EMPLOYER SERVICES AGREEMENT
BY AND BETWEEN
VOYA RETIREMENT INSURANCE AND ANNUITY COMPANY
AND
San Bernardino County ("EMPLOYER")

Effective Date: September 26, 2023

This EMPLOYER SERVICES AGREEMENT (the "Agreement") is effective as of September 26, 2023 (the "Effective Date"), between Voya Retirement Insurance and Annuity Company ("Voya"), a corporation organized and existing under the laws of the State of Connecticut, directly and on behalf of its Affiliates, and San Bernardino County ("Employer"). Voya and Employer are each referred to as a "Party" and collectively as the "Parties" under this Agreement.

WITNESSETH:

WHEREAS, the Employer sponsors a Health Reimbursement Arrangement, as identified on Exhibit A, that is qualified under Sections 105 and 106 of the Internal Revenue Code of 1986; and

WHEREAS, the Employer wishes to engage Voya as an administrative service provider to facilitate the administration of the HRA by providing administrative services; and

WHEREAS, Voya agrees to provide the services set forth in this Agreement; and

WHEREAS, the Parties desire to enter into an agreement to set forth their respective rights, duties and obligations with respect to the delivery of such services.

NOW, THEREFORE, in consideration or the mutual promises and covenants contained herein, it is hereby agreed as follows:

Section 1 – Definitions

When these terms are capitalized in the Agreement they have the meanings set forth below. The words may be singular or plural.

"**Account**" means the participant's HRA (as defined below) administered using the Application or Services.

"**Affiliate**" means entities that currently exist or are later acquired that, directly or indirectly, (i) control, (ii) are controlled by, or (iii) are under common control with Voya or the Employer. An entity will be deemed to control another entity if it has the power to direct or cause the direction of the management or policies of such entity, whether through the ownership or voting securities, by contract, or otherwise.

"**Application**" means the web-based software application(s) and supporting services described in the Application Exhibit(s) attached hereto. For purposes of this Agreement, the singular "Application" refers to all web-based software applications to which the Employer and/or the Participant is granted access.

"**ERISA**" means the Employee Retirement Income Security Act of 1974, as amended, and its associated regulations.

"**HRA**" means Health Reimbursement Account or Arrangement sponsored by the Employer.

"**IRC**" means the Internal Revenue Code of 1986, as amended from time to time, and the regulations promulgated thereunder.

"**IRS**" means the Internal Revenue Service.

"**Participant**" means a person who has established and maintains an Account under the HRA. It is the Employer's sole responsibility to notify Voya when a Participant becomes eligible to make claims for reimbursements pursuant to Section 6.1.

"**PHI**" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, as applied to the information created, received, maintained or transmitted by Voya or its subcontractors from or on behalf of the HRA.

"**Service Fees**" shall include the fees set forth in Exhibit C to the Agreement.

"**Services**" means administrative services as set forth on the Exhibit(s) that assist with processing and administration of Accounts and/or benefit plans/programs and includes the business processes used to deliver the Services.

"**Systems**" means the systems Voya owns or makes available to Employer to facilitate the transfer of information in connection with this Agreement.

Section 2 - Services

Section 2.1 Services. Voya, its Affiliates and its designated subcontractors will perform Services for the HRA as described herein in Exhibit B. All rights granted to, and all benefits received by, the Employer pursuant to this Agreement will extend to Employer's Affiliates.

Section 2.2 Voya's Provision of Services. Voya has subcontracted with (1) Benefit Plan Administrative Services ("BPAS") to provide systems, plan administration, contribution processing, and recordkeeping for the Services; and (2) WEX Health to provide claims processing technology and related services ("WEX"). In addition to BPAS and WEX, Voya may enter into one or more subcontracting agreements in connection with the performance of the

Services under this Agreement (together with BPAS and WEX, each, a “Subcontractor,” and collectively, the “Subcontractors”). Voya may also substitute another subcontractor for BPAS and/or WEX by providing advance written notice to Employer. Voya shall remain responsible for the performance of any Subcontractor. All references to Voya in this Agreement and Exhibits shall be deemed to include a Subcontractor unless otherwise specifically noted.

Section 3 - Employee Benefit Plans

Section 3.1 Responsibility for the Employer’s HRA. Any references in this Agreement to Voya "administering” the HRA or the Accounts are descriptive only and do not confer upon Voya anything beyond certain agreed upon ministerial duties being provided by Voya. Employer accepts total responsibility for its HRA for purposes of this Agreement, including its benefit design and compliance with any laws that apply to Employer or the HRA.

Section 3.2 Employer Initiated HRA Changes. Employer must provide Voya with written notice of any changes to the Employer’s HRA within sixty (60) calendar days prior to the effective date of the change to allow Voya to determine if such change will alter the Services Voya provides under this Agreement. Any material change in the Services must be mutually agreed to in writing by the Parties. For the avoidance of doubt, any changes to the HRA that do not alter the Services or Service Fees hereunder may be agreed to by the Parties via electronic communication, or such other form of written communication to which the Parties agree. Voya will notify Employer if (i) the change increases Voya’s cost of providing Services under this Agreement or (ii) Voya is reasonably unable to implement or administer the change. If the Parties cannot agree to a new Service Fee within thirty (30) days of the notice of the change, or if Voya notifies the Employer that Voya is unable to reasonably implement or administer the change, Voya shall have no obligation to implement or administer the change.

Section 3.3 HRA Consistent with this Agreement. By entering into this Agreement, Employer certifies that Voya’s Services will not conflict with the terms of any plan document, summary plan description, insurance policy, group funding agreement, or other applicable documents governing the HRA.

Section 3.4 Employee Communications. Before distributing any communications describing the HRA, Employer will provide Voya with copies of any such communications that refer to Voya or the Services prior to distributing these materials to Employer’s employees or third parties. Voya will provide any corrections or comments to the Employer in writing within a commercially reasonable time period after receipt. Employer agrees to amend the materials or communications if the references to Voya are not accurate, or any provision is not consistent with this Agreement or the Services that Voya is providing. Voya will not be bound by any communication that has not been reviewed and approved by Voya.

Section 3.5 Affiliated Employers. Employer represents that Employer and any of Employer's Affiliates covered under the HRA make up a single "controlled group" as defined by Section 1563 of the IRC and the regulations thereunder. Employer agrees to provide Voya with a list of Employer's Affiliates covered under the Plan upon request.

Section 4 - Employer's Responsibilities

Section 4.1 Information Employer Provides to Voya. Employer will inform Voya which of Employer's employees, their dependents and/or other persons are Participants. This information must be accurate and provided to Voya in a timely manner and in the format and specifications prescribed by Voya. Employer agrees to provide Voya (or cause Employer's vendor to provide Voya) with all information that Voya reasonably requires to provide Employer's Participants with the

Services as described in accordance with Exhibit B. Employer will notify Voya of any change to this information as soon as reasonably possible. Voya will be entitled to rely on the most current information in Voya's possession regarding eligibility of Participants in paying benefits from the Accounts and providing other Services under this Agreement. Voya shall not be responsible or liable for acts or omissions made in reliance on erroneous data provided by the Employer or any other person, including any Participant, or for the failure of Employer to perform its obligations under this Agreement. Any retroactive eligibility changes which impact claims for benefits from the Account will be mutually agreed upon by the Parties. If Voya agrees to make retroactive eligibility changes, additional reasonable Service Fees may apply, as mutually agreed. The Employer shall also ensure payroll data processors provide timely, accurate and complete data files in the prescribed electronic data file format and method specified by Voya or a Subcontractor, as applicable, in accordance with the Operating Procedures set forth in Exhibit E.

Section 4.2 Employer as Plan Administrator. The Employer or its delegate will exercise all discretion, control and authority with respect to the disposition of the HRA plan assets and the available benefits under the HRA.

Section 4.3 Employer's Administrative Responsibilities. The Employer shall ensure that any plan documents and any other documentation, as applicable, relating to the HRA are appropriately completed, are in compliance with HRA requirements and all applicable law, and are appropriately and timely adopted. The Employer shall provide Voya with a current copy of such documents governing the administration of the HRA. The Employer shall be responsible for distributing summary plan descriptions, summaries of material modifications and all other plan documentation to Participants and other individuals on a timely basis. If the Employer chooses to use the Health Reimbursement Account specimen plan document provided by Voya, then it is the Employer's responsibility to ensure that the specimen plan document complies with applicable state law. Employer acknowledges that Voya (and its affiliates and subcontractors) are not authorized to provide legal or tax advice and no service, communication or other act or omission by Voya should be construed as legal or tax advice.

Section 4.4 Notices to Participants. Employer will give Participants the information and documents they need to obtain benefits under the Plan within a reasonable period of time before benefits under the Plan begins. In the event this Agreement is terminated, Employer will notify all Participants that the Services Voya is providing under this Agreement are discontinued. Employer agrees that if it becomes unable to pay claims as they become due in accordance with this Agreement, it will promptly notify participants.

Section 4.5 Escheatment. Employer is solely responsible for complying with all applicable abandoned property or escheat laws, making any required payments, and filing any required reports. Voya shall provide its standard reports to Employer in order to support Employer's escheatment process, if applicable.

Section 4.6 Tax Reporting. If applicable, Employer is solely responsible for any W-2 and any other tax reporting to the IRS regarding any Account. Voya and its Affiliates do not assume any responsibility for compliance with federal or state laws, including federal tax laws and regulations, applicable to the Employer or the HRA.

Section 4.7 Employer Direction. In the course of providing the Services, Voya may receive written or oral instructions or directions from representatives of the Employer, including its legal counsel (hereinafter collectively referred to as "Employer Directions"), concerning the provision of Services. Employer Directions may include, but shall not be limited to, (i) approval of Voya's choice of methodology or approach to providing the Services; (ii) interpretation of any provision of the HRA; (iii) instructions concerning compliance with applicable laws and regulations; (iv) instructions concerning compliance with subpoenas or other legal process; and (v) notices concerning adjudication of Participants' claims for

benefits. Exhibits B and C and the elections made by the Employer in the HRA Questionnaire shall be deemed to be a standing Employer Direction.

Section 4.8 Reliance. Voya may rely upon and comply with any Employer Direction in performing its obligations under this Agreement. If and to the extent that Voya acts or fails to act as a result of reasonable reliance upon any Employer Direction or any information, data, document or instrument supplied by Employer or a Participant, Voya shall be relieved of any liability arising therefrom and such act or failure to act shall not constitute a default, breach or nonperformance of any warranty or obligation of Voya contained in this Agreement; provided, however, that Voya shall not be relieved of any liability arising out of or resulting from dishonest, fraudulent, or criminal acts of Voya's employees, acting alone or in collusion with others. If Voya requests instruction or direction from Employer and does not receive an Employer Direction in a timely manner, Voya shall be deemed not to have breached this Agreement with respect to any act or failure to act undertaken in good faith relating to the instructions requested.

Section 4.9 Conflict with Agreement. If any Employer Direction is inconsistent with or conflicts with any provision of this Agreement, Voya may, at its discretion, require that such Employer Direction be confirmed in writing (via email or otherwise) by an authorized representative of Employer.

Section 5 – Investment Options

Section 5.1 Selection of Investment Options. Employer shall be solely responsible for the selection of all investment options available to Participants in the HRA. Voya shall have no responsibility or discretion under the terms of this Agreement for the prudence, selection or oversight of any investment options available to Participants in the HRA. Employer acknowledges and agrees that (i) all investment information or investment materials that may be provided to Employer are provided to enable Employer to independently assess available options and make investment decisions for the Plans and (ii) the provision of any such information or materials is not intended to constitute nor should it be construed as the provision of investment advice or investment recommendations by Voya with respect to any investment option that Employer may consider making available under the Plans. Participants shall have the ability to choose their investment allocations and to make participant-directed transfers between investment options, subject to any limitations of the investment platform.

Section 5.2 Investment Advice. Neither Voya nor any of its Affiliates is an investment advice fiduciary (as defined under ERISA, as applicable, or applicable state law) with respect to the Participants nor will Voya or its Affiliates provide any investment advice to the Participants or be responsible or liable for the investment decisions of the Participants. Voya is not giving, and shall not be deemed to have given, the Employer or a Participant legal, tax, or financial advice concerning any of the matters relating to this Agreement or the HRA.

Section 5.3. Modifications to Investment Options. In order to confirm an investment option selected by the Employer can be recordkept, the addition or removal of any investment option to the Plan requires at least sixty (60) calendar days advance written notice of the proposed change in a format prescribed for the process. The change must be mutually agreed and will be made in accordance with a mutually agreed upon schedule for implementing the change. In the event the investment option is not currently traded by the investment platform, the investment option will be made available to implement within sixty (60) days after the execution of a new fund agreement between the Subcontractor and the mutual fund company. The Employer is responsible for reviewing all requirements and restrictions imposed by the mutual fund company and verifying that requirements and restrictions will be met.

