and shall be liable for any such unauthorized use.

2.2. Third Party Services, including the Leave Regulation Update Service, may involve services and materials provided by third parties ("Third Party Services" and "Third Party Providers" respectively) including legal and related content (the "Regulatory Content"). The Regulatory Content may be provided by the Third Party Providers and/or by WFS. Access to the Regulatory Content and Third Party Services may involve additional terms and conditions, which can be accessed via the web pages of the Third Party Providers. WFS will make commercially reasonable efforts to communicate any policies, requirements, or guidelines of those third parties to Customer. Customer agrees to be bound to such additional terms and conditions. ANY ACTUAL OR ALLEDGED VIOLATION OF A THIRD PARTY POLICY, REQUIREMENT, OR GUIDELINE BY CUSTOMER MAY RESULT IN A TERMINATION OF SERVICE AND IS CUSTOMER'S RESPONSIBILITY.

2.3. Customer acknowledges that the Third Party Service may be subject to limitations, delays, and other problems which are beyond the control of WFS and that WFS shall have no liability for any delays, failures, or unavailability resulting from such problem. Notwithstanding anything else in this Agreement, in the event that a Third Party Service fails or is not available, WFS sole and exclusive liability of WFS in any way related to such unavailability of the Third Party Service will be to return

the fees paid for the Third Party Service for the period of time the service was unavailable. This Section survives the termination of the Agreement.

2.4. Notwithstanding anything else in the Agreement, including, but not limited to, claims for breach of confidentiality and data security, or Intellectual Property Right infringement, (a) WFS and Third Party Providers shall have no liability whatsoever for the Regulatory Content and Third Party Services and does not provide any warranties, (b) WFS assumes no responsibility regarding Customer Data used in any text messages as part of a Third Party Service. Customer understands that such data will not be encrypted, and agrees to not send Social Security numbers, national identification numbers, payroll information, or other data considered sensitive in nature via text messages, (c) the Regulatory Content and Third Party Services are the copyrighted materials of WFS, the Third Party Providers or its licensors and they exclusively reserve all rights and interests in such, and (d) THE THIRD PARTY PROVIDERS SHALL HAVE NO LIABILITY TO THE CUSTOMER, AND (e) THE REGULATORY CONTENT AND THIRD PARTY SERVICES ARE PROVIDED ON AN "AS, IS" BASIS AND WITHOUT ANY WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AND (f) THE THIRD PARTY PROVIDER AND WORKFORCE DISCLAIM ALL WARRANTIES WITH RESPECT TO THE REGULATORY CONTENT AND THIRD PARTY SERVICES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, UNINTERRUPTED USE, TITLE, QUIET ENJOYMENT AND INFORMATION COMPLETENESS, CURRENCY OR ACCURACY. TO THE EXTENT SUCH DISCLAIMER CONFLICTS WITH APPLICABLE LAW, THE SCOPE AND DURATION OF ANY APPLICABLE WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. This Section survives the termination of the Agreement.

2.5. Access to the Compliance Portal (if ordered by Customer) may involve additional terms and conditions, which can be accessed via web pages from within the Compliance Portal. If Customer does not agree with such additional terms and conditions within thirty (30) days of delivery of the Compliance Portal, it may terminate the order for the Compliance Portal and WFS shall return all fees related to the Compliance Portal.

3. Additional Terms and Conditions – Text Messaging Services

3.1. WFS is not responsible for any fees incurred as a result of text messages received by Customer employees regardless of whether or not such employees authorize the use of the text messaging service. WFS shall not be responsible for the content of any text messages sent to Customer employees. Customer shall indemnify and hold harmless WFS against all employee claims resulting from Customer's use of the text messaging service.

3.2. Customer shall not attempt to use the Text Messaging Services to access or allow access to Emergency Services. WFS and the Third Party Provider disclaim all liability arising from such use. Neither WFS nor its Third Party Provider and representatives will be liable under any legal or equitable theory for any claim, damage, or loss arising from or relating to the inability to use the Text Messaging Services to contact emergency services. Customer shall ensure that the Text Messaging Services provided hereunder are used in accordance with all applicable laws, regulations and third party rights, as well as the terms of this Agreement, including the Third Party Provider's Acceptable Use Policy, which is hereby incorporated into this Agreement and any data protection statute, regulation, order or similar laws. Except as allowed by applicable law, with respect to any software provided to Customer hereunder, Customer will not reverse engineer, decompile, disassemble or otherwise create, attempt to create or derive, or permit or assist any third party to create or derive the source code of such software.

3.3. WITHOUT LIMITING WFS'S EXPRESS OBLIGATIONS HEREUNDER, WFS AND THE THIRD PARTY PROVIDER HEREBY DISCLAIM ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE AND WARRANTIES RELATED TO THIRD-PARTY EQUIPMENT, MATERIAL, SERVICES, OR SOFTWARE. TEXT MESSAGING SERVICES AND PROPERTIES ARE PROVIDED "AS IS" TO THE FULLEST EXTENT PERMITTED BY LAW.

3.4. WFS and/or Third Party Providers exclusively own and reserve all right, title and interest in and to the Text Messaging Services and related materials provided by WFS or Third Party Provider. All terms and conditions contained within the Agreement related to ownership and confidentiality shall extend equally to the property and information of Third Party Providers.

3.5. EXCEPT FOR LIABILITY ARISING FROM VIOLATIONS OF SECTION 3.1, 3.2, OR SECTION 3.4 OF THIS EXHIBIT, UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, WILL WFS, CUSTOMER OR THIRD PARTY PROVIDERS BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY CHARACTER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, LOST PROFITS, LOST SALES OR BUSINESS, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOST DATA, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES, EVEN IF SUCH PARTY HAS BEEN ADVISED, KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES.

3.6. EXCEPT AS DESCRIBED IN THIS SECTION 3.6, UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, WILL WFS OR THIRD PARTY PROVIDER BE LIABLE TO CUSTOMER FOR ANY DIRECT DAMAGES, COSTS, OR LIABILITIES IN EXCESS OF THE AMOUNTS PAID BY CUSTOMER FOR THE TEXT MESSAGE SERVICES DURING THE TWELVE MONTHS PRECEDING THE INCIDENT OR CLAIM. THE FOREGOING LIMITATION WILL NOT APPLY TO EITHER PARTY'S OBLIGATIONS UNDER SECTION 3.4 OF THIS EXHIBIT.

3.7. THE PROVISIONS OF THIS EXHIBIT ALLOCATE THE RISKS UNDER THIS AGREEMENT BETWEEN THE PARTIES AND THE PARTIES HAVE RELIED ON THE LIMITATIONS SET FORTH HEREIN IN DETERMINING WHETHER TO ENTER INTO THIS AGREEMENT.