Section 6 – Services and Error Correction

Section 6.1 Employer Eligibility Determinations. As set forth in Section 4.1, the Employer, in its sole discretion, shall determine which individuals are eligible to participate in the HRA and shall provide Voya with timely, accurate, and complete initial and ongoing enrollment and eligibility data in

the electronic data file format prescribed by Voya. Such information shall include, but is not limited to, the number and names of individuals eligible for and covered under the HRA, eligibility for making claims for benefits, and any other information determined by Voya to be necessary to provide the Services. Voya shall process initial and ongoing enrollment and eligibility data submitted by the Employer in the format and specifications prescribed by Voya during the implementation process. Voya shall also process enrollment data and benefit elections submitted by the Employer through proper methods established by Voya. The Employer shall provide timely notifications regarding a Participant's eligibility to make claims for benefits.

Section 6.2 Voya's Responsibilities. Voya shall provide certain Services in connection with the HRA. Accordingly, the Employer authorizes Voya to use Voya's standard procedures for the provision of Services that have been designed to ensure that the administration of the HRA. Voya shall not have discretionary authority or discretionary controls respecting any aspect of plan administration or the management of any trust fund and shall not have authority to exercise, nor exercise, any control respecting management and shall not render investment advice with respect to any money or other property of any trust fund.

Section 6.3 Business Associate Agreement. All handling and processing of PHI shall be subject to and comply with the Business Associate Agreement attached herein as Exhibit F ("BAA"). In the event of a conflict between the terms and conditions of the BAA and the terms and conditions of this Agreement, the terms and conditions of the BAA shall govern. Voya shall, with respect to any PHI: (1) comply with the BAA; (2) make no attempt to identify PHI that has been fully or partially de-identified (such as encoded data); and (3) not contact the individuals to whom the PHI pertains except to the extent it is permitted to do so under this Agreement or the BAA.

Section 6.4 Claims Processing. Voya shall process reimbursement claims and appeals in the manner required under the Plan document, or to the extent a claims procedure is not provided for in the Plan document, Voya's claims procedure. Voya is not responsible for processing any appeal of any claim beyond the first level appeal. The Employer is responsible for accepting the auto adjudication procedures to be used in connection with certain payments to be made using the stored value card technology. Voya will process payments of claims and other requests for payment according to requirements specified by IRS regulations. Neither Voya nor its Affiliates have any discretionary authority or control relating to the administration of any Employee Benefit Plan.

Section 6.5 Payments. Voya shall issue payments for HRA-eligible expenses on behalf of a Participant directly to the health provider or shall issue a reimbursement payment for HRA-eligible expenses through either check or direct deposit to the Participant, as directed by the Participant. Voya will process debit card transactions and authorize payments made directly to approved payees (e.g., health care providers, drugstores or qualifying merchants) via a debit card, if requested by the Employer.

Section 6.6 Services/Changes. The Services provided by Voya are generally described in Exhibit B. Any changes to such Services require the written consent of both Parties.

Section 6.7 Error Correction.

6.7.1 Voya Error. Voya shall promptly notify Employer after becoming aware of an error resulting from the acts or omissions of Voya's computer system malfunctions, its staff errors or otherwise caused by Voya's negligent acts. Voya shall make a good faith effort to correct any such error as soon as reasonably practicable after identification of the error and, where applicable, Employer's determination or approval of the correction to be applied to such error. Voya processes investment instructions on an "omnibus" or aggregated basis. If Voya's correction of a Voya processing error results in a loss to the HRA or its Participants, Voya will absorb the loss. If any gain results in connection with the correction of a Voya processing error, Voya will net any such gain against other losses absorbed by Voya and retain any

resulting net gain as a component of its compensation for transaction processing services, including its agreement to make Plan and Participant Accounts whole for losses resulting from Voya processing errors.

6.7.2 Employer Error. Employer shall promptly notify Voya after becoming aware of an error resulting from the acts or omissions of Employer, its agents or third parties, or otherwise caused by the negligent acts of Employer, its agents or third parties. Voya will attempt to correct such errors at Employer's expense, which shall be agreed upon by the parties in advance and also be subject to Voya's receipt of all data reasonably necessary to make such correction.

Section 6.8 Errors of Other Service Providers. Voya shall bear no obligation or responsibility for liability, claims, damages, costs and expenses caused by, arising from or related to any act or omission including, but not limited to, errors, mistakes, willful misconduct, bad faith, fraud, negligent acts or omissions of any trustee, custodian, broker/dealer, insurance company, mutual fund company, third party administrator, prior recordkeeper or any other entity that provides, or has provided, services to the Plan.

Section 7 - Service Fees

Section 7.1 Service Fees. Participant will pay for Voya's Services in accordance with the Service Fees listed in Exhibit C. In addition to the Service Fees specified in Exhibit C, upon prior written notice, Employer shall also pay Voya any additional fee that is authorized by a provision elsewhere in this Agreement if applicable.

Section 7.2 Changes in Service Fees. Voya shall have the right to change the Service Fees with reasonable advanced written notice to Employer (i) any time there are changes made to this Agreement or the provisions of the HRA that affect the Service Fees, or (ii) when there are changes in laws or regulations that affect the Services Voya are providing, or will be required to provide, under this Agreement. Any new Service Fee required by such change will be effective as of the date the changes occur. Voya will provide Employer with a new Exhibit C that will replace the existing Exhibit C or an amendment stating the new Service Fees. If Employer does not agree to any change in Service Fees, then Employer may terminate this Agreement upon written notice. Such termination must be sent by Employer within thirty (30) days after Employer receives written notice of the new Service Fees and the Employer's written notice must state when such termination shall become effective. Employer must still pay any Service Fees due for the periods during which the Agreement is in effect.

Section 7.3: Reimbursement of Plan Expenses: As set forth in Exhibit D, Voya shall reimburse the Plan for reasonable administrative expenses as directed by the Employer.

Section 8 – Funding Benefits

Section 8.1 Funding of Benefits. Employer is solely responsible for transmitting the Account contributions on a schedule and in the form to be agreed upon by the Parties as set forth on Exhibit E. Employer shall cause the funds to be deposited into or credited to the Account of each Participant and provide accompanying data, which accurately indicates each Account (and Account source, as applicable) that will be funded or credited and the dollar amount to be funded or credited to each such Account (and Account source, as applicable). Any payroll deduction or other contributions to a funded Account shall be contributed directly to the Account of the Participant pursuant to the Employer's direction. Employer will provide clear instructions regarding crediting amounts to each Participant's Account. In the event that Employer's instructions are unclear or ambiguous, a reasonable interpretation of the instructions will be accepted. Neither Voya nor its Affiliates or Subcontractors shall have any liability for any funds not received or for any errors in crediting Accounts based on the data provided by Employer

Section 9 – Term of the Agreement

Section 9.1 Term. This Agreement shall commence on September 26, 2023, and shall expire December 31, 2026, but may be terminated earlier in accordance with provisions of this Contract. The Contract term may be extended for one additional two-year period by mutual agreement of the parties.

Section 10 – Termination

Section 10.1 Termination Events.

10.1.1 Either Party may terminate this Agreement immediately upon notice to the other Party, if the other Party (i) materially breaches this Agreement, and fails to remedy such breach within sixty (60) days after receiving notice of the breach from the other Party; (ii) materially breaches this Agreement in a manner that, upon mutual agreement of the Parties, cannot be remedied; (iii) commences bankruptcy or dissolution proceedings, has a receiver appointed for a substantial part of its assets, or ceases to operate in the ordinary course of business.

10.1.2 Voya may terminate this Agreement immediately upon notice to Employer if Employer fails to provide the required funds for payment of benefits under the terms of this Agreement.

10.1.3 Either party may terminate this Agreement immediately upon notice to the other Party if any state or other jurisdiction prohibits a Party from administering the Accounts under the terms of this Agreement; or imposes a material penalty on Employer or Voya, and such penalty is based on the administrative Services specified in this Agreement. In such case, the Party may immediately discontinue the Agreement's application in such state or jurisdiction. Notice must be given to the other Party when reasonably practical. The Agreement will continue to apply in all other states or jurisdictions, or as otherwise specified in this Agreement.

Section 10.2 Termination for Convenience. At any time following the Initial Term, either the Plan Sponsor or Contractor may terminate this Agreement upon at least thirty (30) calendar days' advance written notice to the other party. The Plan Sponsor and Contractor may also mutually agree in writing to terminate this Agreement at any time.

Section 10.3 Cooperation with Transfer. In the event of any termination of this Agreement, Voya shall cooperate with Employer in the transfer of Voya's obligations hereunder to a replacement service provider ("Transition Assistance"). Unless otherwise agreed, Employer shall compensate Voya and shall reimburse Voya for all out-of-pocket expenses incurred in providing Transition Assistance as mutually agreed to by the Parties.

Section 11 – Records and Information

Section 11.1 Records. Voya will keep records relating to the Services Voya provides under this Agreement for as long as Voya is required to do so by law.

Section 11.2 Access to Information. If Employer needs information in Voya's possession for lawful or legitimate purposes other than an audit, Voya will provide Employer access to such information, if it is legally permitted to do so and the information relates to Voya's Services under this Agreement, provided the Employer gives Voya reasonable advance notice and an explanation of the need for such information. Employer represents that Employer has reasonable procedures in place for handling PHI, as required by law. Employer will only use or disclose PHI as permitted under this Agreement or by applicable laws. Voya will provide information only while this Agreement is in effect and for a period of six (6) months after the Agreement terminates, unless Employer demonstrates that the information is required by law. Voya also will provide reasonable access to information to an entity providing Plan administrative services or

consulting services to Employer to enable such entity to provide Plan administrative services or provide consulting services to the Employer, as the case may be, upon the request of the Employer. Before Voya provides PHI to such entity, the parties (i.e. entities that provide Plan administrative services or provide consulting services to Employer), must sign a mutually agreed-upon confidentiality agreement, on terms reasonably acceptable to the Parties.

Section 11.3 Voya's Knowledge. Except as expressly set forth herein, this Agreement will not be construed to transfer or assign any of Voya's rights or proprietary interests in any materials, knowledge, processes, methodologies, formats, or other types of intellectual property that are possessed and owned by Voya prior to the time it begins to provide Services hereunder and independent of the performance of Services hereunder.

Section 11.4 Proprietary Business Information. Each Party will limit the use of the other's Proprietary Business Information to only the information required to administer the Accounts, to perform under this Agreement, or as otherwise permitted under this Agreement. Neither Party will disclose the other's Proprietary Business Information to any person or entity other than to the disclosing Party's employees, subcontractors, or representatives needing access to such information to administer the Accounts, to perform under this Agreement, or as otherwise permitted under this Agreement, except that Voya's financial Proprietary Business Information cannot be disclosed to any third party without Voya's express written consent. This provision shall survive the termination of this Agreement.

Section 11.5 Publicity and Use of Voya/Employer Content. The Parties will not use the other Party's or their Affiliates' names, trademarks, trade names, service marks, logos, or other brand marks (collectively the "Marks") without the other's prior written approval, which may be withheld in that Party's sole discretion. The Parties will instruct all Personnel of this prohibition. Each Party acknowledges that the Marks and all rights therein belong exclusively to the original Party and their Affiliates, and that this Agreement does not confer upon the other Party any rights, goodwill, or other interest in the other Party's Marks. Each Party recognizes the validity of the Marks and will not at any time (i) contest, impair, or jeopardize in any way the other Party's and their Affiliates' right, title, and interest in and to the Marks; (ii) cause the validity or enforceability of the Marks or their ownership thereof to be called into question; or (iii) invalidate, impair, tarnish, disparage, degrade, dilute, or injure the Marks (or the goodwill associated therewith) or the reputation of the other Party or their Affiliates. Each Party will not, and will cause all their Personnel not to, make any "case study," testimonial, press release, or other public announcement regarding this Agreement or any activities performed hereunder. If a Party requires the use of the other Party's Marks in order to provide Services under this Agreement, the other Party grants a limited, revocable, non-transferable, non-exclusive license to use the Marks solely as required to provide Services as further described herein. The Marks may be used and displayed only in the form approved by the Party in writing, which may be amended from time to time. If applicable, the Party may provide written branding standards and requirements with respect to the use of its Marks, and the other Party will comply with all such branding standards and requirements. Upon the termination or expiration of this Agreement or the earlier request of a Party, the other Party will return all Marks to or destroy them, as directed.

Section 11.6 PHI. The Parties' obligations with respect to the use and disclosure of PHI are outlined in the Business Associate Addendum attached to this Agreement as Exhibit F.

Section 12 – System Access

Section 12.1 System Access. Voya grants Employer the nonexclusive, nontransferable right to access and use the functionalities contained within the Systems, under the terms specified in this Agreement. Employer agrees that all rights, title, and interest in the Systems and all rights in patents, copyrights, trademarks, and trade secrets encompassed in the Systems will remain Voya's. To obtain access to the Systems, Employer will obtain, and be responsible for maintaining, at no expense to Voya, the hardware, software, and Internet browser requirements

Voya provides to Employer, including any amendments thereto. Employer will be responsible for obtaining an Internet Service Provider or other access to the Internet. Employer will not (i) access Systems or use, copy, reproduce, modify, or excerpt any Systems documentation provided by Voya in order to access or utilize Systems, for purposes other than as expressly permitted under this Agreement or (ii) share, transfer or lease Employer's right to access and use Systems, to any other person or entity that is not a Party to this Agreement without Voya's consent. Employer may designate any third party to access Systems on Employer's behalf, provided the third party agrees to these terms and conditions of Systems access and Employer assumes joint responsibility for such access.

Section 12.2 Security Procedures. Employer will use commercially reasonable physical and software-based measures to protect the passwords and user IDs provided by Voya for access to and use of any web site provided in connection with the services. Employer shall use commercially reasonable anti-virus software, intrusion detection and prevention system, secure file transfer and connectivity protocols designed to protect any email and confidential communications provided to Voya and maintain appropriate logs and monitoring of system activity. Employer shall notify Voya within a reasonable timeframe of any (a) unauthorized access or damage, including damage caused by computer viruses resulting from direct access connection to the System, and (b) misuse and/or unauthorized disclosure of passwords and user IDs provided by Voya which impact the System.

Section 12.3 System Access Termination. Voya reserves the right to (i) terminate any Employer's System access in the event that such Employer user fails to accept the hardware, software and browser requirements provided by Voya, including any amendments thereto; and (ii) terminate any Employer administrative user's System access (but not Participants' system access) immediately on the date Voya reasonably determines that Employer or a third party designated by Employer to access the Systems on Employer's behalf has materially breached any provision of this Agreement. With respect to subsection (ii) above, Employer's Systems access will be reinstated immediately if Voya determines, in its reasonable discretion, that Employer has corrected the problem, provided reasonable assurances that the material breach is not likely to reoccur and is in alignment with applicable laws and regulations. If Voya terminates Employer's System access, pursuant to subsection (ii) above, Voya will provide an alternative to accessing the data that Employer would have accessed through the System. Employer's System access will terminate upon termination of this Agreement. Upon any of the termination events described in this Agreement, Employer agrees to cease all use of Systems, and Voya will deactivate Employer's identification numbers, passwords, and access to the System as soon as administratively feasible.

Section 13 – Indemnification

13.1 Indemnification

Except to the extent that Voya has properly followed the written direction of an authorized representative of the County, Voya agrees to indemnify, defend (with counsel reasonably approved by County) and hold harmless the County and its authorized officers, employees, agents and volunteers from any and all claims, actions, losses, damages and/or liability arising out of this Agreement from any cause whatsoever, including the acts, errors or omissions of any person and for any costs or expenses incurred by the County on account of any claim except where such indemnification is prohibited by law. This indemnification provision shall apply regardless of the existence or degree of fault of indemnities. Voya's indemnification obligation applies to the County's "active" as well as "passive" negligence but does not apply to the County's "sole negligence" or "willful misconduct" within the meaning of Civil Code Section 2782.

13.2 Additional Insured

All policies, except for Worker's Compensation, Errors and Omissions and Professional Liability policies shall contain additional endorsements naming the County and its officers,

employees, agents and volunteers as additional named insured with respect to liabilities arising out of the performance of services hereunder. The additional insured endorsements shall not limit the scope of coverage for the County to vicarious liability but shall allow coverage for the County to the full extent provided by the policy. Such additional insured coverage shall be at least as broad as Additional Insured (Form B) endorsement form ISO, CG 2010.11 85.

13.3 Waiver of Subrogation Rights

The Contractor shall require the carriers of required coverages to waive all rights of subrogation against the County, its officers, employees, agents, volunteers, contractors and subcontractors. All general or auto liability insurance coverage provided shall not prohibit the Contractor and Contractor's employees or agents from waiving the right of subrogation prior to a loss or claim. The Contractor hereby waives all rights of subrogation against the County.

13.4 Policies Primary and Non-Contributory

All policies required herein are to be primary and non-contributory with any insurance or self-insurance programs carried or administered by the County.

13.5 Severability of Interests

The Contractor agrees to ensure that coverage provided to meet these requirements is applicable separately to each insured and there will be no cross-liability exclusions that preclude coverage for suits between the Contractor and the County or between the County and any other insured or additional insured under the policy.

13.6 Proof of Coverage

The Contractor shall furnish Certificates of Insurance to the County Department administering the Contract evidencing the insurance coverage at the time the Contract is executed, additional endorsements, as required shall be provided prior to the commencement of performance of services hereunder, which certificates shall provide that such insurance shall not be terminated or expire without thirty (30) days written notice to the Department, and Contractor shall maintain such insurance from the time Contractor commences performance of services hereunder until the completion of such services. Within fifteen (15) days of the commencement of this contract, the Contractor shall furnish a copy of the Certificate of Insurance for all applicable policies.

13.7 Acceptability of Insurance Carrier

Unless otherwise approved by Risk Management, insurance shall be written by insurers authorized to do business in the State of California and with a minimum "Best" Insurance Guide rating of "A- VII".

13.8 Reserved

13.9 Failure to Procure Coverage

In the event that any policy of insurance required under this contract does not comply with the requirements, is not procured, or is canceled and not replaced, the County has the right but not the obligation or duty to cancel the contract or obtain insurance if it deems necessary and any premiums paid by the County will be promptly reimbursed by the Contractor or County payments to the Contractor will be reduced to pay for County purchased insurance.

13.10 Insurance Review

Insurance requirements are subject to periodic review by the County. The Director of Risk Management or designee is authorized, but not required, to reduce, waive or suspend any insurance requirements whenever Risk Management determines that any of the required insurance is not available, is unreasonably priced, or is not needed to protect the interests of the County. In addition, if the Department of Risk Management determines that heretofore unreasonably priced or unavailable types of insurance coverage or coverage limits become

reasonably priced or available, the Director of Risk Management or designee is authorized, but not required, to change the above insurance requirements to require additional types of insurance coverage or higher coverage limits, provided that any such change is reasonable in light of past claims against the County, inflation, or any other item reasonably related to the County's risk.

Any change requiring additional types of insurance coverage or higher coverage limits must be made by amendment to this contract. Contractor agrees to execute any such amendment within thirty (30) days of receipt.

Any failure, actual or alleged, on the part of the County to monitor or enforce compliance with any of the insurance and indemnification requirements will not be deemed as a waiver of any rights on the part of the County.

13.11 The Contractor agrees to provide insurance set forth in accordance with the requirements herein. If the Contractor uses existing coverage to comply with these requirements and that coverage does not meet the specified requirements, the Contractor agrees to amend, supplement or endorse the existing coverage to do so.

Without in anyway affecting the indemnity herein provided and in addition thereto, the Contractor shall secure and maintain throughout the contract term the following types of insurance with limits as shown:

13.11.1 Workers' Compensation/Employer's Liability – A program of Workers' Compensation insurance or a state-approved, self-insurance program in an amount and form to meet all applicable requirements of the Labor Code of the State of California, including Employer's Liability with $250,000 limits covering all persons including volunteers providing services on behalf of the Contractor and all risks to such persons under this contract.

If Contractor has no employees, it may certify or warrant to the County that it does not currently have any employees or individuals who are defined as "employees" under the Labor Code and the requirement for Workers' Compensation coverage will be waived by the County's Director of Risk Management.

With respect to Contractors that are non-profit corporations organized under California or Federal law, volunteers for such entities are required to be covered by Workers' Compensation insurance.

13.11.2 Commercial/General Liability Insurance – The Contractor shall carry General Liability Insurance covering all operations performed by or on behalf of the Contractor providing coverage for bodily injury and property damage with a combined single limit of not less than one million dollars ($1,000,000), per occurrence. The policy coverage shall include:

a. Premises operations and mobile equipment.
b. Products and completed operations.
c. Broad form property damage (including completed operations).
d. Explosion, collapse and underground hazards.
e. Personal injury.
f. Contractual liability.
g. $2,000,000 general aggregate limit.

13.11.3 Automobile Liability Insurance – Primary insurance coverage shall be written on ISO Business Auto coverage form for all owned, hired and non-owned automobiles

or symbol 1 (any auto). The policy shall have a combined single limit of not less than one million dollars ($1,000,000) for bodily injury and property damage, per occurrence.

If the Contractor is transporting one or more non-employee passengers in performance of contract services, the automobile liability policy shall have a combined single limit of two million dollars ($2,000,000) for bodily injury and property damage per occurrence.

If the Contractor owns no autos, a non-owned auto endorsement to the General Liability policy described above is acceptable.

13.11.4 Umbrella Liability Insurance – An umbrella (over primary) or excess policy may be used to comply with limits or other primary coverage requirements. When used, the umbrella policy shall apply to bodily injury/property damage, personal injury/advertising injury and shall include a "dropdown" provision providing primary coverage for any liability not covered by the primary policy. The coverage shall also apply to automobile liability.

13.11.5 Professional Liability – Professional Liability Insurance with limits of not less than one million ($1,000,000) per claim and two million ($2,000,000) aggregate limits

or

Errors and Omissions Liability Insurance – Errors and Omissions Liability Insurance with limits of not less than one million ($1,000,000) and two million ($2,000,000) aggregate limits

or

Directors and Officers Insurance coverage with limits of not less than one million ($1,000,000) shall be required for Contracts with charter labor committees or other not-for-profit organizations advising or acting on behalf of the County.

If insurance coverage is provided on a "claims made" policy, the "retroactive date" shall be shown and must be before the date of the state of the contract work. The claims made insurance shall be maintained or "tail" coverage provided for a minimum of five (5) years after contract completion.

13.11.7 **Cyber Liability Insurance** - Cyber Liability Insurance with limits of no less than $1,000,000 for each occurrence or event with an annual aggregate of $2,000,000 covering privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information, alteration of electronic information, extortion and network security. The policy shall protect the involved County entities and cover breach response cost as well as regulatory fines and penalties.

Section 14 - **Confidential Information**

Section 14.1 Voya Data Security Addendum. The Parties acknowledge that Voya has a Data Security Addendum in place as attached hereto in Exhibit G, which shall govern the treatment of Confidential Information (as such term is defined in Exhibit G). Voya reserves the right to modify the Data Security Addendum in whole or in part at any time and without prior notice to the Employer. Voya shall provide an updated Data Security Addendum to the Employer upon request. For purposes of the Data Security Addendum, the "Client" is the Employer.

Section 15 – Limitations on Liability

SECTION 15.1 INDIRECT DAMAGES. SUBJECT TO THE EXCLUSIONS SET FORTH BELOW, AND TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY, ITS AFFILIATES OR PERSONNEL BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR OTHER INDIRECT DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, REGARDLESS OF THE CAUSE OF ACTION, WHETHER IN CONTRACT, TORT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Section 16 – General Provisions

Section 16.1 Independent Contractor Relationship. Voya is an independent contractor of Employer, and this Agreement will not be construed as creating a relationship of employment, agency, partnership, joint venture, or any other form of legal association. Neither Party has any power to bind the other Party or to assume or to create any obligation or responsibility on behalf of the other Party or in the other Party's name.

Section 16.2 Assignment. No Party may, without the prior written consent of the other Party, assign any of its rights or delegate any of its duties under this Agreement. Any attempted assignment without the other Party's consent will be void and invalid. Notwithstanding the foregoing, Voya may assign its duties under this Agreement to a Subcontractor without prior written consent of the Employer. Employer may, upon written notice to Voya and at no additional charge to Employer, assign this Agreement to an Employer Affiliate; to any entity that acquires all or substantially all of Employer's assets or capital stock or results from one or more mergers or initial public offerings or any other corporate reorganization; or to the purchaser of any Employer Affiliate, including the purchaser of any division, department, or line of business of such Employer Affiliate.

Section 16.3 Severability. If a court of competent jurisdiction finds any provision of this Agreement invalid or unenforceable in any circumstances, such provision will be enforced to the maximum extent permissible, and the remainder of this Agreement, and the application of such provision in any other circumstances, will not be affected thereby.

Section 16.4 Governing Law and Venue.
This Agreement shall be construed in accordance with the laws of the State of California. The parties' actions under the Agreement shall comply with all applicable laws, rules, regulations, court orders and governmental agency orders. The venue of any action or claim brought by any party to this Agreement will be the Superior Court of California, San Bernardino County, or the United States District Court, Eastern District, Riverside County. Each party hereby waives any law or rule of the court, which would allow them to request or demand a change of venue. If any action or claim concerning this Agreement is brought by any third-party and filed in another venue, the parties hereto agree to use their best efforts to obtain a change of venue to the Superior Court of California, San Bernardino County.

Section 16.5 Dispute Resolution. All disputes between the Parties arising out of this Agreement will first be submitted for informal resolution between the designated officers of Employer and Voya. If the Parties are still unable to reconcile their differences, they may seek relief from a court of competent jurisdiction. The foregoing will not be construed to prohibit either Party from directly seeking injunctive relief without first complying with this Section.

Section 16.6 Construction of Agreement. This Agreement will not be presumptively construed for or against either Party. Section titles are for convenience only. As used in this Agreement, "will" means the same thing as "shall," and the words "include," "includes," and "including," will always be construed as if followed by the words "without limitation."

Section 16.7 Changes and Modifications. The terms and conditions of this Agreement and any other documents referenced herein may not be amended, waived, or modified, except in a writing signed by authorized representatives of both Parties or as otherwise provided in this Agreement.

Section 16.8 Survival. Those provisions of this Agreement that, by their nature, are intended to survive the termination or expiration of this Agreement will remain in full force and effect following the termination or expiration of this Agreement. Such provisions include Term and Termination; Payment; Intellectual Property Rights and Reports; Confidential Information Indemnification; Exclusion of Damages and Remedies; Non-Solicitation; and Governing Law; Venue – Entire Agreement.

Section 16.9 Waiver/Consent. Failure by either Party to exercise or enforce any right under this Agreement, no matter how long the same may continue, will not be deemed a waiver of such right by such Party. No waiver of any provision of, or consent to any breach of, this Agreement will be deemed a waiver of any other provision of, or consent to any subsequent breach of, this Agreement. A Party's consent to or approval of an act or omission on any one occasion will not be deemed a consent to or approval of said act or omission on any subsequent occasion, or a consent to or approval of any other act or omission on the same or any subsequent occasion. To be effective, a Party's waiver of any right or remedy must be documented in a writing signed by the waiving Party.

Section 16.10 No Third Party Beneficiaries. Nothing in this Agreement will confer any right, remedy, or obligation upon anyone other than Employer, the Employer's Affiliates, Voya, and Voya's Affiliates.

Section 16.11 Notices. All notices relating to this Agreement must be in writing and must reference this Agreement. Such notices will be deemed sufficient if sent (i) by postage-prepaid registered or certified U.S. mail, then five business days after sending; or (ii) by commercial courier, then at the time of receipt confirmed by the recipient to the courier on delivery. All notices to a Party will be sent to its address set forth below, or to such other address as may be designated by that Party by notice to the other Party.

If to Voya:
Voya Retirement Insurance and Annuity Company
Attn: Law Department
One Orange Way
Windsor, Connecticut 06095

With copy to:
Voya Financial, Inc.
Employee Benefits
20 Washington Ave. S.
Minneapolis, MN 55401

If to Employer:
San Bernardino County
Attn: Human Resources Benefits Chief
157 W. 5th Street, First Floor
San Bernardino, CA 92415

With copy to:

Section 16.12 ELECTRONIC SIGNATURES
This Agreement may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same Agreement. The parties shall be entitled to sign and transmit an electronic signature of this Agreement (whether by facsimile, PDF or other mail transmission), which signature shall be binding on the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed Agreement upon request.

Section 16.13 Force Majeure. Except for payment obligations hereunder, a Party's failure to perform any of its obligations under this Agreement shall be excused if and to the extent such failure arises out of causes beyond the reasonable control of the nonperforming Party. Such causes may include, but are not restricted to, (i) acts of God or the public enemy, acts of the government in either its sovereign or contractual capacity, acts of terrorism or war, fires or other loss of facilities, floods, epidemics, quarantine restrictions, strikes, freight embargoes, failure of a common carrier, breach of contract by suppliers or others, computer downtime, telephone system outage, delays or failures of access involving the Internet, World Wide Web or similar services including network traffic and configuration problems therewith, or unusually severe weather, labor disputes, and call demand in excess of telephone capacity or operator capacity and similar occurrences; or (ii) the acts or omissions of the other Party, including in the case of Voya, its reliance upon the Employer's or information, data documents or instruments provided by Employer or any Participant, provided, however, that in every such case the failure to perform must be beyond the reasonable control of the non-performing Party.

Section 16.14 Entire Agreement. This Agreement, including all exhibits and documents referenced herein, constitutes the entire agreement between the Parties with respect to the subject matter hereof, and supersedes and replaces all other prior agreements, communications, and understandings (written and oral) regarding its subject matter. Terms and conditions on or attached to quotes, Employer Purchase Orders, or preprinted forms will be of no force or effect, even if acknowledged or accepted by Employer.

VOYA RETIREMENT INSURANCE AND ANNUITY COMPANY

By _____
Authorized Signature

Print Name: Gavin Gruenberg

Print Title: Vice President

SAN BERNARDINO COUNTY

By _____
Authorized Signature

Print Name: Dawn Rowe

Print Title: Chair, Board of Supervisors

EXHIBIT A – HEALTH REIMBURSEMENT ACCOUNT PLAN NAME(S)

SAN BERNARDINO COUNTY RETIREMENT MEDICAL TRUST PLAN

EXHIBIT B – SERVICES

This Exhibit B is attached to and made a part of the Employer Services Agreement between Voya and Employer. If not otherwise defined, capitalized terms in this Exhibit A have the same meaning as in the Employer Services Agreement.

Overview of the Plan Services

Under the Plan, Voya provides administrative, customer and recordkeeping services to Employer and the Participants in connection with the Accounts. These services include:

General:

- Implementation of web-based Application and supporting services, including periodic updating with changes in status, connecting Participants to Accounts through the Application.
- Prepare Plan document and Trust document, if applicable, for Employer approval. Employer is responsible for ensuring that any documents provided by Voya comply with applicable law.
- Completing enrollment set up and ongoing Account maintenance of Participants on the Application.
- Provide standard communication and education material to participants and Employers.
- Provide Employer Portal with access to summary and detailed plan level reporting. Custom reports available upon request, and may be subject to an additional fee.
- Provide HRA Participant Portal for access to Account information and transactional capabilities for plan investments and claims reimbursements.
- Provide a toll-free call center to support HRA plan-related questions from both participants and employers
- Provide participants instructions for online Account registration to the HRA Participant portal.
- Electronic delivery (referred to as "Go Green") and posting of participant quarterly statements, confirmations, and other notices in the HRA Participant Portal. Participants may opt out of electronic delivery in the HRA Participant Portal and elect to receive documents via U.S. mail subject to an additional monthly fee.
- Provide instructions and requirements to Employer regarding payroll and census process, contribution submission, funding transmittal instructions, and any other applicable Employer responsibilities. Information is included in Attachment D (Operating Procedures).
- Posting of Plan contributions received from Employer in accordance with the requirements in Attachment D (Operating Procedures) to each Participant's Account.
- Update participant-level demographic, Account information, and employment status changes for active Participants using data provided by the Employer.
- Update participant-level demographic and account information for Participants who have been identified as terminated by the Employer, using data provided by the Participant.
- Provide Participants, upon eligibility for medical expense reimbursements, with access to a debit card as a payment method, if requested by Employer.

- Processing reimbursement claims and first-level appeals in the manner required under the Plan document, or to the extent a claims procedure is not provided for in the Plan document, Voya's claims procedure, as applicable.

- Receiving and adjudicating for payment, claims and other requests for payment in accordance with IRS guidance regarding substantiation, the terms of the Accounts, and any written claim procedures or other practices established by the Employer and communicated to Voya.

- Perform discrimination testing, if elected by the Employer, to assist Employer in complying with federal qualifications for HRAs. Employer shall provide all information necessary to complete such testing. Should the HRA plan fail any applicable nondiscrimination tests, the Employer must provide direction on corrective actions for the plan.

- Prepare signature ready IRS Form 990 Series and disclosure forms, as required

EXHIBIT C – FEES

This schedule applies for the term of the contract and may be updated at the time of renewal.

Fees are based on standard communications and file formats. Any special mailings, file modifications, plan rebuilds (changes to the plan once implementation has been completed) or custom reporting may be assessed an additional fee. Fees also reflect that the current administrator will facilitate outstanding claims reimbursement requests.

Direct Compensation

Annual Asset Based Fee: This fee is deducted in monthly installments from each Participant's Account.

Annual Asset Based Fee: 0.03%

This fees applies on:
☒ All investment options, including Voya Fixed Account
OR
☐ Mutual fund investment options only

Annual Per Participant Fee: This fee is deducted in monthly installments from each Participant's Account.

Annual Per Participant Fee Actively Employed (Non-claims active) Participants: $4.80

Annual Per Participant Fee for Terminated/Separated from Service (Claims Active) Participants: $24.00

Ancillary Participant Fees:

Replacement Debit Cards*:* **$5.00**
- *Two initial debit cards are provided at no fee*

Participant Election of Mailed Statements: $0.50 per month deducted from each Participant's Account
- *Electronic delivery of statements, confirmations, and notices are provided at no fee*

Debit Card Customization- Employer Fees:

- Co-branded Debit Card: $500 one-time charge
- Private label card: $3,000 one-time charge and $0.50 per card at time of fulfillment (requires minimum order of 10,000 cards)

Indirect Compensation

Fund Revenue and Float: Voya, an Affiliate or Subcontractor has entered into contracts with certain investment funds and fund service providers (the "Funds") pursuant to which such Funds compensate Voya, an Affiliate or Subcontractor, as applicable, for administrative and sub-transfer agency functions performed by Voya, an Affiliate or Subcontractor (the "Fund Revenue"). The Fund Revenue paid to Voya, an Affiliate or Subcontractor from such investment products, if any, shall not be a source of compensation for the services rendered under this Agreement, but will instead be returned to plan participants whose account balances generated the Fund Revenue in accordance with procedures mutually agreed to by the Parties. In addition, one or more bank accounts may be established, either directly or through a custodian or other Subcontractor, to hold (i) contributions pending investment direction and/or (ii) amounts pending distribution from the HRA. Any earnings credited to a Voya, an Affiliate or Subcontractor based on amounts held in the Accounts ("float") shall constitute a part of overall compensation for the Services.

EXHIBIT D – REIMBURSMENT OF PLAN EXPENSES

Voya shall reimburse the County $126,250 per quarter ($505,000 annually), on a proportional basis, for reasonable and necessary administrative expenses for covered plans. This is the total amount to be paid to the County without regard to the number of plans covered in this Agreement or plans covered in separate Agreements.

EXHIBIT E – OPERATING PROCEDURES

Subcontractor (and to the extent applicable, Voya) shall coordinate with the Employer and the Employer's payroll vendor, as necessary, to initiate electronic reporting of contributions, using the standard file layout provided and in accordance with operating procedures. Once Subcontractor begins to receive electronic reporting of contributions, contribution processing may begin. The following steps must be completed to initiate each contribution to the Plan:

Submission of Contribution Data:

1. Employer submits contribution data through Subcontractor's secure file transfer method for the payroll application.
2. Subcontractor processes contribution data received.
3. **Contribution data must be received in Good Order in order for contributions to be processed.**

Verification of Contribution Data:

1. Subcontractor will send a notification to Employer via email to the Payroll Contact the Employer has identified for the Plan stating that the payroll data is ready for approval. Upon receipt of notification, Employer must log into the payroll tool to review contribution totals and electronically sign-off/approve verifying the integrity of the contribution data provided for the contributions.
2. In addition, by signing-off and approving the contribution data, the Plan Sponsor signifies to Subcontractor that contribution funds have been made available for Subcontractor to complete the transaction.
3. Employer's electronic sign-off/approval of contribution data must be received by Subcontractor for contributions to be processed.

Transmittal of Funds:

1. Employer may wire funds to the Omnibus Trading Account at Community Bank, N.A. or make use of the ACH Debit Policy for deposit to the Omnibus Trading Account. Any funds remitted must include the 6-digit BPAS assigned Plan Identification Number ("BPANbr") and indicate the pay period for which the funds are remitted.

Automated Debit Policy. If the Employer authorizes to initiate debit entries in connection with contributions and other payments made to the Plan, as directed by the Employer, through an Automated Clearing House ("ACH") electronic funds transfer from the account set up for this purpose, such account shall be designated by the Employer on a "BPAS ACH Authorization" form. Employer may subsequently designate another bank account by directing in writing or such other medium as may be acceptable to Subcontractor. Employer will be responsible for submitting contributions and other payment data via electronic means acceptable to Subcontractor. Employer also directs that the Employer's completed ACH Authorization, or subsequent direction acceptable to Subcontractor which supersedes the original, shall serve as authorization to the bank indicated by the Employer to accept any such debit entries initiated to the designated bank account. Employer agrees that it shall be solely responsible for ensuring that Subcontractor is in receipt of the information necessary to initiate and effectuate the transfer of funds pursuant to this instruction and that the bank account designated by the Employer now or in the future, contains sufficient funds to satisfy the ACH request. Further, Employer agrees and acknowledges that

1. If it should fail to make sufficient funds available in its bank account for ACH purposes, Subcontractor reserves the right to reverse these new contribution trades in Participants' accounts, 2) these purchases will not be considered "plan assets" until the funds have actually been delivered to Subcontractor, and 3) if the Employer fails to deliver settlement proceeds, Employer will assume full responsibility for resolving this matter with plan participants, including any financial restitution.
2. Funds held in the Omnibus Trade Account are the property of the Employer. Once the money is transferred (invested) the funds become the property of the Plan.
3. **Funds must be received in Good Order for contributions to be processed.**

The Trade Date for the processing of contributions will not exceed two (2) business days from Supplier's receipt of valid census information, approved verification data and funding in Good Order.

Processing Of Contributions:

Trade Date
Contributions will be processed after receipt by Subcontractor in Good Order on a Business Day. Good Order requirement includes Employer's Verification of Contribution Data, as outlined above, and the amount of the contribution must be equal to the amount of the verified contribution data. If Employer's Verification of Contribution Data is completed before 3:30PM ET and correct funding is received before 4:00 PM ET, Subcontractor shall use its best efforts to trade contributions received in Good Order effective that Business Day.

Transactions will be priced at Trade Date's NAV, provided that Subcontractor receives the Participating Fund's prices (NAVs) for Trade Date prior to 6:30 p.m. ET. (At times the funds may encounter heavy trading or system malfunctions and may not provide NAV in a timely manner). Subcontractor will transmit transactions over the System to the Participating Funds (or their transfer agent) on Trade Date. However, the Trade Date for contributions may be up to two (2) Business days after receipt by Subcontractor. Subcontractor will use its best efforts to affect transactions based in fund trading restrictions and custodial timing after receipt of transaction instructions. Instructions received on a day that is not a business day shall be deemed to have been received as of the first business day thereafter. A "Business day" is a day on which the Subcontractor, the New York Stock Exchange, and all other entities contracted by Voya to provide trade execution and settlement are open for business.

Subcontractor will not be responsible or have any liability for any loss or diminution in value that may occur if transactions are not executed due to (i) circumstances not within Subcontractor's or Voya's control or (ii) a Holiday or close of business of Subcontractor, the New York Stock Exchange, or any other entities contracted by Voya to provide trade execution and settlement.

Wire Date
Subcontractor will cause funds representing result of transactions traded to be wired to the fund(s) the morning following Trade Date. Subcontractor or its designee is solely responsible for the coordination with each Fund of the wire transfer or deposit of funds for the purchase and redemption of fund shares and will ensure that payment occurs on a timely basis in order to obtain Trade Date's NAV. The Funds' inability to accept or receive deposit of funds goes beyond Subcontractor's responsibility.

Changes to Operating Procedures:

This Exhibit E, Operating Procedures, may be subject to change. Any changes shall be communicated to the Employer at least thirty (30) calendar days in advance of the change.

EXHIBIT F - BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "**BAA**"), effective on the last signature date below, is incorporated into and made part of the **Employer Services Agreement (**the "**Agreement**") by and between San Bernardino County ("**Covered Entity**") and Voya Retirement Insurance and Annuity Company ("**Voya**"). Covered Entity and Voya may be referred to individually as a "**Party**" or collectively as the "**Parties**."

WHEREAS, Covered Entity and Voya have entered the Agreement dated September 26, 2023 in connection with which Voya is required to provide assurances that Voya will appropriately safeguard all health information protected under the Privacy Rule and Security Rule (as defined below) that is disclosed by, or created or received by, Voya on behalf of such Covered Entity;

NOW, THEREFORE, and in consideration for the mutual benefit provided to each Party under the Agreement, the Parties agree as follows:

1. **BACKGROUND AND PURPOSE**. The Parties have entered into, and may in the future enter into, one or more written agreements, that require Voya to create, receive, maintain and/or transmit "protected health information" (the "**Underlying Contract(s)**"), as the term is defined under 45 C.F.R. § 160.103 but is limited to the protected health information that Voya creates, receives, maintains, or transmits from or on behalf of the Covered Entity as the Covered Entity's "Business Associate" as defined at 45 C.F.R. § 160.103 ("**PHI**"). Such PHI is subject to protection under the Health Insurance Portability and Accountability Act of 1996, as amended ("**HIPAA**"), Title XIII, Subtitle D, of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5), known as the Health Information Technology for Economic and Clinical Health Act, as amended (the "**HITECH Act**"), and the implementing regulations for HIPAA and the HITECH Act, including, without limitation, the Standards for Privacy of Individually Identifiable Health Information, set forth at 45 C.F.R. Part 160 and Part 164 (Subparts A and E) (the "**Privacy Rule**"), the Security Standards for the Protection of Electronic Protected Health Information, set forth at 45 C.F.R. Part 160 and Part 164 (Subparts A and C) (the "**Security Rule**"), the Standards for Electronic Transactions, set forth at 45 C.F.R. Parts 160 and 162 (the "**Electronic Transactions Rule**"), and the Breach Notification for Unsecured Protected Health Information, set forth at 45 C.F.R. Parts 160 and 164 (Subpart D) (the "**Breach Notification Rule**"), as such implementing regulations may have been or may in the future be amended from time to time (the Privacy Rule, the Security Rule, the Electronic Transactions Rule and the Breach Notification Rule, as amended from time to time, are referred to collectively as the "**Rules**") (HIPAA, the HITECH Act, and the Rules, collectively, the "**HIPAA Laws**").

This BAA shall supplement and/or amend the Agreement only with respect to Voya's Use, Disclosure, and creation of PHI under the Underlying Contract(s) to allow Covered Entity to comply with the HIPAA Laws. Except as so supplemented and/or amended, the terms of the Agreement shall continue unchanged and shall apply with full force and effect to govern the matters addressed in this BAA and in the Agreement.

DEFINITIONS. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings given in the HIPAA Laws.

2. **VOYA'S OBLIGATIONS WITH RESPECT TO PHI**.

2.1 Permitted Uses and Disclosures of PHI. Except as otherwise specified in this BAA, Voya may make any and all Uses and Disclosures of PHI necessary to perform its obligations under the Underlying Contract(s), or as Required by Law. Unless otherwise limited herein, Voya may, as a Business Associate of Covered Entity:

(a) Provide Data Aggregation services relating to the Health Care Operations of the Covered Entity;

(b) Use or Disclose PHI as Required by Law;

(c) De-identify any and all PHI obtained by Voya under this BAA in accordance with the de-identification requirements of the Privacy Rule guidance issued by the Secretary from time to time, and use and disclose such de-identified data for any of Voya's purposes in a manner solely determined

by Voya, for an indefinite period including beyond the termination of this BAA or the Underlying Contract. This BAA shall not apply to such de-identified data, the de-identified data will cease to be considered the confidential information or property of the Covered Entity including pursuant to any Underlying Contract.

(d) Use or Disclose PHI for the proper management and administration, such as audits and for other compliance requests from federal or state agencies, of Voya or to carry out the legal responsibilities of Voya, pursuant to 45 C.F.R. §164.504(e)(4), provided that (i) such Use or Disclosure is Required by Law, (ii) Voya obtains reasonable assurances from the person or entity which does not qualify as a subcontractor that is a Business Associate under the Rules and to which Voya discloses PHI for such purposes permitted under this Section 3.1(d) that such PHI will be held confidentially, Used or further Disclosed only as required by law or the purpose for which it was disclosed to such person or entity, and that such third party shall notify Voya of any instances of which the third party is aware in which the confidentiality of the PHI received pursuant to this provision has been or third party reasonably believes has been breached.

Under no circumstances may Voya Use or further Disclose PHI in a manner that would violate the HIPAA Laws if done by the Covered Entity.

2.2 Voya's Obligations. With regard to its Use and/or Disclosure of PHI, Voya agrees to:

(a) Use or Disclose only the minimum necessary PHI to perform or fulfill a specific function required or permitted hereunder, in accordance with the HIPAA Laws as stated in 45 CFR 164.502(b) and 45 CFR 164.514.

(b) Not Use or Disclose PHI other than as permitted or required by this BAA or as Required By Law.

(c) Use appropriate safeguards and with respect to PHI transmitted by or maintained in Electronic Media, comply with subpart C of 45 C.F.R. Part 164 regarding provisions of the Security Rule applicable to such information, to prevent the Use or Disclosure of PHI other than as provided for by this BAA.

(d) Ensure that any subcontractor that is a Business Associate, as included in the definition of Business Associate at 45 C.F.R. 160.103, (each a "Subcontractor") enters into an agreement or similar arrangement which complies with the HIPAA Laws requirements for agreements between "Business Associates" and "Covered Entities", as each term is used under the HIPAA Laws, and subject to restrictions and limitations at least as restrictive as those imposed upon Voya in this BAA.

(e) Within thirty (30) days of receiving a written request from Covered Entity, make available to the Covered Entity such PHI necessary for Covered Entity to comply with its obligations under 45 C.F.R. § 164.524 in responding to an Individual's request for access to his or her PHI where Voya maintains PHI in a Designated Record Set. In the event any individual requests access to PHI directly from Voya, Voya shall within ten (10) business days forward such request to Covered Entity. Any denials of access to the PHI requested shall be the exclusive responsibility of the Covered Entity.

(f) Within thirty (30) days of receiving a written request from Covered Entity, make available to the Covered Entity such PHI necessary for Covered Entity to comply with its obligations under 45 C.F.R. § 164.526 in responding to an Individual's request for amendment and Voya shall incorporate any amendments to the PHI as directed or instructed by Covered Entity in accordance with 45 C.F.R. § 164.526 where Voya maintains PHI in the Designated Record Set. In the event any Individual requests an amendment to PHI directly from Voya, Voya shall within ten (10) business days forward such request to Covered Entity.

(g) Within forty-five (45) days of receiving a written request from Covered Entity, make available to the Covered Entity the information required for the Covered Entity to provide an accounting

of disclosures of PHI as required by the Privacy Rule. In the event the request for an accounting is delivered directly to Voya, Voya shall within thirty (30) business days forward such request to the Covered Entity. Voya shall retain its records regarding Uses and Disclosures of PHI that are required to be maintained in a Designated Record Set for no less than six (6) years following the termination of this BAA.

(h) To the extent that Voya carries out Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Voya shall comply with the HIPAA Laws that apply to the Covered Entity in performance of such obligation(s), as required under 45 C.F.R. § 164.504(e)(2)(ii)(H).

(i) Promptly notify the Covered Entity of Voya's receipt of any request for production or subpoena of PHI, in connection with any governmental investigation or governmental or civil proceeding. If the Covered Entity decides to challenge the validity of or assume responsibility for responding to such request or subpoena, Voya shall reasonably cooperate with the Covered Entity in connection therewith.

(j) Make its internal practices, books and records relating to the Use and Disclosure of PHI available to the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Laws.

(k) Use reasonable commercial efforts to mitigate any harmful effect that is known to Voya of a Use or Disclosure of PHI by Voya in violation of the requirements of this BAA.

(l) Voya agrees to use appropriate safeguards to prevent any unauthorized or unlawful Use, access or Disclosure of the PHI, including but not limited to any Use, access or Disclosure not provided for by this BAA. Voya shall implement administrative, physical and technical safeguards required by the HIPAA Laws and comply with the policies, procedures and documentation requirements of the Security Rule.

(m) Report promptly and without unreasonable delay to Covered Entity any Use or Disclosure of PHI not provided for or permitted by this BAA and any Breach or Successful Security Incident, but in no event no more than sixty (60) days after it is discovered. Such notification shall include the information required under 45 C.F.R. § 164.410. "Successful Security Incident" shall mean any Security Incident that results in the unauthorized use, access, disclosure, modification or destruction of electronic PHI.

3. **OBLIGATIONS OF COVERED ENTITY**.

3.1 Covered Entity agrees to timely notify Voya, in writing, of any arrangements of the Covered Entity including any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR § 164.520 that may impact in any manner the Use and/or Disclosure of that PHI by Voya under this BAA.

3.2 Covered Entity further agrees not to request Voya to Use or Disclose PHI in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity, except to the extent that Voya will use or disclose Protected Health Information for the management and administration and legal responsibilities of the Voya.

3.3 Covered Entity shall notify Voya of any changes in, or revocation of, the permission by an Individual to Use or Disclose his or her Protected Health Information, to the extent that such changes may affect Voya's Use or Disclosure of Protected Health Information.

3.4 Covered Entity shall notify Voya of any restriction on the Use or Disclosure of Protected Health Information that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Voya's Use or Disclosure of Protected Health Information.

3.5 Covered Entity shall disclose to Voya only the minimum amount of Protected Health

Information necessary to allow Voya to fulfill its obligations to Covered Entity under the Underlying Contract.

4. **TERM.** This BAA shall commence as of the Effective Date and expire, unless earlier terminated pursuant to Section 5 hereof, at such time as the Underlying Contract(s) is terminated or expires and Voya returns or destroys PHI in accordance with the terms of this BAA.

5. **TERMINATION**. Should a Party become aware of a material breach of this BAA, including without limitation a pattern of activity or practice that constitutes a breach of a material term of this BAA, the non-breaching Party shall provide the breaching Party with written notice of such breach in sufficient detail to enable the breaching Party to understand the specific nature of the breach. The non-breaching Party shall be entitled to immediately terminate this BAA and the Underlying Contract associated with such breach if, after the non-breaching Party provides such notice of breach to the breaching Party, the breaching Party fails to cure the breach within a reasonable time period not to exceed thirty (30) days from the breaching Party's receipt of such notice; provided, however, the non-breaching Party shall have the discretion to agree to such longer cure period based on the nature of the breach involved and subject to the HIPAA Laws.

6. **RETURN OR DESTRUCTION OF PHI**. Upon the expiration or termination of this BAA and/or the Underlying Contract(s), Voya, with respect to PHI received from Covered Entity, or created, maintained or received by Voya on behalf of Covered Entity, including any and all PHI in the possession of Voya's Subcontractors and such third parties permitted to receive such PHI under and in accordance with the terms of this BAA and the HIPAA Laws, shall:

(a) Retain only that PHI which is necessary for Voya to continue its proper management and administration or to carry out its legal responsibilities;

(b) Return to Covered Entity or destroy, as agreed to by Covered Entity, the remaining PHI that Voya still maintains in any form;

(c) Continue to use appropriate safeguards and comply with the Security Rule with respect to PHI transmitted by or maintained in Electronic Media to prevent Use or Disclosure of the PHI, other than as provided for in this Section, for as long as Voya retains the PHI;

(d) Not Use or Disclose the PHI retained by Voya other than for the purposes for which such PHI was retained and subject to the same conditions set forth in Section 2 hereof which applied prior to termination;

(e) Return to Covered Entity or destroy, as agreed to by Covered Entity, the PHI retained by Voya when it is no longer needed by Voya for its proper management and administration or to carry out its legal responsibilities; and

(f) Where the return or destruction of PHI is infeasible, Voya shall notify Covered Entity in a writing of sufficient specificity of the circumstances which make such return or destruction infeasible, and upon acceptance and agreement by Covered Entity, Voya shall continue to extend the protections of this BAA to such PHI and limit further use or disclosure of PHI to those purposes which make the return or destruction infeasible, for as long as Voya retains the PHI.

7. **MISCELLANEOUS**.

7.1 Survival. The respective rights and obligations of Voya and Covered Entity under this BAA which by their nature shall survive this BAA shall survive the expiration or termination of this BAA indefinitely, including without limitation Section 6.

7.2 Interpretation. The terms of this BAA shall prevail in the case of any conflict with the terms of any Underlying Contract to the extent necessary to allow Covered Entity to comply with the HIPAA Laws. Any ambiguity in this BAA shall be resolved in favor of a meaning that permits Covered Entity and Voya to comply with the HIPAA Laws. The citations to the HIPAA Laws in several paragraphs of this BAA are for reference only and shall not be relevant in interpreting any provision of this BAA.

7.3 No Third Party Beneficiaries. Nothing in this BAA shall confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

7.4 Amendment. This BAA constitutes the entire agreement between the Parties with respect to PHI, and may not be modified, nor will any provision be waived or amended, except in a writing duly signed by authorized representatives of the Parties.

7.5 Waiver. A waiver with respect to one event will not be construed as continuing, or as a bar or waiver of any right or remedy as to subsequent events.

7.6 Changes in the HIPAA Laws. To the extent that any relevant provision of the HIPAA Laws is materially amended in a manner that changes the obligations of Voya or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s) to this BAA to give effect to those revised obligations.

7.7 Governing Law and Venue. This Agreement shall be construed in accordance with the laws of the State of California. The parties' actions under the Agreement shall comply with all applicable laws, rules, regulations, court orders, and governmental agency orders. The venue of any action or claim brought by any party to this Agreement will be the Superior Court of California, San Bernardino County, or the United States District Court, Eastern District, Riverside County. Each party hereby waives any law or rule of court, which would allow them to request or demand a change of venue. If any action or claim concerning this Agreement is brought by any third-party and filed in another venue, the parties hereto agree to use their best efforts to obtain a change of venue to the Superior Court of California, San Bernardino County.

7.8 Regulatory References. A reference in this BAA to a section of the Code of Federal Regulations, the Privacy Rule, the Security Rule, or to another section of HIPAA means the section, as amended from time to time.

7.9 Notices. All notices and communications required by this BAA shall be in writing. Such notices and communications shall be given in one of the following forms: (i) by delivery in person; (ii) by a nationally-recognized, next-day courier service; (iii) by first-class, registered or certified mail, postage prepaid; or (iv) by electronic mail to the address that each party specifies in writing.

7.10 Confidentiality. The terms of this BAA shall remain confidential except as described hereunder and in the Underlying Contract, except that Voya may disclose the terms of this BAA to entities that Voya reasonably believes are other Business Associates of Covered Entity.

7.11 Severability. The invalidity or unenforceability of any provisions of this BAA shall not affect the validity or enforceability of any other provision of this BAA or the Underlying Contract, which shall remain in full force and effect

7.12 Construction and Interpretation. The section headings contained in this BAA are for reference purposes only and shall not in any way affect the meaning or interpretation of this BAA. This BAA has been negotiated by the parties at arm's-length and each of them has had an opportunity to modify the language of the BAA. Accordingly, the BAA shall be treated as having been drafted equally by the parties, and the language shall be construed as a whole and according to its fair meaning. Any presumption or principle that the language is to be construed against any party shall not apply. This BAA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. A signed copy of this Agreement delivered by facsimile, e-mail or other means of electronic transmission shall be deemed to have the same legal effect as the delivery of an original signed copy of this Agreement.

7.13 Entire Agreement. This BAA constitutes the entire and full agreement between the Parties with respect to the subject matter hereof and supersedes and replaces any previous version of this agreement.

IN WITNESS WHEREOF, each of the undersigned has caused this BAA to be duly executed in its name and on its behalf.

San Bernardino County (Covered Entity) By:_____ Print Name: Dawn Rowe Print Title: Chair, Board of Supervisors Date: 09/26/2023	**Voya Retirement Insurance and Annuity Company** By:_____ Print Name: Gavin Gruenberg Print Title: Vice President Date:

EXHIBIT G – DATA SECURITY ADDENDUM

1. Definitions.

"Affected Persons" means Client's and its Affiliate's former and current employees whose Personal Information ("PI") may have been disclosed or compromised as a result of an Information Security Incident.

"Affiliates" means any entities that, now or in the future, control, are controlled by, or are under common control with Client. An entity will be deemed to control another entity if it has the power to direct or cause the direction of the management or policies of such entity, whether through ownership, voting securities, contract, or otherwise.

"Confidential Information" means (a) non-public information concerning the Disclosing Party, its affiliates, and their respective businesses, products, processes, and services, including technical, marketing, agent, customer, financial, personnel, and planning information; (b) PI; (c) trade secrets; and (d) any other information that is marked confidential or which, under the circumstances surrounding disclosure, the Non-Disclosing Party should know is treated as confidential by the Disclosing Party. Except with respect to PI, which will be treated as Confidential Information under all circumstances, Confidential Information will not include (A) information lawfully obtained or developed by the Non- Disclosing Party independently of the Disclosing Party's Confidential Information and without breach of any obligation of confidentiality; or (B) information that enters the public domain without breach of any obligation of confidentiality. All Confidential Information will remain the property of the Disclosing Party.

"Information Security Incident" means any breach of security or cyber security incident impacting Voya that has a reasonable likelihood of (a) resulting in the loss or unauthorized access, use or disclosure of Client PI; (b) materially affecting the normal operation of Voya; or (c) preventing Voya from complying with all of the privacy and security requirements set forth in this Agreement.

"Law" means all U.S. and non-U.S. laws, ordinances, rules, regulations, declarations, decrees, directives, legislative enactments and governmental authority orders and subpoenas.

"Personal Information (PI)" means any information or data that (a) identifies an individual, including by name, signature, address, telephone number or other unique identifier; (b) can be used to identify or authenticate an individual, including passwords, PINs, biometric data, unique identification numbers (e.g., Social Security numbers), answers to security questions or other personal identifiers; (c) is "non-public personal information" as defined in the Gramm-Leach-Bliley Act 15 U.S.C. § 6809(4) or "protected health information" as defined in 45 C.F.R. § 160.103; (d) is an account number or credit card number or debit card number, in combination with any required security code, access code, or password, that would permit access to an individual's financial account; or (e) is "Personal Information" as defined in The California Consumer Privacy Act of 2018 (Cal. Civ. Code Division 3, Part 4, Title 1.81.5).

"Services" means the services that Voya provides to Client pursuant to this Agreement.

"Voya Personnel" means Voya's employees and subcontractors engaged in the performance of Services.

2. Data Security.

2.1. Security Standards and Controls.

(a) Voya will establish and maintain:

(i) administrative, technical, and physical safeguards against the destruction, loss, or alteration of confidential Information; and

(ii) Appropriate security measures to protect Confidential Information, which measures meet or exceed the requirements of all applicable Laws relating to personal information security.

(b) In addition, Voya will implement and maintain the following information security controls:

(i) Privileged access rights will be restricted and controlled;

(ii) An inventory of assets relevant to the lifecycle of information will be maintained;

(iii) Network security controls will include, at a minimum, firewall and intrusion prevention services;

(iv) Detection, prevention and recovery controls to protect against malware will be implemented;

(v) Information about technical vulnerabilities of Voya's information systems will be obtained and evaluated in a timely fashion and appropriate measures taken to address the risk;

(vi) Detailed event logs recording user activities, exceptions, faults, access attempts, operating system logs, and information security events will be produced, retained and regularly reviewed as needed; and

(vii) Development, testing and operational environments will be separated to reduce the risks of unauthorized access or changes to the operational environment.

2.2. Information Security Policies. Voya will implement and maintain written policies, standards or procedures that address the following areas:

(a) Information security;
(b) Data governance and classification;
(c) Access controls and identity management;
(d) Asset management;
(e) Business continuity and disaster recovery planning and resources;
(f) Capacity and performance planning;
(g) Systems operations and availability concerns;
(h) Systems and network security;
(i) Systems and application development, quality assurance and change management;
(j) Physical security and environmental controls;
(k) Customer data privacy;
(l) Patch management;
(m) Maintenance, monitoring and analysis of security audit logs;
(n) Vendor and third party service provider management; and
(o) Incident response, including clearly defined roles and decision making authority and a logging and monitoring framework to allow the isolation of an incident.

2.3. Subcontractors. Voya will implement and maintain policies and procedures to ensure the security of Confidential Information and related systems that are accessible to, or held by, third party service providers. Voya will not allow any third parties to access Voya's systems or store or process sensitive data, unless such third parties have entered into written contracts with Voya that require, at a minimum, the following:

(a) The use of encryption to protect sensitive PI in transit, and the use of encryption or other mitigating controls to protect sensitive PI at rest;
(b) Prompt notice to be provided in the event of a cyber security incident;
(c) The ability of Voya or its agents to perform information security assessments; and
(d) Representations and warranties concerning adequate information security.

2.4. Encryption Standards, Multifactor Authentication and Protection of Confidential Information.

(a) Voya will implement and maintain cryptographic controls for the protection of Confidential Information, including the following:

(i) Use of an encryption standard equal to or better than the industry standards included in applicable National Institute for Standards and Technology Special Publications (or such higher encryption standard required by applicable Law) to protect Confidential Information at rest and in transit over un-trusted networks;

(ii) Use of cryptographic techniques to provide evidence of the occurrence or nonoccurrence of an event or action;

(iii) Use of cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources; and

(iv) Development and implementation of policies on the use, protection and lifetime of cryptographic keys through their entire lifecycle.

(b) In addition to the controls described in clause (a) above, Voya will:

(i) Implement multi-factor authentication for all remote access to Voya's networks;

(ii) Ensure that no Client PI is (A) placed on unencrypted removable media, mobile devices, computing equipment or laptops or (B) stored outside the United States; and

(iii) Ensure that media containing Confidential Information is protected against unauthorized access, misuse or corruption during transport.

2.5. Information Security Roles and Responsibilities. Voya will employ personnel adequate to manage Voya's information security risks and perform the core cyber security functions of identify, protect, detect, respond and recover. Voya will designate a qualified employee to serve as its Chief Information Security Officer ("CISO") responsible for overseeing and implementing its information security program and enforcing its information security policies. Voya will define roles and responsibilities with respect to information security, including by identifying responsibilities for the protection of individual assets, for carrying out specific information security processes, and for information security risk management activities, including acceptance of residual risks. These responsibilities should be supplemented, where appropriate, with more detailed guidance for specific sites and information processing facilities.

2.6. Segregation of Duties. Voya must segregate duties and areas of responsibility in order to reduce opportunities for unauthorized modification or misuse of Voya's assets and ensure that no single person can access, modify or use assets without authorization or detection. Controls should be designed to separate the initiation of an event from its authorization. If segregation is not reasonably possible, other controls such as monitoring of activities, audit trails and management supervision should be utilized. Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

2.7. Information Security Awareness, Education and Training. Voya will provide regular information security education and training to all Voya Personnel, as relevant for their job function. In addition, Voya will provide mandatory training to information security personnel and require key information security personnel to stay abreast of changing cyber security threats and countermeasures.

2.8. Vulnerability Assessments. Voya will conduct monthly vulnerability assessments that meet the following criteria:

(a) All production servers and network devices must be scanned at least monthly;

(b) All vulnerabilities must be rated;

(c) All vulnerability remediation must be prioritized based on risk;

(d) All tools used for scanning must have signatures updated at least monthly with the latest vulnerability data; and,

(e) Voya will implement and maintain a formal process for tracking and resolving issues in a timely fashion.

2.9 Penetration Testing. If any Services to be provided by Voya include the hosting or support of one or more externally facing applications that can be used to access systems that store or process Client data, the terms of this Section will apply.

(a) At least once every 12 months during the Term and prior to any major changes being moved into production, Voya will conduct a Valid Penetration Test (as defined below) on each internet facing application described above. As used herein, a "Valid Penetration Test" means a series of tests performed by a team of certified professionals, which tests mimic real-world attack scenarios on the information system under test and include, without limitation, the following:

(i) Information-gathering steps and scanning for vulnerabilities;

(ii) Manual testing of the system for logical flaws, configuration flaws, or programming flaws that impact the system's ability to ensure the confidentiality, integrity, or availability of Client's information assets;

(iii) System-compromise steps;

(iv) Escalation-of-privilege steps; and

(v) Assignment of a rating for each issue based on the level of potential risk exposure to Client's brand or information assets.

(b) Upon Client's request, Voya will provide to Client an executive summary of any material issues or vulnerabilities identified by the most recent Valid Penetration Test along with the scope of systems tested. The report may be redacted to ensure confidentiality.

2.10 Physical and Environmental Security. Voya will ensure that all sites are physically secure, including the following:

(a) Sound perimeters with no gaps where a break-in could easily occur;

(b) Exterior roof, walls and flooring of solid construction and all external doors suitable protected against unauthorized access with control mechanisms such as locks, bars, alarms, etc.;

(c) All doors and windows to operational areas locked when unattended;

(d) Equipment protected from power failures and other disruptions caused by failures in supporting utilities;

(e) Closed-circuit television cameras at site entry/ exit points; badge readings at all site entry points, or other means to prevent unauthorized access; and

(f) Visitor sign-in/ mandatory escort at site; and

(g) With respect to remote work environments, if the foregoing controls are not present, then Voya will use commercially reasonable efforts to mitigate any increased risk associated with such remote work environments, by, for example, limiting the types of access and functional roles eligible for a remote work environment, restricting access to a virtual private network (vpn) or virtual desktop infrastructure (vdi), providing formal guidance and standards for workspace security, and enhancing data protection controls such as data masking, logging and monitoring.

2.11 Information Security Incident Notification.

(a) In the event of any Information Security Incident, Voya will, at its sole expense promptly (and in any event within 72 hours after Voya confirms an Information Security Incident) report such Information Security Incident to Client by sending an email to Client Contact Information, summarizing in reasonable detail the effect on Client, if known, and designating a single point of contact at Voya who will be:

(i) Available to Client for information and assistance related to the Information Security Incident; investigate such Information Security Incident, perform a root cause analysis,

develop a corrective action plan and take all necessary corrective actions;

(ii) Mitigate, as expeditiously as possible, any harmful effect of such Information Security Incident and cooperate with Client in any reasonable and lawful efforts to prevent, mitigate, rectify and remediate the effects of the Information Security Incident;

(iii) Provide a written report to Client containing all information necessary for Client to determine compliance with all applicable laws, including the extent to which notification to affected persons or to government or regulatory authorities is required; and

(iv) Cooperate with Client in providing any filings, communications, notices, press releases or reports related to such Information Security Incident.

(b) In addition to the other indemnification obligations of Voya set forth in this Agreement, Voya will indemnify, defend and hold harmless Client from and against any and all claims, suits, causes of action, liability, loss, costs and damages, including reasonable attorneys' fees, arising out of or relating to any Information Security Incident, which may include, without limitation:

(i) Expenses incurred to provide notice to Affected Persons and to law-enforcement agencies, regulatory bodies or other third parties as required to comply with law;

(ii) Expenses related to any reasonably anticipated and commercially recognized consumer data breach mitigation efforts, including, but not limited to, costs associated with the offering of credit monitoring or a similar identify theft protection or mitigation product for a period of at least twelve (12) months or such longer time as is required by applicable laws or any other similar protective measures designed to mitigate any damages to the Affected Persons; and

(iv) Fines or penalties that Client pays to any governmental or regulatory authority under legal or regulatory order as a result of the Information Security Incident.

2.12. Risk Assessments. Upon Client's request no more than once per year, Voya will complete an industry standard information security questionnaire and provide relevant Service Organization Control ("SOC") audit reports, when available. Voya's standard security requirements are set forth in Exhibit G and Exhibit H. Voya represents and warrants that, as of the Effective Date, the statements in Exhibit G and Exhibit H are true and correct in all material respects.

3. Privacy and PII

3.1. With respect to any PI, Voya will:

(a) Comply with the Voya Privacy Notice at www.voya.com/privacy-notice;

(b) Retain, use, process and disclose all PI accessed, obtained or produced by Voya only to perform its obligations under this Agreement and as specifically permitted by this Agreement, or as otherwise instructed by Client, and not for any other purpose;

(c) Refrain from selling such PI or using such PI for any other purpose, including for its own commercial benefit;

(d) Treat all PI as Confidential Information;

(e) Comply with the provisions of this Agreement to return, store or destroy the PI; and

(f) Comply with all applicable Laws with respect to processing of PI.

Voya hereby certifies to Client that it understands the restrictions and obligations set forth above and will ensure that Voya and all Voya Personnel comply with the same.

3.2 As needed to comply with applicable Laws concerning the processing of PI or personal information security, or to the extent required by any changes in such Laws or the enactment of new Laws, the Parties agree to work cooperatively and in good faith to amend this Agreement in a mutually agreeable and timely manner, or to enter into further mutually agreeable agreements in an effort to comply with any such Laws applicable to the Parties. If the Parties cannot so agree, or if Voya cannot comply with the new or additional requirements, Client may terminate this Agreement upon written notice to Voya.

4. Confidential Information.

4.1. Confidential Information. Either Party ("Disclosing Party") may disclose Confidential Information to the other Party ("Non-Disclosing Party") in connection with this Agreement.

4.2. Use and Disclosure of Confidential Information. The Non-Disclosing Party agrees that it will disclose the Disclosing Party's Confidential Information only to its employees, agents, consultants, and contractors who have a need to know and are bound by obligations of confidentiality no less restrictive than those contained in this Agreement. In addition, Voya agrees that it will use the Disclosing Party's Confidential Information only for the purposes of performing its obligations under this Agreement. The Non-Disclosing Party will use all reasonable care in handling and securing the Disclosing Party's Confidential Information and will employ all security measures used for its own proprietary information of similar nature. These confidentiality obligations will not restrict any disclosure of Confidential Information required by Law or by order of a court, regulatory authority or governmental agency; provided, that the Non-Disclosing Party will limit any such disclosure to the information actually required to be disclosed. Notwithstanding anything to the contrary, Client may fully comply with requests for information from regulators of Client and the Client Affiliates.

4.3. Treatment of Confidential Information Following Termination. Promptly following the termination or expiration of this Agreement, or earlier if requested by the Disclosing Party, the Non-Disclosing Party will return to the Disclosing Party any and all physical and electronic materials in the Non-Disclosing Party's possession or control containing the Disclosing Party's Confidential Information. The materials must be delivered via a secure method and upon such media as may be reasonably required by the Disclosing Party.

Alternatively, with the Disclosing Party's prior written consent, the Non-Disclosing Party may permanently destroy or delete the Disclosing Party's Confidential Information and, if requested, will promptly certify the destruction or deletion in writing to the Disclosing Party. Notwithstanding the foregoing, if the Non-Disclosing Party, due to requirements of applicable Law, must retain any of the Disclosing Party's Confidential Information, or is unable to permanently destroy or delete the Disclosing Party's Confidential Information as permitted above within 60 days after termination of this Agreement, the Non- Disclosing Party will so notify the Disclosing Party in writing, and the Parties will confirm any extended period needed for permanent destruction or deletion of the Disclosing Party's Confidential Information. All Confidential Information in the Non-Disclosing Party's possession or control will continue to be subject to the confidentiality provisions of this Agreement. The methods used to destroy and delete the Confidential Information must ensure that no Confidential Information remains readable and cannot be reconstructed so to be readable. Destruction and deletion must also comply with the following specific requirements:

MEDIUM	DESTRUCTION METHOD
Hard copy	Shredding, pulverizing, burning, or other permanent destruction method
Electronic tangible media, such as disks and tapes	Destruction or erasure of the media
Hard drive or similar storage device	Storage frame metadata removal to hide the organizational structure that combines disks into usable volumes and physical destruction of the media with a Certificate of Destruction (COD)

4.4 Period of Confidentiality. The restrictions on use, disclosure, and reproduction of Confidential Information set forth in this Section will, with respect to PI and Confidential Information that constitutes a "trade secret" (as that term is defined under applicable Law), be perpetual, and will, with respect to other Confidential Information, remain in full force and effect during the term of this Agreement and for three years following the termination or expiration of this Agreement.

4.5. Injunctive Relief. The Parties agree that the breach, or threatened breach, of any of the confidentiality provisions of this Agreement may cause irreparable harm without adequate remedy at law. Upon any such breach or threatened breach, the Disclosing Party will be entitled to injunctive relief to prevent the Non-Disclosing Party from commencing or continuing any action constituting such breach, without having to post a bond or other security and without having to prove the inadequacy of other available remedies. Nothing in this Section will limit any other remedy available to either Party.

5. Cyber Liability Insurance. During the Term, Voya will, at its own cost and expense, obtain and maintain in full force and effect, with financially sound and reputable insurers, cyber liability insurance to cover Voya's obligations under this Addendum. Upon execution of the Agreement, Voya will provide Client with a certificate of insurance evidencing the following coverage and amount with such insurer:

Risk Covered: Network Security (a.k.a. Cyber/IT)
Limits: $50,000,000

6. Disaster Recovery and Business Continuity Plan. Voya maintains, and will continue to maintain throughout the Term, (a) a written disaster recovery plan ("Disaster Recovery Plan"), which Disaster Recovery Plan is designed to maintain Client's access to services and prevent the unintended loss or destruction of Client data; and (b) a written business continuity plan ("BCP") that permits Voya to recover from a disaster and continue providing services to customers, including Client, within the recovery time objectives set forth in the BCP. Upon Client's reasonable request, Voya will provide Client with evidence of disaster recovery test date and result outcome.

Exhibit H

Security Requirements

FC:	Foundation Controls
FC-1:	Information Asset Management
FC-1.1	Voya implements and maintains an inventory list and assigns ownership for all computing assets including, but not limited to, hardware and software used in the accessing, storage, processing, or transmission of Client PI.
FC-1.2	Voya reviews and updates the inventory list of assets for correctness and completeness at least once every 12 months and updates the inventory list as changes are made to the computing assets.
FC-2:	Data Privacy and Confidentiality
FC-2.1	Voya will maintain an Information and Risk Management policy that is reviewed and approved by management at least annually.
FC-2.2	Voya protects the privacy and confidentiality of all Client PI received, disclosed, created, or otherwise in Voya's possession by complying with the following requirements:
FC-2.2A	Such information is encrypted at rest on mobile devices (including mobile storage devices), portable computers, and in transit over un-trusted networks with an encryption standard equal to or better than Advanced Encryption Standard (AES) 256 bit encryption or such higher encryption standard required by applicable law.
FC-2.2B	All hardcopy documents and removable media are physically protected from unauthorized disclosure by locking them in a lockable cabinet or safe when not in use and ensuring that appropriate shipping methods (tamper-proof packaging sent by special courier with signatures) are employed whenever the need to physically transport such documents and removable media arises.
FC-2.2C	All media is labeled and securely stored in accordance with Voya policies.
FC-2.2D	All electronic media is securely sanitized or destroyed when no longer required in accordance with industry standards.
FC-3:	Configuration Management
FC-3.1	Voya implements and maintains accurate and complete configuration details (e.g., Infrastructure Build Standards) for all computing assets used in accessing, storing, processing, or transmitting Client PI.
FC-3.2	Voya reviews configuration details of the computing assets at least once every 12 months to validate that no unauthorized changes have been made to the assets.
FC-3.3	Voya updates the configuration details of all computing assets used to access, process, store, or transmit Client PI as configuration changes take place.
FC-4:	Operating Procedures and Responsibilities
FC-4.1	Voya implements and maintains operational procedures for information processing facilities and designates specific roles or personnel responsible for managing and maintaining the quality and security of such facilities, including, but not limited to, formal handover of activity, status updates, operational problems, escalation procedures and reports on current responsibilities. Voya IT policies and standards document the policies and procedures for job scheduling processes and tools.
FC-4.2	Voya updates the operational procedures as changes take place and performs a comprehensive review and update of the procedures at least once every 2 years.
FC-5:	Security Awareness and Training

FC-5.1	Voya performs pre-employment background checks, including criminal history for 7 years, credit score and history (if applicable), credentials verification (if applicable), and educational background.
FC-5.2	Voya implements and maintains a documented security awareness program for all Voya Personnel which covers access to Client PI.
FC-5.3	Voya's security awareness program includes security requirements, acceptable use of computing assets, legal responsibilities, and business controls, as well as training in the correct use of information processing facilities and physical security controls.
FC-5.4	Voya ensures that all Voya Personnel complete security awareness training prior to being provided access to Client PI and at least annually thereafter. Voya provides mandatory annual training programs that include security awareness training to all Personnel.
UA:	**User Access Controls**
UA-1:	User Access Controls
UA-1.1	Voya implements and maintains identity management system(s) and authentication process(es) for all systems that access, process, store, or transmit Client PI.
UA-1.2	Voya ensures that the following user access controls are in place:
UA-1.2A	The "Least Privilege" concept is implemented ensuring no user has more privileges than they require in performing their assigned duties.
UA-1.2B	Users requiring elevated privileges as a normal part of their job responsibilities have a regular, non-privileged account to perform regular business functions.
UA-1.2C	All users have an individual account which cannot be shared
UA-1.2D	Account Names/IDs are constructed not to reveal the privilege level of the account or position of the account holder.
UA-1.2E	System- or application-level service accounts are owned by a member of management or an IT system administration delegate and only have the privileges necessary to function as required by the application, system, or database for which the account has been created.
UA-1.2F	Automated processes disable access upon 24 hours of termination and initiate manager review on employee position changes, in accordance with Voya policies.
UA-2:	Access Control Management
UA-2.1	Voya maintains a comprehensive physical security program. Access to Voya facilities is restricted and logs are maintained for all access. Physical security and environmental controls are present in Voya buildings.
UA-2.2	Voya ensures that access to systems that access, process, store, or transmit Client PI is limited to only those personnel who have been specifically authorized to have access in accordance with the users' assigned job responsibilities.
UA-2.3	Voya ensures that accounts for systems that access, process, store, or transmit Client PI are controlled in the following manner:
UA-2.3A	Users must provide a unique ID and Password for access to systems. Access to applications/systems is limited to a need-to-know basis, and is enforced through role based access controls.
UA-2.3B	Accounts are protected on computing assets by screen-savers that are configured with an inactivity time-out of not more than 15 minutes.
UA-2.3C	Accounts are locked after no more than 5 consecutive failed logon attempts, depending upon the system and platform.
UA-2.3D	Accounts remain locked until unlocked by an Administrator or through an approved and secure end-user self-service process.

UA-2.3E	Accounts are reviewed on a periodic and regular basis to ensure that the account is still required, access is appropriate, and the account is assigned to the appropriate user.
UA2.4	Voya ensures that wireless mobile devices are secured against threats coming from these wireless networks and wireless connections are required to be encrypted.
UA-3:	User Access Management
UA-3.1	Voya ensures that passwords for all accounts on systems that access, process, store, or transmit Client PI are configured and managed in accordance with industry standards:
UA-4:	Information Access Restriction
UA-4.1	Voya implements information access restrictions on all systems used to access, process, store, or transmit Client Information.
UA-4.2	Voya ensures the following Information Access Restrictions are in place:
UA-4.2A	Access to underlying operating systems and application features that the user does not require access to in the performance of their assigned responsibilities are strictly controlled.
UA-4.2B	Access to source code and libraries are restricted to only those individuals who have been specifically approved to have access. A person who develops code changes cannot be the same person who migrates the code change into production.
UA-4.2C	Access between Development, Test, and Production environments are strictly controlled. The version management system provides segregation of code, data and environments.
UA-4.2D	Temporary privileged access to production data is granted to authorized personnel based on job function for emergency support and only via access control and logging security tools.
PS:	**Platform Security Controls**
PS-1:	Computer System Security (Servers and Multi-user System sonly)
PS-1.1	Voya implements and manages a formal process for ensuring that all computer systems that access, process, store, or transmit Client PI are protected and configured as follows prior to and while remaining in a production status:
PS-1.1A	Systems are assigned to an asset owner within Voya's organization.
PS-1.1B	Systems are located in a data center or similarly controlled environment with appropriate physical security mechanisms and environmental controls to ensure systems are protected from theft, vandalism, unplanned outages, or other intentional or unintentional hazards.
PS-1.1C	All systems are configured to meet Voya standards, monitored to ensure a compliant state, and patched as required to maintain a high degree of security. Issues found to be out of compliance are required to be tracked to closure.
PS-1.1D	Systems are configured with commercially available and licensed anti-virus software which is set to perform active scans, perform scans of uploaded or downloaded data/files/web content, and is updated on at least on a daily basis.
PS-1.1E	System clocks are configured to synchronize with a reputable time source (e.g., NTP).
PS-1.1F	Systems display a warning banner to all individuals during the logon process that indicates only authorized users may access the system.
PS-1.1G	Systems that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.

PS-1.1H	All high and medium vulnerability and risk issues identified are remediated utilizing a risk based approach and in alignment with application team code release schedules.
PS-1.1I	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor systems.
PS-2:	Network Security
PS-2.1	To ensure systems accessing, processing, storing, or transmitting Client PI are protected from network related threats, Voya implements the following network security controls prior to connecting any network component to a production network and for the duration that the component remains in a production status.
PS-2.1A	Networks are constructed using a defense-in-depth architecture, are terminated at a firewall where there are connections to external networks, and are routinely scanned for unapproved nodes and networks.
PS-2.1B	Business-to-Business (B2B) and Third Party network connections (Trusted) to systems accessing, processing, storing, or transmitting Client PI are permitted only after a rigorous risk assessment and formal approval by Voya management. Network connections from un- trusted sources to internal resources are not permitted at any time.
PS-2.1C	Network components (switches, routers, load balancers, etc.) are located in a data center or a secure area or facility.
PS-2.1D	Voya systems are configured to provide only essential capabilities and restrict the use of any unneeded functions, ports, protocols and services.
PS-2.1E	Intrusion detection/prevention technologies, firewalls, and proxy technologies are implemented, monitored and managed to ensure only authorized and approved traffic is allowed within and between segments of the network.
PS-2.1F	Internal Voya wireless networks are configured with the most robust security standards available, including but not limited to, 802.11i/n, strong authentication, IP/MAC address filtering, firewall protection, and intrusion detection/prevention.
PS-2.1G	Wireless networks are not used to access Client Information unless the information is encrypted at either the file or transport level.
PS-2.1H	Network components that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.
PS-2.1I	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor network components.
PS-3:	Generic Application and Database Security
PS-3.1	Voya implements and maintains an application security certification and assurance process that ensures that all applications that access, process, store, or transmit Client PI provide the following:
PS-3.1A	Application and database design ensures security, accuracy, completeness, timeliness, and authentication/authorization of inputs, processing, and outputs.
PS-3.1B	All data inputs are validated for invalid characters, out of range values, invalid command sequences, exceeding data limits, etc. prior to being accepted for production. Voya implements static source code analysis tools to validate data inputs.
PS-3.1C	Application source code developed in house by Voya is protected through the use of a source code repository that ensures version and access control. The version management system provides segregation of code, data and environments.

PS-3.1D	Applications and databases are tested for security robustness and corrective measures are applied prior to the application being placed into a production environment. All systems are configured to meet Voya standards, monitored to ensure compliance state, and patched as required to maintain a high degree of security.
PS-3.1E	Applications and databases are implemented into a production environment with minimal privileges and critical configuration files and storage subsystems are protected from unauthorized access.
PS-3.1F	Applications and databases that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.
PS-3.1G	Voya ensures that Consumer/Internet facing applications have been designed and implemented using multi-factor authentication architecture. Web sessions require the use of an HTTPS (encrypted) connection, as well as authorization to approved data and services.
PS-3.1H	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor applications and databases.
PS-4:	Workstation and Mobile Devices Security (End User Devices)
PS-4.1	Voya ensures that the following security controls have been implemented and are maintained to protect Client PI accessed, processed, stored, or transmitted on workstations and mobile devices.
PS-4.1A	Workstations are located in a physically secure environment with mechanisms in place to prevent unauthorized personnel from accessing data stored on the device, reconfiguring the BIOS or system components, or from booting the device from unauthorized media. Portable devices are configured for boot-up encryption.
PS-4.1B	Laptops/portable computers and other mobile devices are assigned to an owner who is responsible for physically securing the device at all times, and the owner of the device must receive adequate awareness training on mobile device physical security.
PS-4.1C	Portable devices are configured for boot-up encryption. All laptop hard drives are encrypted using AES 256. Any device deemed "remote" requires hard drive encryption.
PS-4.1D	All workstations, laptops/portable computers and other mobile devices (where applicable) are configured with commercially available and licensed anti-virus software which is set to perform active scans, to perform scans of uploaded or downloaded data/files/web content, and is updated on at least a daily basis.
PS-4.1E	All workstations, laptops/portable computers and other mobile devices (where applicable) are configured with a commercially available and licensed operating system, patched according to manufacturer's recommendations, hardened according to best industry practices and standards and configured so that regular users do not have administrative privileges.
PS-4.1F	Laptops/portable computers and other mobile devices (where applicable) are configured with personal firewall technology.
PS-4.1G	Workstations, laptops/portable computers and other mobile devices (where applicable) display a warning banner to all individuals during the logon process that indicates that only authorized users may access the system or device.
PS-4.1H	Voya implements and maintains processes for recovering laptops/portable computers and mobile devices from terminated Voya Personnel.
PS-5:	Backup and Restore
PS-5.1	Voya implements and maintains backup and restore procedures to ensure that all Client PI received, disclosed, created, or otherwise in the possession of Voya is appropriately protected against loss.

PS-5.2	Voya ensures that backups are securely stored and storage systems are physically and logically protected.
PS-5.3	Voya implements a backup and availability schedule to meet business and regulatory requirements.
PS-6:	Remote Network Access Controls
PS-6.1	Voya implements and maintains a remote network access control strategy or process.
PS-6.2	Voya ensures the following remote network access controls are in place:
PS-6.2A	Users requiring remote access are appropriately authorized by Voya management.
PS-6.2B	Remote access connections are established through the use of Virtual Private Networking (VPN) or secure VDI mechanisms that provide transmission security, encryption and connection timeout (e.g. split-tunneling disabled.)
PS-6.2C	Only Voya approved and controlled (managed) computing devices are used when remotely accessing (where applicable) Voya's computing environments where Client PI is held. Any device deemed "remote" requires data encryption. Encrypted communications are required for all remote connections.
PS-6.2D	Users are thoroughly authenticated using multi-factor authentication prior to being provided remote access.
ITR:	**IT Resilience Controls**
ITR-1:	Architecture
ITR-1.1	Voya ensures that the architecture of computing environments where Client PI is accessed, processed, stored, or transmitted incorporates reasonable industry best practices for authentication/authorization, monitoring/management, network design, connectivity design, firewall and intrusion prevention technologies and storage and backup capabilities.
ITR-2:	Hardware and Software Infrastructure Resilience
ITR-2.1	Voya ensures all hardware and software components classified with an availability rating of "critical" used in the accessing, processing, storage, or transmission of Client PI is: • Identified and cataloged • Supported by the manufacturer of the component (or if developed in- house, follows Voya's SDLC Policy which includes quality/security) • Applications and systems classified as A4 may be designed with high availability features and have no single point offailure • Reviewed on a regular basis for capacity implications (at minimum once every 12months)
ITR-2.2	Voya maintains Business Continuity Plans to address business unit and departmental actions to be undertaken before, during and after an incident or disaster. Voya's Disaster Recovery Plan addresses the recovery and availability of systems and data.
ITR-3:	Capacity Assurance
ITR-3.1	Voya ensures that computing environments used to access, process, store, or transmit Client PI are assessed for capacity and performance on a periodic basis (at minimum once every 12 months) and appropriate corrective actions are taken to make the environment sufficiently robust enough to perform its stated mission.
CM:	**Change Management Controls**
CM-1:	Change Management Process
CM-1.1	Voya implements and maintains a change control process to ensure that all changes to the environment where Client PI is accessed, processed, stored, or transmitted is strictly documented, assessed for impact, and approved by personnel authorized by Voya to provide approval for such changes, thoroughly tested, accepted by management, and tracked.

CM-1.2	Voya implements an emergency change control process to manage changes required in an emergency situation where a computing system is down or there are imminent threats/risks to critical systems involving Client PI.
CM-2:	Separation of Environments
CM-2.1	Voya maintains physically and/or logically separate development, test, and production computing environments. Development, testing, and acceptance environments are separate from the production environment.
CM-2.2	Voya ensures that Client data used for development or testing purposes is completely depersonalized/desensitized of confidential values prior to entering a development or test environment. Data is depersonalized in non-production controlled environments for testing purposes with required approvals. PI elements are required to be depersonalized in non- productionenvironments.
SM:	**Security Monitoring Controls**
SM-1:	Security Event Monitoring and Incident Management
SM-1.1	Voya implements and maintains a security event monitoring process and associated mechanisms to ensure events on computing systems, networks, and applications that can impact the security level of that asset or the data residing therein are detected in as close to real-time as possible for those assets used to access, process, store, or transmit Client PI.
SM-1.2	Voya implements and maintains an incident management process to ensure that all events with a potential security impact are identified, investigated, contained, remediated, and reported to Client effectively and in a timely manner.
SM-1.3	Voya has implemented monitoring controls that provide real-time notifications of events related to loss of confidentiality, the integrity, or the availability of systems.
SM-1.4	Event logs (audit trails) are stored for analysis purposes for a minimum period of 3 years.
SM-2:	Technical State Compliance
SM-2.1	Voya ensures computing environments that access, process, store, or transmit Client PII are continually in compliance with quality and security requirements including, but not limited to, authentication/authorization, monitoring/management, network design, connectivity design, firewall and intrusion prevention technologies, and storage and backup capabilities.
SM-2.2	Voya ensures IT Risk Management facilitates risk assessments of information technology processes and procedures in accordance with the annual IT Risk Assessment Plan approved by the IT/Privacy Risk Committee. Risk Assessment results are communicated to management for awareness and resolution or risk acceptance of findings based on management's risk appetite.
SM-3:	Security and Penetration Testing
SM-3.1	Voya implements and maintains vulnerability and penetration testing (Ethical Hacking) processes to ensure the computing environment where Client PII is accessed, processed, stored, or transmitted is continually protected from internal and external security threats.
SM-3.2	Voya implements and maintains a process for vulnerability scanning on at least a monthly basis and ensures issues are remediated, utilizing a risk based approach within a reasonable timeframe.
SM-3.3	Penetration testing (Ethical Hacking) of Internet facing systems or systems exposed to un- trusted networks is conducted prior to the system being deployed into a production status, after any significant changes, and then at least once every 12 months thereafter.